2022-09

WATER-BASED MITIGATION TECHNIQUES AND NETWORK INTEGRATION TO COUNTER DRONE SWARMS

Way, Meagan K.

Monterey, CA; Naval Postgraduate School

http://hdl.handle.net/10945/71097

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

WATER-BASED MITIGATION TECHNIQUES AND NETWORK INTEGRATION TO COUNTER DRONE SWARMS

by

Meagan K. Way

September 2022

Thesis Advisor:	Raymond R. Buettner Jr.
Second Reader:	Glenn R. Cook

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 WATER-BASED MITIGATION TECHNIQUES AND NETWORK INTEGRATION TO COUNTER DRONE SWARMS	**5. FUNDING NUMBERS** RM4TT; RFN5M
6. AUTHOR(S) Meagan K. Way	
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) CRUSAR, Monterey, CA 93943; RRTO	**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)

Potential and current U.S. adversaries are purchasing and deploying commercial small Unmanned Aircraft Systems (sUAS) in networked swarms. These swarms can be used for intelligence collection and reconnaissance, and have the potential to be weaponized as well. Additionally, the unlawful, but probably not malicious, activity of civilian UAS (drone) operators is of increasing concern. More specifically, there is increased risk to naval assets while in constrained environments, such as harbor transit, where both navigation and weaponized responses are serious concerns. This thesis uses the scenario of protecting a U.S. Navy destroyer entering and exiting a harbor to develop a sUAS mitigation procedure based on existing firefighting and counter-piracy technologies. The proposed procedure includes a communications plan and can be implemented almost immediately using existing civilian and military assets. Additional recommendations to improve the performance of such procedures are provided.

14. SUBJECT TERMS UAS, drone swarm, swarm, drone, autonomous, s-UAS, small-unmanned aircraft systems, unmanned aircraft system	**15. NUMBER OF PAGES** 93
	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

WATER-BASED MITIGATION TECHNIQUES AND NETWORK INTEGRATION TO COUNTER DRONE SWARMS

Meagan K. Way
Lieutenant, United States Navy
BS, University of Memphis, 2013

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN NETWORK OPERATIONS AND TECHNOLOGY

from the

NAVAL POSTGRADUATE SCHOOL
September 2022

Approved by: Raymond R. Buettner Jr.
Advisor

Glenn R. Cook
Second Reader

Alex Bordetsky
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Potential and current U.S. adversaries are purchasing and deploying commercial small Unmanned Aircraft Systems (sUAS) in networked swarms. These swarms can be used for intelligence collection and reconnaissance, and have the potential to be weaponized as well. Additionally, the unlawful, but probably not malicious, activity of civilian UAS (drone) operators is of increasing concern. More specifically, there is increased risk to naval assets while in constrained environments, such as harbor transit, where both navigation and weaponized responses are serious concerns. This thesis uses the scenario of protecting a U.S. Navy destroyer entering and exiting a harbor to develop a sUAS mitigation procedure based on existing firefighting and counter-piracy technologies. The proposed procedure includes a communications plan and can be implemented almost immediately using existing civilian and military assets. Additional recommendations to improve the performance of such procedures are provided.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

APDS	Armor piercing discarding sabot
ATHENA	Advanced Test High Energy Asset
B2B	bridge-to-bridge
C2	command and control
C3	command, control and communication
CDS	Common Display Systems
CIC	Combat Information Center
CICWO	CIC Watch Officer
CIWS	close-in weapon system
CO	Commanding Officer
COMMO	Communications Officer
COMM PLAN	communications plan
C-RAM	Counter Rocket, Artillery, and Mortar
C-UAS	counter unmanned aircraft system
CRUSAR	Consortium for Robotics and Unmanned Systems Education and Research
CIWS	close-in weapon system
CLWS	Compact Laser Weapon System
CORIAN	Counter-Remote Control Model Aircraft Integrated Air Defense Network
C-UAS	counter unmanned aerial system
DDG	guided missile destroyer
DESRON	Destroyer Squadron
DOD	Department of Defense
DON	Department of the Navy
DRAKE	Drone Restricted Access Using Known EW
EAPS	Enhanced Area Protection and Survivability System
ECO	Edison Chouest Offshore
EM	electromagnetic
EMI	electromagnetic interference

EMP	electromagnetic pulse
EO	electro-optical
GCS	ground control station
GHz	gigahertz
GNSS	Global Navigation Satellite System
GPM	gallons per minute
GPS	Global Positioning System
HELIOS	High Energy Laser with Integrated Optical-dazzler and Surveillance
HELWS	High-Energy Laser Weapon System
HPM	high power microwave
Hz	hertz
IR	infrared
ISIC	Immediate Superior in Charge
ISIS	Islamic State of Iraq and Syria
ISM	industrial, scientific and medical
ISR	intelligence, surveillance and reconnaissance
JFMM	Joint Fleet Maintenance Manual
LaWS	Laser Weapon System
LMADIS	Light Marine Air Defense Integrated System
LoS	line of sight
LWSD	Laser Weapon System Demonstrator
NNEMP	non-nuclear electromagnetic pulse
NSWDD	Naval Surface Warfare Center Dahlgren Division
ODIN	Optical Dazzling Indicator
OOD	Officer of the Deck
PSI	pounds per square inch
RAM	Rolling Airframe Missile
RDA	research, development and acquisition
RF	radio frequency
RSSC	Regional Satellite Communications Support Center
SDHP	San Diego Harbor Police

SNR	signal-to-noise ratio
SUAS	small unmanned aircraft system
THOR	Tactical High Power Operational Responder
UAS	unmanned aerial system
UAV	unmanned aerial vehicle
U/I	Under Instruction
USCG	United States Coast Guard
USCGC	United States Coast Guard Cutter
USN	United States Navy
VHF	very high frequency
WMFFP	Water Mist Fire Fighting Pump
XO	Executive Officer

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First and foremost, I want to thank my advisor, Dr. Raymond Buettner, for his guidance and patience during the writing of this thesis. His expertise and knowledge led to a very interesting topic and ignited a love of UASs for me. A big thank you to my second reader, Mr. Glenn Cook, for being a great professor and mentor during my time at NPS. Most importantly, I thank my family. I thank my husband, Justin, for supporting me and being my rock during the hard days and sleepless nights and for being a wonderful father to our kids, Hudson and Haven. I could not have completed this thesis without your love and support.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

This thesis defines the general requirements for the integration of a water-based unmanned aircraft system (UAS) swarm mitigation technique into the operations of a U.S. Navy (USN) Destroyer (DDG) using existing assets, along with the communications required for this integration. UAS are the next major evolution in military warfare as they continue to fill more roles previously performed by manned aerial systems. UASs have proliferated the civilian and commercial markets at an astronomical rate. As presented at the 2016 8th International Conference on Cyber Conflict, UASs are currently used for various military applications, such as intelligence, surveillance and reconnaissance, as well as federal and local law enforcement missions, to include monitoring, rescue, and border control (Hartmann & Giles, 2016).

Because of the simplicity, availability and relatively low cost of UASs on the market today, there are growing instances of civilian and commercial UASs being utilized in a hostile manner. U.S. adversaries, nonstate actors and individuals are beginning to operate large quantities of small unmanned aircraft systems (sUAS) for attacks, evident in the UAS attack on a Russian air base in 2018 (Dockrill, 2018) and the Syrian oil production field UAS attack in 2019 (Pawlyk, 2019). There was a coordinated drone swarm attack on U.S. troops at At-Tanf, a U.S. base located in Syria (Liebermann, 2021). In 2022, reconnaissance drones have been used by Ukraine on the frontlines of war to look for Russian artillery, and some have been used offensively to drop small explosives on Russian vehicles (Shankland, 2022). Autonomous use of UASs is a threat that is growing rapidly, with UAS swarms being researched and developed by nation-states around the world. As swarming technology matures it will inevitably migrate beyond the control and use of nation-states.

Because of the potential threat that UAS swarms pose against the U.S. domestically and internationally, the development and use of counter-UAS (C-UAS) technologies have become a priority for the Department of Defense (DOD) and law enforcement agencies. According to the Congressional Research Service, the DOD is planning to spend around $636 million on C-UAS research, development and acquisition (RDA) in fiscal year 2022

(Hoehn & Sayler, 2021) along with approximately $75 million in the procurement of C-UAS technologies. The DOD is working to “maintain a time and [UAS] technology advantage over threat users” (Wilson, 2018, para. 4). To align with the *National Defense Strategy*, the Department of the Navy (DON) created the Unmanned Campaign Framework to “increase lethality, capacity, survivability, operational tempo, deterrence, and operational readiness” (Department of the Navy [DON], 2021, para. 4).

All branches of the DOD have implemented C-UAS measures, both non-kinetic and kinetic. Kinetic methods involve the physical interdiction of the UAS, such as nets and munitions. Non-kinetic methods involve incapacitating the UAS through a method outside of the kinetic realm, such as jamming or disabling the electrical components of a UAS. However, whenever a warship is navigating the waters of a harbor environment, the use of kinetic and non-kinetic counter-swarm techniques can be inhibited due to the harbor environments being surrounded by non-military vessels, businesses and even residential neighborhoods. In order for a warship to reduce the risk of UAS swarms in this environment there needs to be an integrated mitigation technique that can be safely employed to reduce the ability of these swarms to target the warship.

A. PROBLEM STATEMENT

The development of C-UAS technology is increasing in importance for the DOD in order to keep up with the errant and malevolent use of sUAS. Due to the unique characteristics of the domestic harbor environment, a non-kinetic swarm mitigation technique should be developed to reduce the effectiveness of UAS swarms that may target ships transiting the harbor. A water-based mitigation strategy as a swarm defense option is explored in this thesis. Existing firefighting and counter-piracy technologies are proposed to accomplish this mitigation and provide an inexpensive solution that is suitable for almost immediate implementation. Additionally, a communications pathway must be established with the involved entities in the harbor for an effective C-UAS swarm water mitigation technique so a communications CONOP is also proposed.

B. BACKGROUND AND NEED

Inexpensive unmanned aerial vehicles (UAV) are commonly referred to as "drones" in the civilian sector and have become accessible to nearly the entire consumer market. UAS have become an invaluable asset for U.S. military, particularly for intelligence-gathering missions and operations. Speicher defines the term UAV as the aircraft itself, whereas the larger UAS consists of the UAV and the components needed to operate the UAV, including the ground control station (GCS) and communications packages (Speicher, 2016). The DOD states that UAS encompasses the equipment, personnel and the communications required to control a UAV (Joint Chiefs of Staff [JCS], 2020). Although "drones" is a popular lexicon used by the general public, this thesis will refer to unpiloted aircraft and onboard components as UAS throughout due to the military context. The term UAV will describe the vehicle without the components required for a UAS. UAS technology has expanded significantly since the late 20th century, enabling an increase in capabilities and missions for the military.

UAS serve a multitude of purposes and services based on the sensor capabilities available. UAS swarms allow the military to "monitor the region much more efficiently with a minimal manual effort, by automatically sending an alert to the base station upon detection of movement" (Tahir et al., 2019, section 2.1). Missions that are amenable to the use of swarm technology have been and are under study. Cartography, also known as map drawing, is an underrepresented use of UAS. Search and rescue is another application in which UAS are utilized to provide up-to-date, real time, aerial images to search and rescue teams (Tahir et al., 2019). Drones can be outfitted with thermal imaging cameras to aid search and rescue operations (Callahan, 2021). Along with search and rescue, UAS swarms can aid firefighters in locating fire hot spots using geospatial data (Press, 2022). Cartography and search and rescue are examples of how swarm technology can allow for more efficient coverage of large areas. As UAS technology advances, many more non-military applications will be developed.

UAS swarms will be the next major cutting-edge technology in modern military warfare. Although swarm technology is still in the early stages of adoption and "there is no clear threshold on the quantity of drones that must be connected to create a swarm"

(Gagaridis, 2022, under “The ‘Swarming’ Concept”), the wars of the future will likely be fought largely with swarm technology and autonomous systems. As warfare evolves, drone swarms can greatly enhance a warfighter’s capability by eliminating vulnerabilities through swarm redundancy and collective resiliency (Gagaridis, 2022).

Pentagon leaders believe that the ultimate threat on the future battlefield will be small drone swarms, not IEDs (Williams, 2021). Just as the U.S. military is exploring the use of swarms during military operations, Breeden states other militaries are using swarm drones in exercises with the intent to deploy them in the future (Breeden, 2021). Terrorists can easily target a DDG and plan a swarm attack through the use of open-sourced information for determining ship location, placement of weapons systems onboard, and deployment schedule. Current military C-UAS weapons systems may not be able to defend against swarms effectively, especially in the domestic harbor environment. Innovations in C-UAS technology must fill the gap between the swarm threat and the capability to defend against the swarm threat. UAS operating as a swarm are difficult to defeat, because UAS swarms are designed to be resilient and autonomously reconfigure as individual UAS are destroyed. According to Breeden, swarm intelligence is a term commonly used to describe the autonomous resiliency of UAS swarms (Breeden, 2021).

C. PURPOSE

This research addresses the general challenge of mitigating UAS swarm risk in the domestic harbor environment by focusing on a specific ship type (DDG) and a specific harbor (San Diego). This research is focused on a DDG because a larger ship, such as an aircraft carrier, would likely be too large to protect with water effectively. The San Diego Harbor was chosen as the research environment due to its importance as a U.S. domestic port, along with its challenging proximity to both collateral damage, such as civilian infrastructures, and many potential launch points for threats along the shoreline. A water-mitigation technique is a safer solution for addressing a UAS swarm problem in the San Diego Harbor. A mitigation technique would be a preventative measure, whereas countering the UAS swarm occurs when the threat is already identified. This thesis proposes utilizing the water resources available in the harbor and developing a communications network between a USN DDG, the U.S. Coast Guard (USCG), San Diego Harbor Police (SDHP) fireboats and Edison Chouest Offshore (ECO) tugboats.

This thesis researches and investigates the effects of a water mitigation maritime strategy to mitigate against a UAS swarm attack. There is no significant research on the U.S. military mitigating swarms using water sources readily available as each ship navigates in and out of the harbor. The requirements for this research will include establishing an effective command, control and communication (C3) system between Navy warships, SDHP fireboats, USCG and ECO tugboats to successfully defend against a potential swarm threat. The development of a water mitigation technique would not only benefit USN warships in port, but also ground forces located near bodies of water. Along with military applications, civilian law enforcement could benefit from this water mitigation research.

D. RESEARCH QUESTIONS

This research will define the general requirements for integrating or deconflicting a water-based UAS swarm mitigation technique using fireboats, tugboats, the USCG and a USN DDG. It will focus on defining the communications options available for the afore mentioned technology to defend against a UAS swarm attack in the San Diego Harbor. To achieve success against a UAS swarm, the research questions that will be explored are: How could water cannons be used as a part of a non-kinetic UAS mitigation strategy, particularly in the context of the San Diego Harbor? What are the communications requirements needed for a USN DDG, fireboats, USCG and tugboats to utilize a water mitigation technique against a UAS swarm threat in the San Diego Harbor?

E. RESEARCH APPROACH, LIMITATIONS AND CHALLENGES

UAS technology is rapidly advancing, much quicker than countermeasures can be developed. Therefore, there will never be an all-inclusive technology that can counter all UAS and UAS swarms. However, this thesis intends to provide a proof of concept for a mitigation method that could potentially allow DDGs, civilian fireboats and tugboats, and the USCG to communicate and destroy adversary UAS swarms using readily available water sources. To accomplish this task, a significant amount of background research had to be conducted to fully understand the problem at hand. To understand UAS swarms, an understanding of how a UAS operates and communicates, as well as the capabilities, had to be developed. Addressing the current C-UAS technologies and their limitations allows the research to show the benefit of a water-mitigation technique instead of a C-UAS method. The San Diego Harbor was picked for the hypothetical environment of this thesis to highlight how current kinetic and non-kinetic C-UAS techniques are not always feasible. Also, limiting the scenario to one location, the San Diego Harbor, allows specific entities to be involved in the defense against possible UAS swarms.

COVID-19 was a major limiting factor for the experimentation phase of this thesis due to social distancing and limited travel across the DOD. It prevented the testing of a water mitigation technique as an effective defense against a UAS swarm and impacted the opportunity to conduct the final part of the thesis. Ideally, water cannons would have been used to provide a wall of water for a DDG in the San Diego Harbor with help from the tugboats, SDHP fireboats and the USCG in an attempt to protect against any simulated UAS swarm threats. Experimentation would have allowed data collection in order to prove proof of concept. However, the research was concluded without the benefit of experimentation and physical data collection.

F. THESIS OUTLINE

This thesis is organized as follows. Chapter II is a literature review of UAS technologies. A history of swarm attacks set the tone for the introduction of UAS swarm technology. Next, UAS capabilities and classifications, along with UAS command and control methods are presented. Chapter III provides a detailed overview of current C-UAS technologies and highlights the deficiencies and limitations in the current UAS countermeasures, including the C-UAS technologies onboard USN DDGs. Chapter IV outlines the entities involved in the water mitigation strategy of this thesis, the equipment onboard each, and the design and benefit of the strategy and the network integration to make this strategy a success. Conclusions and recommendations for future studies are presented in Chapter V.

II. UAS TECHNOLOGY AND THE THREAT

In order to respond to UAS threats, there must be an understanding of the threat itself. Chapter II starts with examples of UAS attacks to establish the urgent need to defend against these threats. The research then takes an in-depth look at UAS technology, capabilities and classifications in order to understand how the system operates in order to develop effective countermeasures. The Command and Control (C2) of UAS are outlined, along with UAS threats, in order to understand which C-UAS techniques would be used to eliminate those threats, as well as limitations in current C-UAS methods.

A. HISTORY OF UAS ATTACKS

In the early morning hours of January 10, 2018, 13 armed UAS attacked Hmeimin air base, a Russian air base located in the Latakia province of Syria. In total, seven UAS were shot down and non-kinetic measures were taken to bring down the other six UAS. This UAS attack was the first time that UAS were reported to be used in a loosely coordinated assault against a military target, aimed to attack the headquarters of Russian military operations (Dockrill, 2018). On this day, a new method of aerial warfare was born (Sly, 2018).

On September 14, 2019, Saudi Arabia's Abqaiq oil production facility and the Al Khurais oil production field fell under attack by cruise missiles and a weaponized group of UAS. The group of UAS were timed at launch to facilitate a nearly simultaneous arrival and were suspected to have originated in Iran. This UAS attack showcased the lack of C-UAS technologies in the Saudi Arabia's air-defense system (Sisk, 2019). These weaponized UAS were highly accurate in their attack with the destruction of 12 of the gas-oil separation tanks located at Abqaiq, essentially hindering the production of about five million barrels per day for Saudi Arabia (Pawlyk, 2019).

U.S. Central Command released a statement on a weaponized UAV attack that occurred on July 30, 2021, against the Motor Tanker Mercer Street near the Oman coast. It was determined that the Iranian-produced UAV was part of a one-way operation with military-grade, nitrate-based explosives and destruction as the mission. The single UAV produced a six-foot hole in the tanker and killed two crewmembers on board (Urban, 2021).

The rise in UAS utilization by U.S. enemies is fueling the need for the DOD to develop counter technologies to the UAS threat. These three UAS attack examples were carried out by only a handful of UAS and caused significant damage. If a swarm of autonomous UAS were to carry out the same attacks, the property damage and loss of life could have been much greater.

B. CLASSIFICATION

Classification of UAS is essential to understanding how a UAS is designed and how it operates. It is important to note that there is not one single categorization method that exists for UAS (Castillo-Effen et al., 2017), and there are variations between the civilian and military UAS categories. Understanding the design elements and operational characteristics will help differentiate and identify the UAS in a swarm. Generally, UAV are classified based on their size, range, altitude and number of rotors, as seen in the chart in Figure 1.

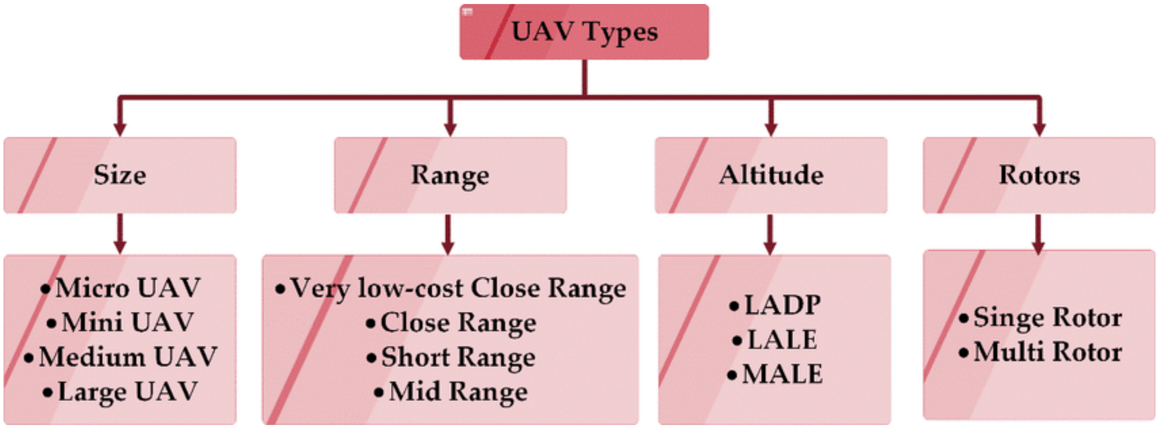


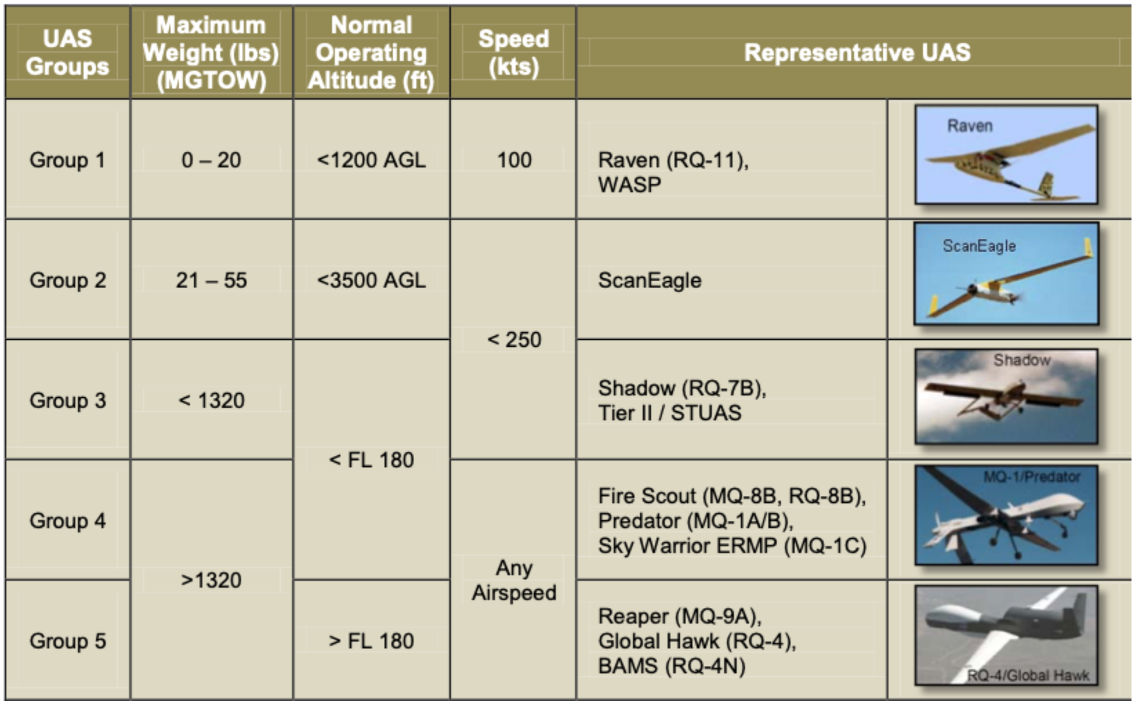
Figure 1. UAV types. Source: Ganesan et al. (2020).

The DOD specifically categorizes UAS into three categories: weight, operating altitude and airspeed (Castillo-Effen et al., 2017). Table 1 shows the DOD UAS classification scheme that breaks down UAS into five separate groups. This thesis will address additional characterization, because these characteristics ultimately determine which C-UAS measures will be taken against the UAS swarm threat.

1. Size

The size of a UAV is the simplest method of categorization. Table 1 describes group 1 as having a maximum weight of 20 pounds or less, and a UAS with a total weight of less than 55 pounds is categorized as an sUAS (Castillo-Effen et al., 2017).

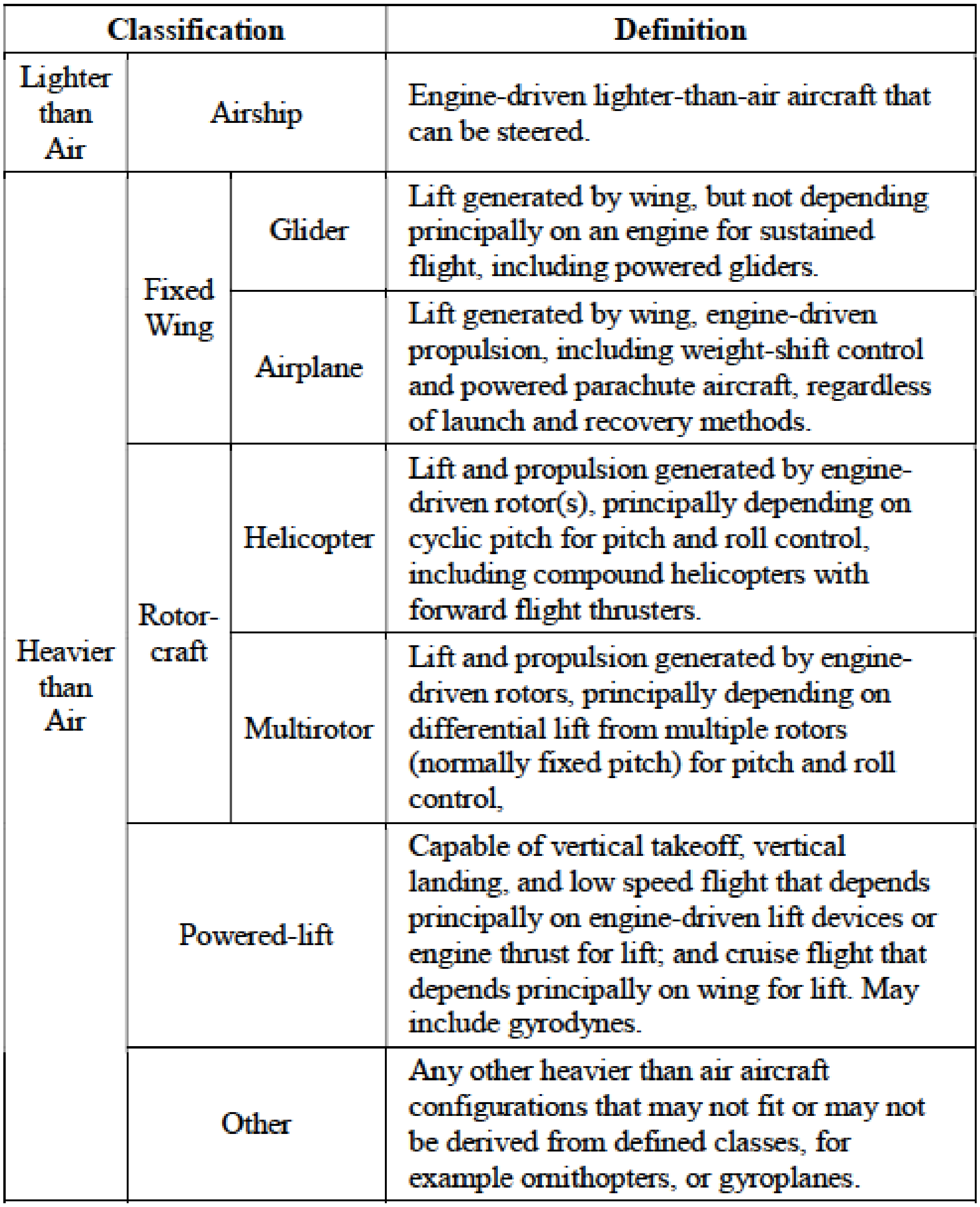
Table 1. DOD UAS classification guide: Source: DOD (2011).



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

The weight of a UAS can determine its performance and capabilities, but is mainly considered when factoring the safety-risk the sUAS poses against human populations. Table 2 is an example of sUAS being characterized by weight, either lighter than air or heavier than air (Castillo-Effen et al., 2017).

Table 2. sUAS Aircraft Configuration Classification. Source: Castillo-Effen et al. (2017).

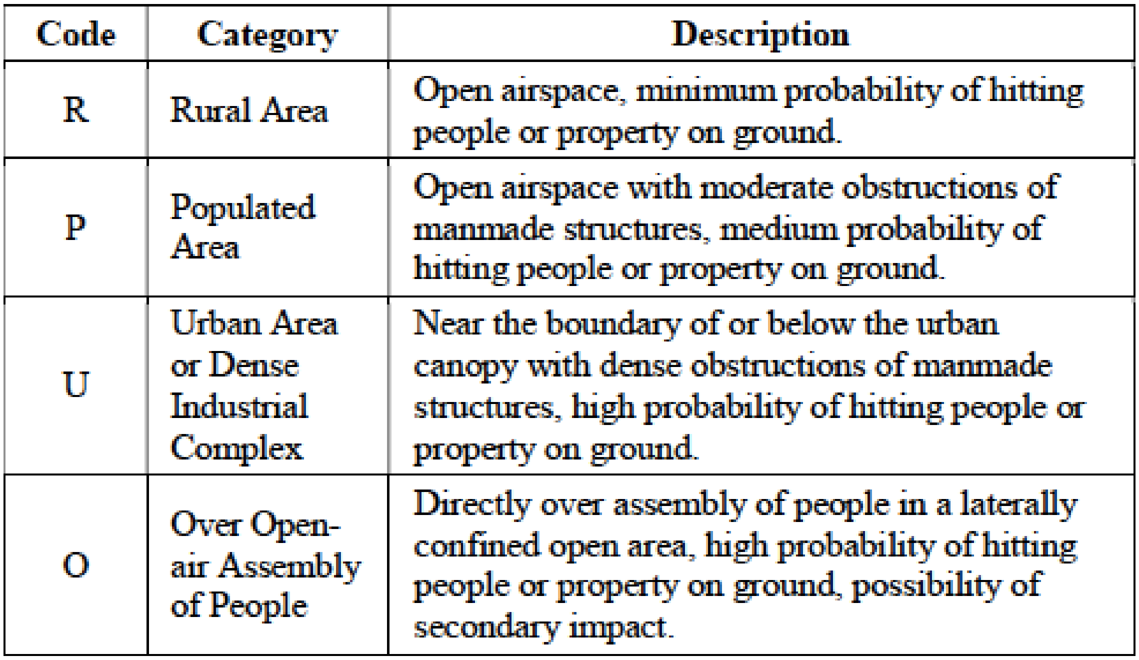


Classification			Definition
Lighter than Air	Airship		Engine-driven lighter-than-air aircraft that can be steered.
Heavier than Air	Fixed Wing	Glider	Lift generated by wing, but not depending principally on an engine for sustained flight, including powered gliders.
		Airplane	Lift generated by wing, engine-driven propulsion, including weight-shift control and powered parachute aircraft, regardless of launch and recovery methods.
	Rotor-craft	Helicopter	Lift and propulsion generated by engine-driven rotor(s), principally depending on cyclic pitch for pitch and roll control, including compound helicopters with forward flight thrusters.
		Multirotor	Lift and propulsion generated by engine-driven rotors, principally depending on differential lift from multiple rotors (normally fixed pitch) for pitch and roll control,
	Powered-lift		Capable of vertical takeoff, vertical landing, and low speed flight that depends principally on engine-driven lift devices or engine thrust for lift; and cruise flight that depends principally on wing for lift. May include gyrodynes.
	Other		Any other heavier than air aircraft configurations that may not fit or may not be derived from defined classes, for example ornithopters, or gyroplanes.

2. Type of Flight

Type of flight is another method of categorization for UAS. This method is similar to the way general aviation flights are categorized. The location of the UAS flight is important in determining what the UAS can withstand and its possible trajectory. Table 3 shows four different types of flight categories: rural area, populated area, urban area and over open-air assembly of people (Castillo-Effen et al., 2017).

Table 3. sUAS Type of Flight. Source: Castillo-Effen et al. (2017).



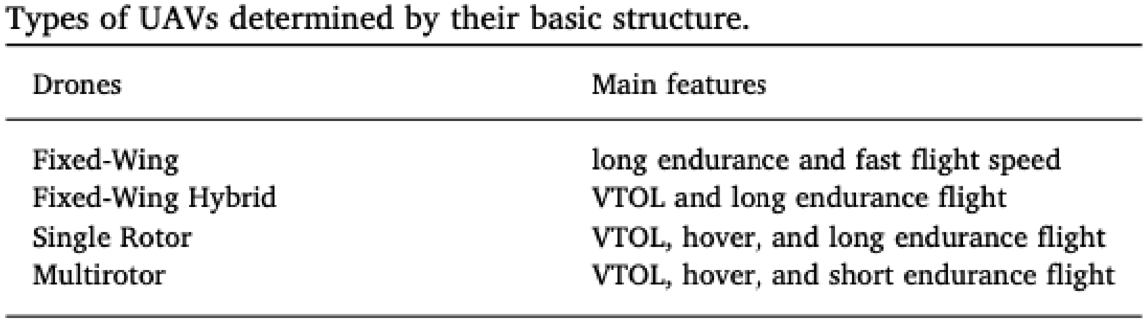
Code	Category	Description
R	Rural Area	Open airspace, minimum probability of hitting people or property on ground.
P	Populated Area	Open airspace with moderate obstructions of manmade structures, medium probability of hitting people or property on ground.
U	Urban Area or Dense Industrial Complex	Near the boundary of or below the urban canopy with dense obstructions of manmade structures, high probability of hitting people or property on ground.
O	Over Open-air Assembly of People	Directly over assembly of people in a laterally confined open area, high probability of hitting people or property on ground, possibility of secondary impact.

As described by Castillo-Effen et al., the rural category is described as open airspace with a lack of structures, buildings and other obstructions (2017). The popular area category may cause UAS encounter manmade structures with a medium-likelihood to come in contact with a population or building. The third category is urban, described as having a high probability of hitting obstructions. The final category of type of flight is over open-air assembly of people, requiring an assessment of trajectory due to the highest possibility of impacting humans or property (Castillo-Effen et al., 2017).

3. Fixed Wing or Rotary Wing

UAVs are broadly categorized as either fixed wing or rotary wing, with these two classifications broken down further into fixed wing hybrid and single rotor or multirotor, as shown in Table 4.

Table 4. UAV categorized by structure. Source: Tahir et al. (2019).



Types of UAVs determined by their basic structure.

Drones	Main features
Fixed-Wing	long endurance and fast flight speed
Fixed-Wing Hybrid	VTOL and long endurance flight
Single Rotor	VTOL, hover, and long endurance flight
Multirotor	VTOL, hover, and short endurance flight

The capabilities of fixed and rotary wing UAS often overlap, and missions typically utilize a combination of both categories of UAS for success. In order to understand the differences between fixed and rotary wing, an assessment and comparison of the pros and cons must be performed.

a. Fixed wing

Fixed wing UAS are preferred when a long-range vehicle is needed, such as aerial mapping of a large geographical area or when the UAS needs to operate at higher altitudes (Airborne Drones, 2017). Fixed wing UAS are able to carry payloads for longer distances because of the ratio of superior lift versus weight and thrust versus drag. Similar to other fixed wing aircraft, fixed wing UAS need a significant amount of runway clearance for take-off and landing or a complex launch and recovery mechanism. According to Airborne Drones, this disadvantage makes fixed wing UAS unsuitable for any operations requiring stationary capabilities, such as inspection work (2017).

b. Fixed wing hybrid

Fixed wing hybrid UAS use automation and fixed-wing powered flight for flying and maneuvering (Tahir et al., 2019). The purpose of using a fixed wing hybrid UAS is to take off and land vertically but also retain the benefits of a fixed wing aircraft. This category of UAS is in the beginning stages, but Amazon is tackling this new UAS approach with its Prime Air delivery UAS (Chapman, 2019), and Walgreens has contracted a delivery company, Wing, to deliver goods to consumers (Rains, 2021). As UAS technology advances, fixed wing hybrid UAS will likely become more popular in the consumer UAS market. Figure 2 is Amazon’s Prime Air delivery, an example of a fixed wing hybrid UAS. Figure 3 shows the Walgreens Wing delivery hybrid drone with fixed wing and hover propellers.

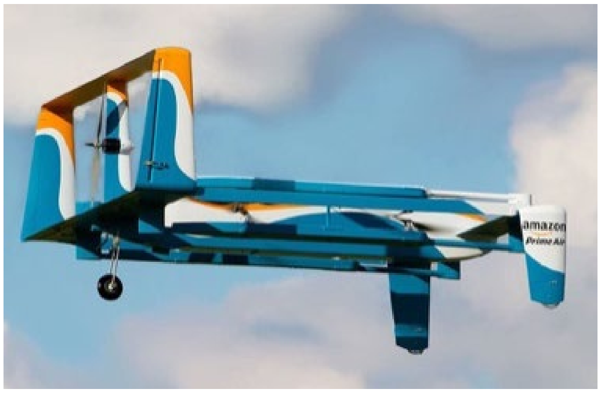


Figure 2. Amazon’s Prime Air delivery UAS. Source: Chapman (2019).

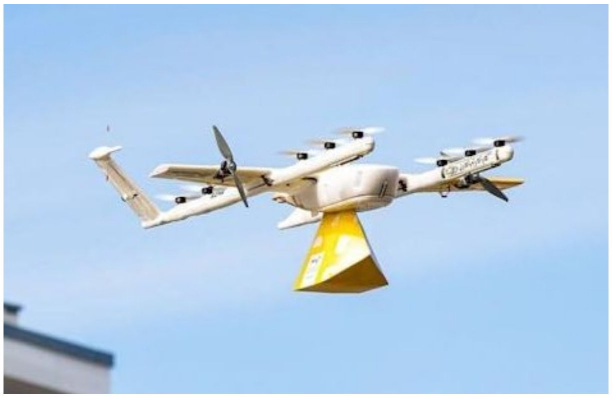


Figure 3. Wing drone delivery company hybrid UAS. Source: Rains (2021).

c. Multirotor

Multirotor UAS are primarily used for missions that require a shorter flight time, usually between 15 and 30 minutes. Similar to helicopters, multirotor UAS are able to maneuver into tight spaces and take off and land with little clearance. Figure 4 shows three examples of multirotor, fixed wing and single rotor UAS.

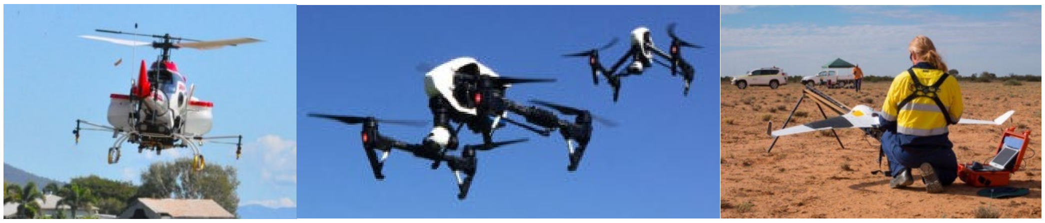


Figure 4. Multirotor, fixed wing and single rotor UAS.
Source: Chapman (2019).

A multirotor UAS has the advantageous capability of lifting off and landing in a vertical motion (Airborne Drones, 2017). Multirotor UAS are user friendly and easy to master. Despite its clear advantages, a major drawback of utilizing multirotor UAS is the inability to fly long distances. Table 5 gives an overview of the pros and cons of each UAS structure.

Table 5. Pros and cons of UAS structures. Adapted from Chapman (2019).

Type of Structure	Pros	Cons
Multirotor	• Accessibility • Ease of use • VTOL and hover flight • Good camera control • Can operate in a confined area	• Short flight times • Small payload capacity
Fixed Wing	• Long endurance • Large area coverage • Fast flight speed	• Launch and recovery needs a lot of space • No VTOL/hover • Harder to fly, more training needed • Expensive
Single Rotor	• VTOL and hover flight • Long endurance (with gas power)	• More dangerous • Harder to fly, more training needed • Expensive
Fixed Wing Hybrid	• VTOL and long-endurance flight	• Not perfect at hovering or forward flight • Still in development

C. UAS COMMAND AND CONTROL

UAS within a swarm communicate wirelessly to share navigation and telemetry data, along with larger files such as images or videos. UAS communications are susceptible to interference, either intentional or unintentional. To understand how to disrupt or defeat a UAS swarm, a topic addressed in Chapter III, an understanding of radio frequency (RF) communications needs to be established.

1. UAS Communication

The foundation of UAS communications is the electromagnetic (EM) spectrum. The EM spectrum models EM energy as propagating in the form of waves. Each frequency range of wave propagation has an application in the real world, from relatively long wavelength radio waves used for FM radio to short wavelength gamma rays resulting from radioactive decay of atomic nuclei. Visible light is the only portion of the EM spectrum that is observable to the naked eye. Figure 5 shows common applications of the EM spectrum.

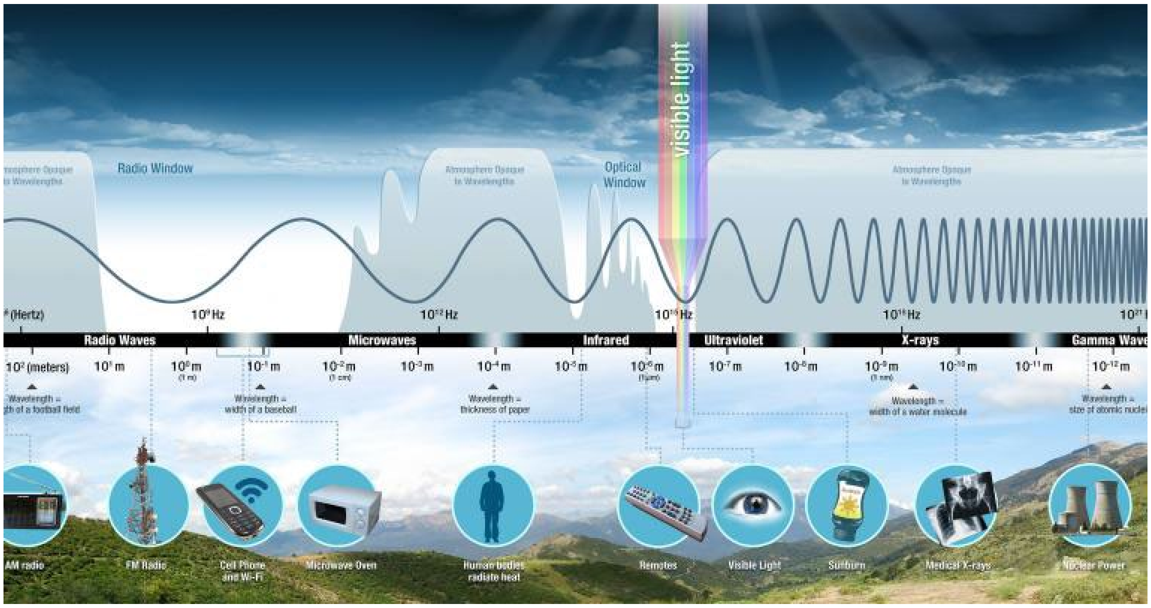


Figure 5. EM spectrum and its applications. Source: Butcher et al. (2016).

UAS communications use the radio wave, microwave, and millimeter wave frequencies of the EM spectrum, from 30 hertz (Hz) to 300 gigahertz (GHz), to transmit information and data. The frequency, bandwidth and antennas used by a UAS determines its ability to receive and transmit data successfully. The following sections explain the anatomy of EM waves in relation to UAS communications.

a. Frequency

An EM wave is categorized by its frequency, which is the rate at which something occurs given a specific period of time. In relation to EM waves, the frequency is the number of times the crest of the waves passes a particular point within one second, with each repetition described as a Hz. For example, if a wave passes four cycles by a specific point in one second, then the wave has a frequency of 4 Hz (Butcher et al., 2016). The wave can also be described by wavelength (λ), as shown in the equation $\lambda = \frac{c}{f}$ where c represents the speed of light, $3x10^8$ meters per second, divided by the frequency. Figure 6 is a visual representation of frequency and wavelength.

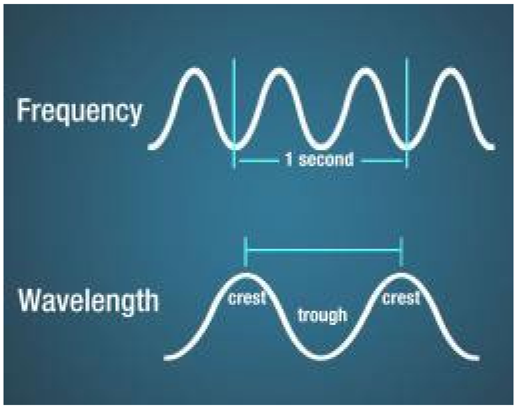


Figure 6. Visual of frequency and wavelength. Source: Butcher et al. (2016).

Frequencies vary in their ability to transmit data over distances. Frequency and wavelength are inversely proportional, meaning the lower frequencies have longer wavelengths and can propagate further, whereas higher frequencies have shorter wavelengths and can only travel shorter distances. Lower frequency waves trade off being able to travel long distances with a reduced ability to carry data. Higher frequency waves are able to carry more information but often are constrained to line of site propagation limits. More than 90% of GCS use 2.4 GHz in the industrial, scientific and medical (ISM) band to communicate with UAV, but wireless computer networks also use this frequency. Therefore, 5.8 GHz is also used to avoid interference with wireless computer networks. As said by Butcher et al. in *Tour of the Electromagnetic Spectrum*, 433 MHz is a frequency that is sometimes used for communications requiring a longer distance than 2.4 GHz can accommodate (2016).

b. Bandwidth

The range of frequencies used to make up a signal is referred to as the bandwidth. Frequency and bandwidth are proportional. For example, higher frequencies have more bandwidth than lower frequencies, and more data can be transferred. Therefore, UAS that use lower frequencies with smaller bandwidth would not be able to transmit large data files, such as video or higher resolution images.

c. Antenna

UAS transmit and receive information in the form of RF energy over long distances for communications with the GCS or other UAS in the swarm. Antennas have four characteristics that affect UAS operations: radiation pattern, directivity, polarization and bandwidth.

(1) Radiation Pattern

A radiation pattern is a description of how an antenna distributes its energy in space, indicating the antenna's strength. Antennas do not radiate energy in all directions, but in certain directions and angles that form a pattern. The radiation pattern of typical directional antenna is typically modeled as having three sections: a main lobe, side lobes and a back lobe, as depicted in Figure 7. The main lobe is where most of the radiated energy is located and is considered the desired radiation direction of the antenna (McNeil, 2017). The side and back lobes are by products of inefficient antenna design, waste energy, and create vulnerabilities to interception, exploitation, and jamming. In order to improve the efficiency and directivity of antennas, the side lobes and back lobe are typically reduced or eliminated through improved design and directivity.

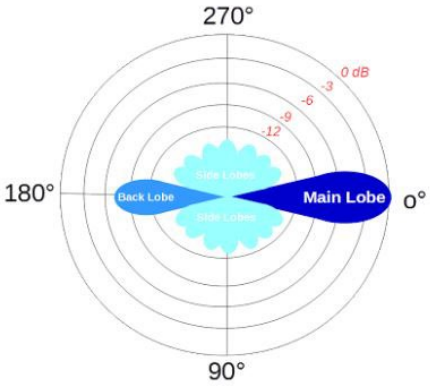


Figure 7. Radiation pattern with lobes. Source: McNeil (2017).

(2) Directivity

Antenna directivity is a fundamental parameter that refers to “how ‘directional’ an antenna radiation pattern is” (Bevelacqua, 2015, para. 1). Antennas with low directivity are often used for mobile applications, such as UAS swarms, because the direction between the transmitter and receiver are constantly changing with a need to transmit and receive in various directions. Antennas with high directivity are used for more fixed applications, such as satellite television (Hughes, 2016), where a centralized beam is necessary to maximize power transfers.

(3) Polarization

Antenna polarization refers to the orientation, or plane, of the electrical field of EM waves. There are two commonly used antenna polarization for UAS communications: linear and circular. Polarization in part determines the antenna pattern of the transmitted energy, and antennas receive or transmit signals based on the polarization of the incoming or outgoing signal. The polarization of the RF antenna must be matched to the incoming signal in order to maximize the amount of signal that is received without losses due to a mismatch.

(4) Antenna bandwidth

Antennas can receive and transmit a wide range of RF frequencies. This is known as the antenna bandwidth and is one factor in determining what type of antenna(s) a UAV will have onboard for communications with the GCS and other UAS in the swarm.

2. UAS Control Modes

The levels of autonomous control vary based upon the task, mission or operation that the UAS or swarm is performing. The levels of autonomy range from no autonomy to full autonomy. Traditionally-operated UAS are controlled by human decisions, and fully autonomous UAS and swarms are controlled by algorithmic decisions. In a 2018 conference for the IEEE, Campion et al. stated these levels of autonomous control use two different forms of communications architectures: infrastructure-based and ad-hoc network-based (2019).

The infrastructure-based communications architecture involves a GCS receiving telemetry data from multiple UAV and then uses this data to coordinate the flight paths of each UAV. With infrastructure-based architecture there is no need for networking between the UAV because the GCS communicates directly with each UAV. Because each UAV communicates directly with the GCS, this architecture would not be used in a swarm. Figure 8 is a visual depiction of an infrastructure-based communications architecture for central control of multiple UAV.

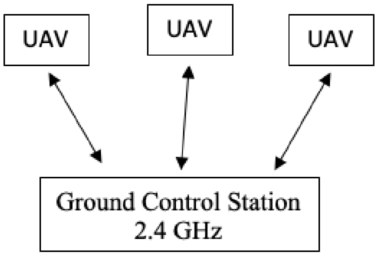


Figure 8. Infrastructure-based UAV swarm communications architecture. Adapted from Campion et al. (2019).

Ad-hoc network-based communications architecture does not require physical infrastructure, but instead relies on dynamic routing algorithms to create a wireless network suitable for a UAS swarm. Because an ad-hoc network does not require physical infrastructure, such as routers or access points, this network is redundant during operations. An ad-hoc architecture allows all UAS in the swarm to communicate in real-time, because each UAS does not need to reach back to the GCS for telemetry data. Figure 9 is a visual representation of an ad-hoc network-based communications architecture for UAS swarms.

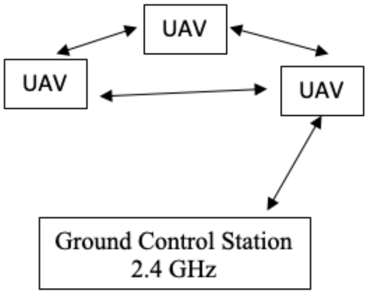


Figure 9. Ad-hoc network-based UAS swarm communications architecture. Adapted from Campion et al. (2019).

D. UAS SWARM TECHNOLOGY

1. Self-Organization

One distinction between a UAS and a UAS swarm is the ability to self-organize. Specifically, "a swarm is generally defined as a group of behaving entities that together coordinate to produce a significant or desired result or behavior" (Campion et al., 2018, Sec. 2, para. 2). UAS in a swarm can make decisions together and amongst themselves in real-time without the input from a human controller on the ground (McMullan, 2019). This allows the UAS in a swarm to respond to unforeseen hostile UAS in an adaptable manner, which is valuable for military objectives but also utilized by the enemy (McMullan, 2019). UAS swarms can be compared to a swarm of bees in nature. Each bee thinks for itself while coordinating with the large collective of bees, but without being controlled by a central queen bee (McMullen, 2019). Analysts predict that UAS swarms will eventually be able to assess a target, plan out a mission and execute the plan with little to no human involvement (Safi, 2019).

According to Kallenborn, the baseline of UAS swarm technology is the ability of UAS in a swarm to share information without human intervention and then make decisions based on that information (2018). This autonomous decision-making process is known as autonomy (Kallenborn, 2018). An autonomous UAS swarm makes decisions by algorithms and is described by Campion et al. (2018) as a three-step decision-making process: data, control and process. Figure 10 shows how an autonomous UAS swarm would make decisions during flight.

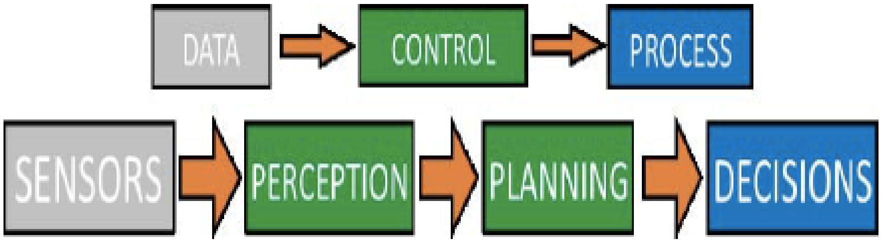


Figure 10. Decision-making process of an autonomous UAS swarm. Source: Campion et al. (2018).

The data stage of the decision-making process consists of sensors utilizing raw data, such as global positioning system (GPS), airspeed, acoustic sensors and cameras (Campion et al., 2018). The second stage of the process is control, consisting of two sub-phases: perception and planning. Perception for an autonomous system creates useable, pertinent information from unclear data that is gathered during the data stage. Planning is the portion of the control stage where the useful information collected during the perception phase is then used to make a decision about the task at hand. The last stage of the decision-making system is the process stage. This stage is when the autonomous system acts on the decisions made during the planning sub-phase (Campion et al., 2018).

2. Capabilities

The capabilities of a swarm are determined by four factors: swarm size, diversity, customization and hardening (Kallenborn, 2018). Swarm capabilities determine the types of missions and attacks they can perform. The same capabilities also determine which C-UAS methods will be effective or ineffective. Because of the survivability due to graceful degradation of large UAS swarms, they are a potential threat to conventional military forces and assets.

a. Swarm size

The size of the swarm helps determine the capabilities of the swarm. Bigger swarms are not significantly affected by the loss of a few UAS, because they can reconfigure quickly with inter-drone communications (Kallenborn, 2018). As the swarm size grows, there is an increase in the amount of information being handled. This increase in inputs can significantly impact the behaviors and decisions of the swarm, and could also mean an increase in collisions.

b. Diversity

A UAS swarm is not necessarily uniform throughout in terms of size and type of UAS. Diversity within a swarm allows for different capabilities and the performance of a variety of functions. UAS can operate and communicate across warfare areas. For example, undersea UAS can coordinate actions with aerial UAS to perform missions. When a multitude of diverse UAS join together in a swarm, their capabilities may compound and can be more effective than individual UAS (Kallenborn, 2018). UAS within a swarm may also perform different roles based on their capabilities. For example, target strikes are carried out by attack UAS and communications UAS are responsible for maintaining network connectivity within the swarm. UAS within the swarm may be different sizes in order to optimize targeting.

c. Customization

In order for the swarm to be effective, it must be customizable, flexible and adaptable to the needs of the operator. UAS can be added or removed from the swarm as needed. Being able to customize the swarm allows the operator to adjust which UAS and associated payloads are in the swarm, which determines the capabilities and missions of the UAS. An adversary can customize a swarm's capabilities to defeat C-UAS systems, making them harder to defend against. There is a concept being developed currently that shows how small groups of UAS can break off from the larger swarm in order to conduct simultaneous missions. The smaller UAS group would then rejoin the swarm when their particular mission is complete (Kallenborn, 2018).

d. Hardening

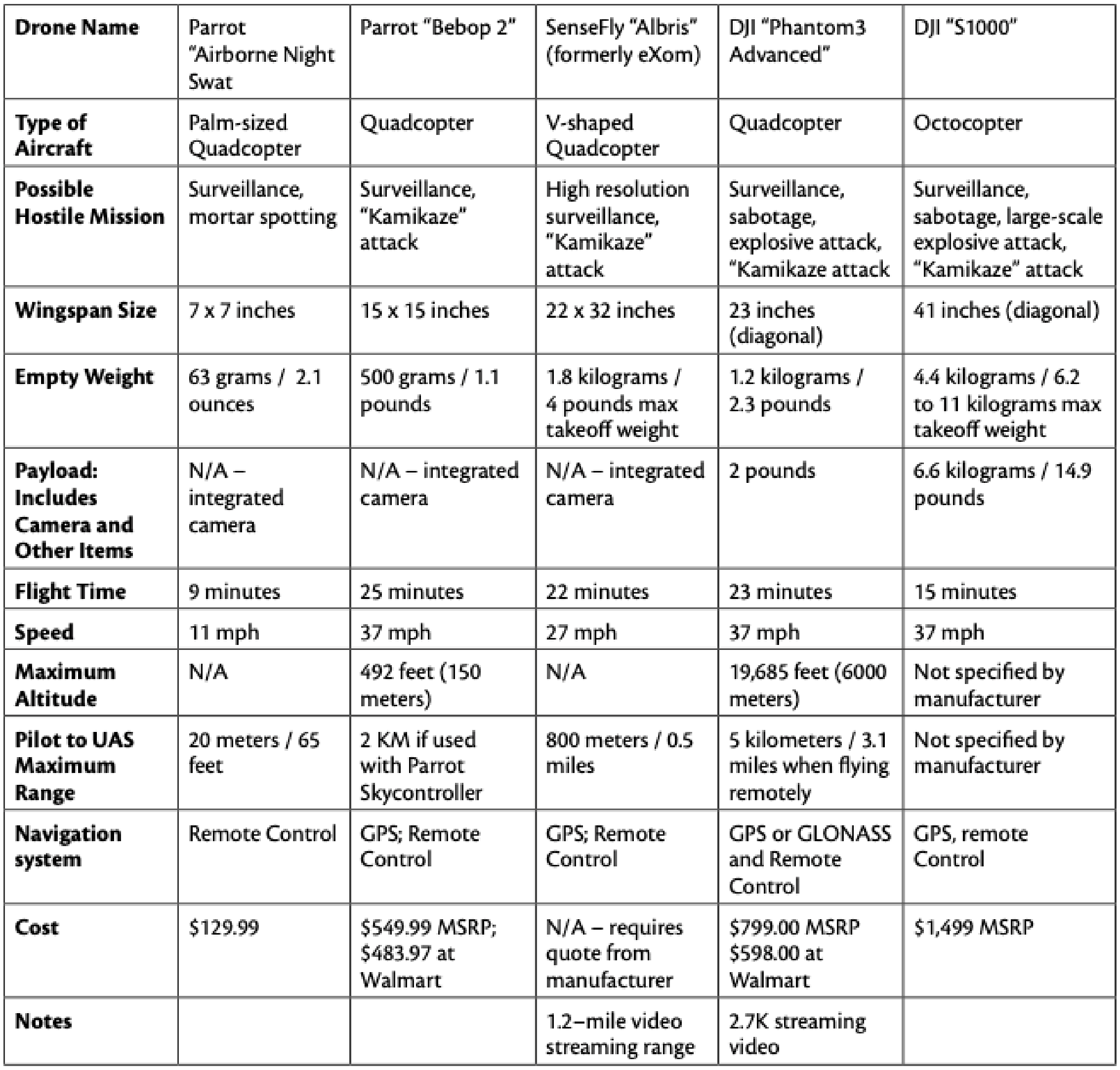
The concept of hardening refers to tools, techniques, software, hardware, etc., that is used to reduce vulnerabilities and security risks in a technology system. The biggest vulnerability to a swarm is an interruption in communications due to electronic warfare. Therefore, UAS in a swarm would need to develop a mechanism to mitigate this vulnerability, such as using environment cues vice RF frequencies for communication (Kallenborn, 2018). Kallenborn uses stigmergy, which is a mechanism of indirect communications used by swarming insects that can be applied to a UAS swarm.

E. UAS THREATS

With the low cost, accessibility and global proliferation of UAS, the potential for adversary use has increased, fueling the focus on C-UAS technologies for the military. Advances in applicable technologies have provided sUAS with an increasing ability to carry weaponized payloads, fly significant distances and use GPS for location accuracy (Palmer & Geis, 2017), making them an attractive attack platform for U.S. adversaries.

The weaponization of sUAS is a growing concern for the DOD. For as little as $129, anyone with ill intentions can purchase a UAS and outfit it with simple weapons that can cause major damage to military equipment and injure or kill personnel. These small, cheap UAS have been nicknamed "Costco drones," and have led to the U.S. military not always having the upper hand in the air in certain areas of operation (Rassoul, 2022). Table 6 is an example of a few affordable commercial sUAS that are on the consumer market today.

Table 6. Currently available commercial sUASs.
Source: Palmer and Geis (2017).



Drone Name	Parrot “Airborne Night Swat	Parrot “Bebop 2”	SenseFly “Albris” (formerly eXom)	DJI “Phantom3 Advanced”	DJI “S1000”
Type of Aircraft	Palm-sized Quadcopter	Quadcopter	V-shaped Quadcopter	Quadcopter	Octocopter
Possible Hostile Mission	Surveillance, mortar spotting	Surveillance, “Kamikaze” attack	High resolution surveillance, "Kamikaze" attack	Surveillance, sabotage, explosive attack, “Kamikaze attack	Surveillance, sabotage, large-scale explosive attack, “Kamikaze” attack
Wingspan Size	7 x 7 inches	15 x 15 inches	22 x 32 inches	23 inches (diagonal)	41 inches (diagonal)
Empty Weight	63 grams / 2.1 ounces	500 grams / 1.1 pounds	1.8 kilograms / 4 pounds max takeoff weight	1.2 kilograms / 2.3 pounds	4.4 kilograms / 6.2 to 11 kilograms max takeoff weight
Payload: Includes Camera and Other Items	N/A – integrated camera	N/A – integrated camera	N/A – integrated camera	2 pounds	6.6 kilograms / 14.9 pounds
Flight Time	9 minutes	25 minutes	22 minutes	23 minutes	15 minutes
Speed	11 mph	37 mph	27 mph	37 mph	37 mph
Maximum Altitude	N/A	492 feet (150 meters)	N/A	19,685 feet (6000 meters)	Not specified by manufacturer
Pilot to UAS Maximum Range	20 meters / 65 feet	2 KM if used with Parrot Skycontroller	800 meters / 0.5 miles	5 kilometers / 3.1 miles when flying remotely	Not specified by manufacturer
Navigation system	Remote Control	GPS; Remote Control	GPS; Remote Control	GPS or GLONASS and Remote Control	GPS, remote Control
Cost	$129.99	$549.99 MSRP; $483.97 at Walmart	N/A – requires quote from manufacturer	$799.00 MSRP $598.00 at Walmart	$1,499 MSRP
Notes			1.2–mile video streaming range	2.7K streaming video	

As early as 2014, the Islamic State of Iraq and Syria (ISIS), a terrorist group, used the DJI “Phantom3 Advanced” quadcopter to record videos of Syrian military targets (Palmer & Geis, 2017). The DJI “Phantom3 Advanced” quadcopter, costing as little as $598 at Walmart, can fly for 23 minutes at 37 mph, making it ideal for hostile surveillance in order to plan and coordinate future attacks. The DJI “S1000” is an octocopter that can only fly for 15 minutes on a single battery charge, but it can carry a payload of up to 14.9 pounds. This is the equivalent weight of six Thermite grenades. Thermite grenades burn at

4,000 degrees Fahrenheit, which is hot enough to destroy an aircraft (Palmer & Geis, 2017). UAS not only have the potential to carry a payload of explosive weapons, but they can also carry something as simple as spike strips to disable aircraft on a runway. A swarm could act in the same manner as a flock of birds, creating enough damage to an aircraft's engine or airframe in takeoff or landing mode to cause a crash. Figure 11 shows a DJI "Phantom3 Advanced" UAV with a camera that can capture imagery and video for surveillance.

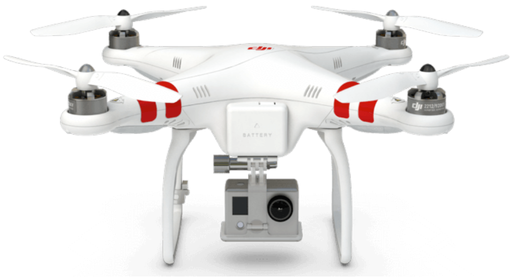


Figure 11. DJI "Phantom3 Advanced."
Source: Phantom 3 Advanced- Specs (2020).

THIS PAGE INTENTIONALLY LEFT BLANK

III. COUNTER-UAS TECHNIQUES AND LIMITATIONS

The increase in C-UAS technology development within the DOD is directly linked to the rise in threats that unmanned aircraft pose against civilians and the military. C-UAS focuses on countering not only the unmanned vehicle itself, but the components that make up the unmanned system, rendering it useless and unable to complete its mission. There are many C-UAS systems available on the market today, but there is room for C-UAS development based on certain scenarios and environments. Chapter III explores the various methods used to detect, identify, and defeat enemy UAS. The C-UAS methods referenced in this chapter are not all-inclusive, as C-UAS technologies are continuously being developed as new UAS threats emerge.

A. UAS DETECTION AND IDENTIFICATION

Unauthorized UAS can be detected through a number of different sensors: radar, passive RF signal detection, electro-optical (EO), infrared (IR), acoustic and combined sensors. Radar systems are used to detect UAS based on their radar signatures. The radar then processes the radar returns, employing algorithms to determine if the radar returns are from UAS or other objects, such as birds (Michael, 2018). Passive RF sensors use commonly known frequencies broadcast by UAV to identify their presence, and also detect wireless signals used by GCS to control UAS during flight. (Hoehn & Sayler, 2021). Algorithms then identify and locate UAS, separating their RF signatures from that of the other RF signals in the area (Michael, 2018). EO uses visual signatures and IR uses heat signatures for detection. Acoustic sensors use acoustic signatures, such as the sound of the propeller blades and the motor, to identify the presence and direction of a UAV, and in some cases to determine the make and model of a UAS. The military often utilizes a multi-layered, combined sensor technology approach for UAS detection.

Sensors used to detect unauthorized UAS have several limitations based on performance. EO and IR systems are most effective in clear, unobstructed airspace with a direct line of sight (LoS) to the target. Clouds, severe weather, and natural or man-made obstructions in the surrounding environment can degrade the ability of the systems to detect

UAS. Acoustic sensors are limited by ambient noise present in the environment that can mask the presence of a UAS until they are very near the sensor, and identification of a type signature can be made more difficult in a noisy environment. RF detection systems can likewise be affected by natural and man-made RF noise inherent in the environment, and they reference a library of commonly used UAS frequency bands for identification, requiring ambiguity resolution of the signals from those of communications systems that use the same frequencies. The acoustic and frequency band libraries must be updated routinely to keep up with the growing number of UAS entering the market. The sensitivity of detection systems can also be limiting. C-UAS detection systems must be "sensitive enough to detect all UAS operating within the area of use, but...[being] too sensitive may create an overwhelming number of false positives" (Michel, 2018, p. 6). Detection systems are also limited in their ability to determine whether a UAS is friendly or hostile, allied or adversary. This limitation can result in the misidentification of a UAS as legitimate or illegitimate.

B. INTERDICTION

The DOD has invested in a wide range of C-UAS technologies in order to ensure robustness for defense against UAS and sUAS swarms. There are two methods for the interdiction of a UAS that are analyzed in this thesis: kinetic and non-kinetic. Both methods are effective in defeating UAS and UAS swarms but each is utilized for different scenarios. The kinetic approach disables UAS with the intention of destroying or damaging the UAS, which typically will not allow for further exploitation. The non-kinetic approach refers to disabling the UAS without the use of a kinetic mechanism. An added benefit to utilizing a non-kinetic approach is the possibility of recovering the undamaged UAS to exploit for intelligence or criminal investigation purposes. Examples of the two C-UAS methods are outlined below.

1. Non-kinetic UAS

Non-kinetic C-UAS use non-destructive techniques with the added benefit of exploitation for possible military intelligence purposes. Non-kinetic C-UAS methods include RF jamming, GNSS jamming, hacking and spoofing. An overview of non-kinetic C-UAS methods are described below, along with examples and limitations.

a. Electromagnetic jamming

The most common form of interdiction is electromagnetic jamming, also known as RF jamming, with 259 systems currently using signals jamming as a C-UAS method (Michel, 2019). According to the DOD Dictionary of Military and Associated Terms, jamming is the "deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of preventing or reducing an enemy's effective use of the electromagnetic spectrum, with the intent of degrading or neutralizing the enemy's combat capability" (JCS, 2018, p. 70). Jamming interferes with the enemy's ability to receive a transmission and transfer information between the transmitter and receiver. In the case of jamming a UAS, the jamming target is the UAS receiver, as depicted in Figure 12.

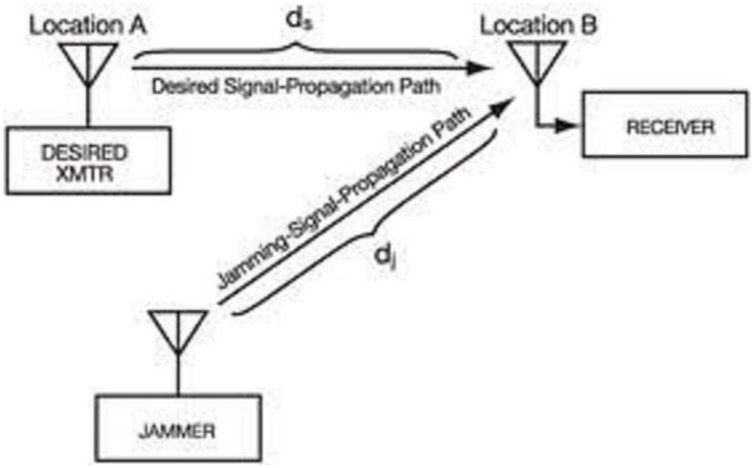

Location A
d$_s$
Location B
Desired Signal-Propagation Path
RECEIVER
DESIRED XMTR
Jamming-Signal-Propagation Path
d$_j$
JAMMER

Figure 12. UAS Jamming Geometry. Source: Nichols et al. (2018).

In June 2019, an Iranian fixed wing UAS was brought down when Marines aboard the *USS Boxer* employed a jamming technique to disrupt the UAS signal. The particular system that Marines employed was the Light Marine Air Defense Integrated System (LMADIS). LMADIS is an electronic warfare system that intercepts UAS with a combination of jamming, radars and guns. The radars and guns are commonly mounted on

Marine vehicles, such as a diesel-powered MRZR vehicle in this situation (LaGrone, 2019). Another jamming system is the anti-UAS defense system, tested during the 2017 Maneuver Fires Integrated Experiment in Oklahoma. This system has two radars to provide 360-degree coverage and one camera to identify targets (Wilson, 2018). Dedrone's DroneDefender, a 20-pound, shoulder-mounted weapon, uses jamming to disrupt communications between the UAV and operator, which renders the UAS useless (Pawlyk, 2020). Figure 13 shows MADIS mounted on a Polaris MRZR vehicle.

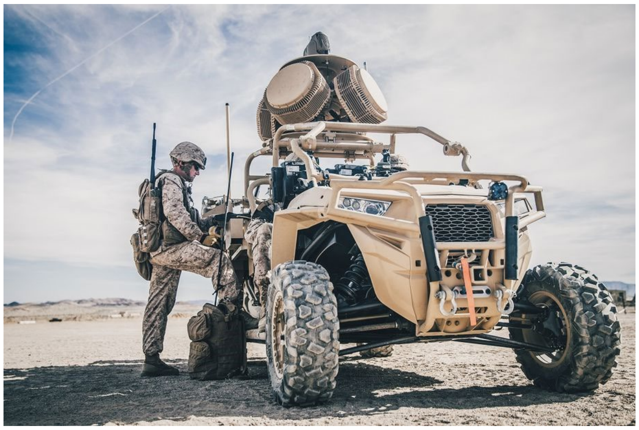


Figure 13. LMADIS mounted on Polaris MRZR Marine vehicle. Source: Liptak (2019).

Similar to the LMADIS, the Navy developed the DroneSentry-X to detect and jam radio frequency signals. It uses artificial intelligence to scan 360 degrees and uses sensors to identify and defeat incoming UAS through non-kinetic jamming (Larson, 2021). Figure 14 shows DroneSentry-X mounted onto a mobile vehicle.

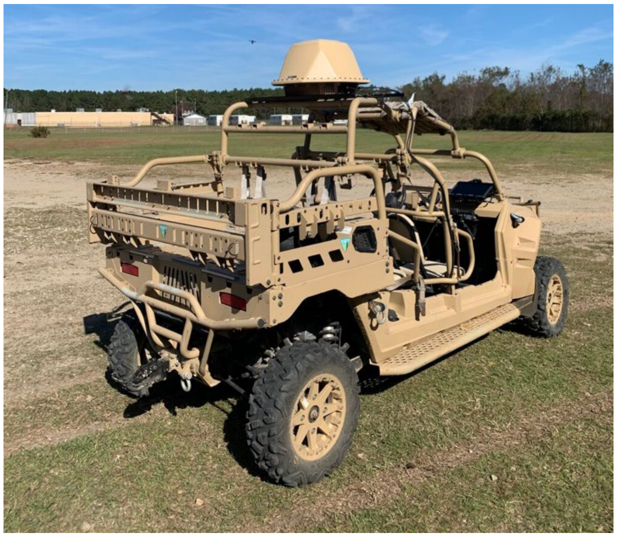


Figure 14. DroneSentry-X. Source: DroneShield (2021).

Electromagnetic jamming has several limitations. One limitation is jamming can interfere with friendly communication links utilizing the same frequencies. There have been instances where jammers have interrupted air traffic management operations (Michel, 2018), leading to the FAA banning the use of jammers at airports. Jammers also typically require the target receiver to be located within LoS of the jammer. Because the GCS is not usually within LoS of the jammer, the GCS is typically a target. According to Michel, some UAS are capable of operating without an RF link, making RF jamming a useless countermeasure to defend against those UAS (Michel, 2019).

b. Global Navigation Satellite System (GNSS) jamming

GNSS is a satellite navigation system used by sensors onboard UAS to guide the UAS on a flight path to its destination. When flying autonomously without a human operator, GNSS enables the UAS to reliably navigate. UAS use GNSS to perform aerial mapping for terrain surveys, traffic monitoring, disaster monitoring, among other applications. GNSS jammers mitigate the hostile use of UAS with GNSS sensors onboard by affecting the signal-to-noise ratio (SNR) of the signals being received. When the signal becomes too weak, the ranging measurements cannot be generated, causing signal deterioration or a “total loss of lock of the GNSS signals...and the position solution cannot be computed” (Pokrajac et al., 2018). Figure 15 shows the five steps involved in the GNSS concept. GNSS jamming affects the third step in Figure 15, which prevents steps four and five from occurring.

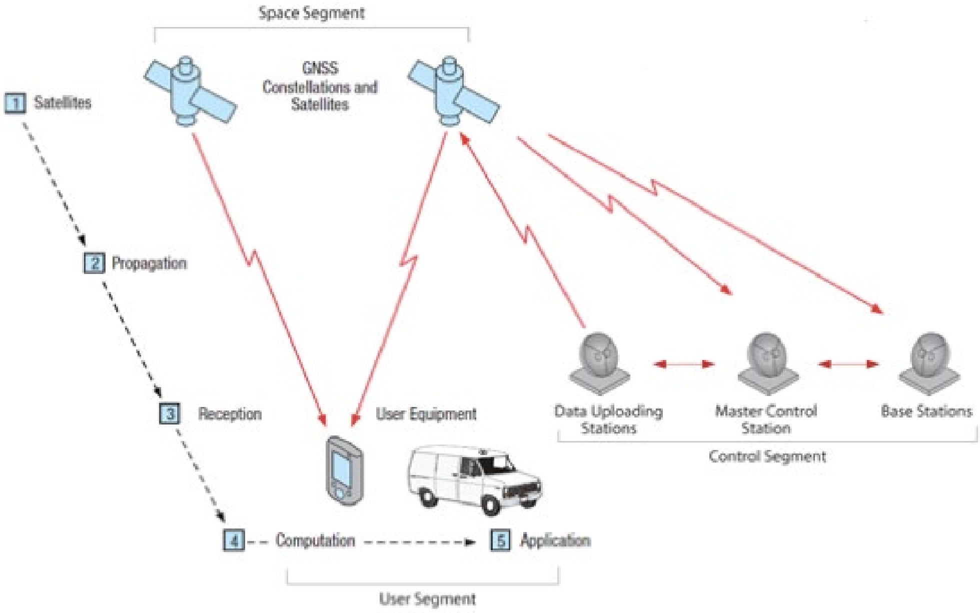


Figure 15. Basic concept of GNSS. Source: Pokrajac et al. (2018).

The physical location of GNSS antennas on the UAS can be a limitation. Its location on the UAS can cause interference if the GNSS antenna is placed close to the electronic systems, causing electromagnetic compatibility problems (Wilde et al., n.d.).

c. Hacking

UAS hacking involves infiltrating the UAS with malware in order to take control and physically redirect the UAS, similar to hacking in laptops and computers. Hacking into a UAS requires a connection to either the remote controller or interception of the signal.

An early example of UAS hacking is the Skyjack Project. Skyjack is a UAS platform that is able to disconnect a UAV from its ground station controller wirelessly and then redirect the UAS to perform commands from the Skyjack platform (Fisher, 2013). Specifically, the Skyjack UAS utilizes a wireless key cracking application to take over control of the target UAS without having to exploit a security vulnerability. Parrot AR

UAS is an example of using one UAS to hack another. The Parrot AR UAS acts as a slave UAS and uses WiFi Pineapple to act as the master to create a fake terminal on SSH sessions. As commands are "entered in the master device it will be executed in the slave device, making it completely under the control of the WiFi Pineapple device" (Vattapparamban et al., 2016, p. 220).

Adversaries can easily prevent hacking. For example, anti-virus is an effective tool to prevent hacking, because it allows the ground controller to operate in a virus-free environment. The UAS can also be connected through a virtual private network, which encrypts the connection from the operator and the internet, and allows the UAS operator's internet usage to remain anonymous. UAS protected with a sel4 kernel are currently in development, which prevents the entire system from being compromised and makes the UAS resistant to hacking (Corrigan, 2020).

d. Spoofing

Spoofing, also known as protocol manipulation, involves remotely interfering with UAS and inputting false information. The spoofer is able to confuse the UAS into thinking the spoofer's signal is legitimate, allowing the spoofer to take over the UAS flight and also download the UAS data (Friedberg, 2019).

For example, MalDrone is a malware strain that is specifically aimed to spoof the connection link between the UAV and controller and control the UAS navigation. Commercial GPS signals are easily spoofed because they are unencrypted. Fake GPS coordinates are then transmitted to the UAS control system (Vattapparamban et al., 2016). Figure 16 is an example of GPS spoofing where the path of the UAS is replaced with a spoofed trajectory.

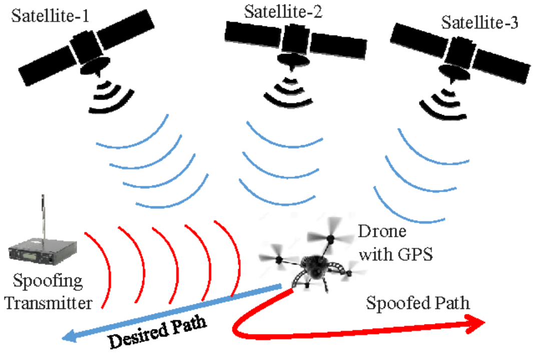


Figure 16. GPS spoofing example. Source: Vattapparamban et al. (2016).

Spoofing has its limitations as a C-UAS method. The main limitation is that it is not effective against all UAS. Some UAS have the ability to resist spoofing attacks by protecting or encrypting the communications links. Spoofing systems are also complex and often hard to implement as a C-UAS measure (Michel, 2019). Many UAS on the market today are outfitted with accelerometers and gyroscopes as an alternative to GPS, which makes GPS spoofing an ineffective C-UAS tactic.

2. Kinetic C-UAS

Kinetic C-UAS focuses on damaging or disabling a UAS to render it non-operational. Gathering information for intelligence purposes is not always possible due to the damage that kinetic C-UAS can inflict on enemy UAS. Kinetic methods include: munitions, nets, birds of prey, lasers, non-nuclear electromagnetic pulse (NNEMP), high-power microwave (HPM) and swarm-on-swarm. An overview and examples of kinetic C-UAS methods are described below.

a. Munitions

Munitions are a C-UAS technique that involves ammunition and a weapons system. These weapons systems are typically used for defense against cruise missiles, rockets, and artillery, but are also being utilized to defend against unmanned vehicles.

Munitions range from small ammunition to rockets to missiles. The Army has been testing the Enhanced Area Protection and Survivability System (EAPS) that fires 50-millimeter munitions up to 1 kilometer away. Figure 17 shows EAPS sending the UAS flight path corrections and then exploding the munition at the range that causes the most damage to the UAS.

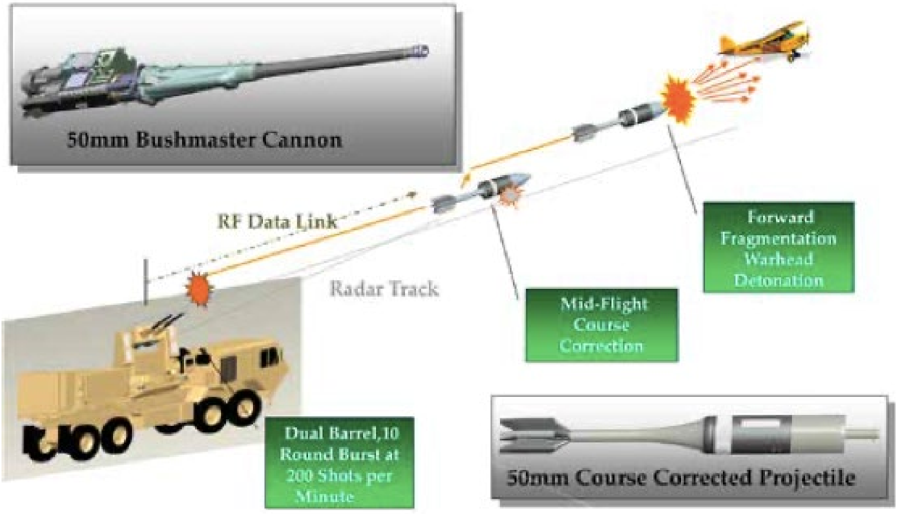

50mm Bushmaster Cannon
RF Data Link
Radar Track
Forward Fragmentation Warhead Detonation
Mid-Flight Course Correction
Dual Barrel,10 Round Burst at 200 Shots per Minute
50mm Course Corrected Projectile

Figure 17. EAPS. Source: Palmer and Geis (2017).

During Operation IRAQI FREEDOM/ENDURING FREEDOM Northrup Grumman developed a Counter Rocket, Artillery, and Mortar (C-RAM) system that employs a Gatling gun that fires up to 4,500 20-millimeter rounds per minute at rocket, artillery or mortar threats at a range up to 1.2 kilometers. The system has been configured to be radar-aimed in order to counter unmanned threats (Palmer & Geis, 2017). Raytheon Technologies has built a missile defense system called the Iron Dome, which consists of the Tamir interceptor and launcher and the SkyHunter missile. This weapons system was developed to counter cruise missiles and other threats, such as enemy UAS and munitions (Judson, 2020). Figure 18 shows an Army C-RAM System firing 20-millimeter rounds.

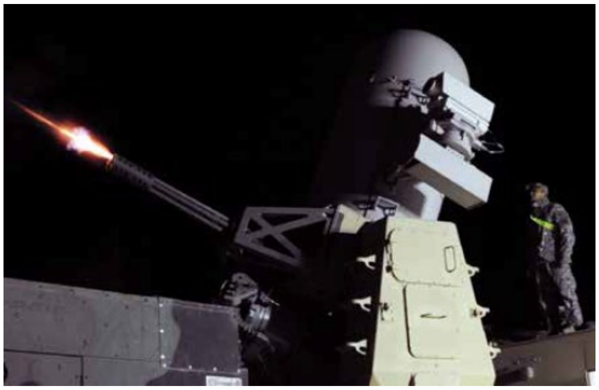


Figure 18. Army C-RAM System. Source: Palmer and Geis (2017).

A failure of a gun to fire correctly, also known as misfire, is a disadvantage to using munitions as a defense mechanism. Because of the possibility of collateral damage, there would be certain environments where munitions would not be an effective countermeasure for UAS, such as the largely populated San Diego harbor.

b. Nets

Nets are a simple, kinetic C-UAS method that safely trap and remove unauthorized UAS from the airspace. Nets can be deployed from a UAS or from the ground. The captured UAS can either be brought to the ground immediately or carried to a secure location for further exploitation and intelligence gathering.

An example of C-UAS nets is Delft Dynamic’s product, the DroneCatcher. DroneCatcher is a multicopter, also known as a multirotor UAS, that is armed with a net gun range of up to 20 meters that deploys after sensors onboard locate the target UAS. The DroneCatcher either carries the captured enemy UAS to a predetermined location or releases a parachute to harmlessly guide it to the ground (Delft Dynamics, 2019). The future of C-UAS net technology includes AI-enabled UAS that target hostile UAS and deploy nets, also known as Drone Hunter. Figure 19 shows an unauthorized UAS being captured in a net trap by Tokyo’s Metropolitan Police Department.

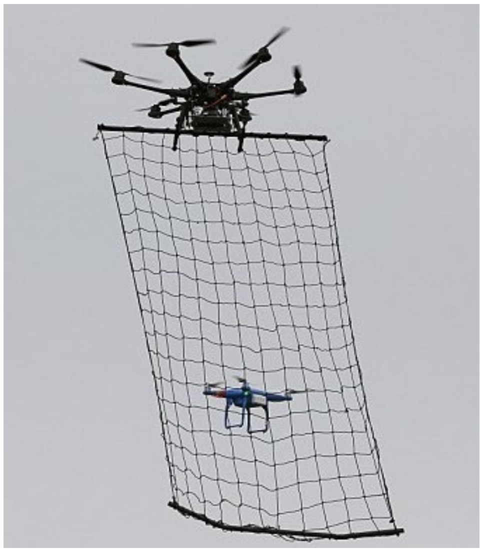


Figure 19. Net trap. Source: Liberatore (2015).

Net-based C-UAS methods, although effective, can be hazardous in certain situations and environments. When a UAS is caught in a net equipped with a parachute, the entangled UAS falls to the ground. There is a risk that the parachute does not deploy correctly or the UAS net capture occurs at a low altitude. Using nets to stop UAS mid-flight can result in damage to infrastructure and poses a danger to populations on the ground.

c. Birds of prey

Utilizing trained birds of prey, such as falcons and eagles, is considered one of the most cost-effective C-UAS solutions. The large birds are trained to intercept hostile UASs during flight. According to Singh, birds are able to intercept approximately 95 percent of the UAS they are sent to capture, a higher success rate than some of the more damaging, costly kinetic C-UAS methods (2018). Guard From Above, a Dutch company in the Netherlands, describes falcons as “a low-tech solution for a high-tech problem” (Nikolic, 2017, p. 153). Trained birds of prey can fly at speeds upward of 75 miles per hour and have talons powerful enough to penetrate through bone.

Since 2016, Scotland Metropolitan Police have used trained eagles to capture suspicious UASs and transport them to safe areas (Vattapparamban et al., 2016). ‘Guard

From Above' claims to be the first company in the world to have trained and used birds of prey to intercept hostile UAS. This company has successfully incorporated C-UAS birds into the Dutch National Guard, and provides training for birds and bird handlers for law enforcement and military clients worldwide. Figure 20 shows how birds of prey can physically capture a UAV.

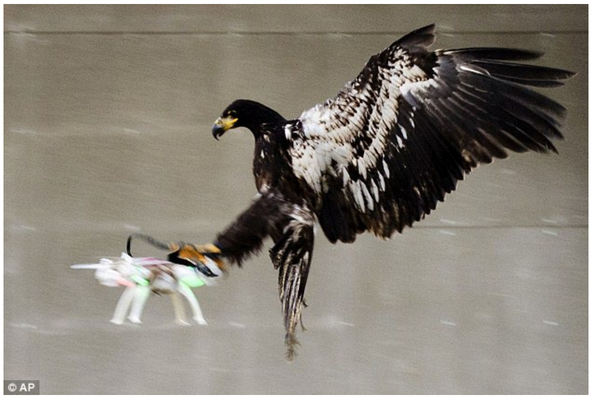


Figure 20. Birds of prey used to capture a UAV. Source: Witherow (2016).

Animal safety is the main limitation of using birds of prey for C-UAS. Rotating UAS blades could potentially harm or kill trained birds. Another concern is that these birds are being trained to hunt for objects outside of their normal diet, making this very unnatural. Human interference with birds that were endangered not so long ago is also a concern. Falconry is unlikely to advance from the urban environment to use in an operational environment due to the safety limitations.

d. Lasers

Laser weapons systems provide precision targeting of sUAS through the use of a highly directional high-intensity light beam. The intent of lasers is to cause physical damage or destroy the sUAS itself with a large amount of electromagnetic energy focused into a narrow beam. Laser weapons systems are primarily used by the military to target sUAS during flight, and not likely to be used against the GCS or operator on the ground.

The Air Force has been field testing the High-Energy Laser Weapon System (HELWS) since August 2020, a system designed to neutralize UAS within seconds (Hoehn & Sayler, 2021). The Navy tested the only operational directed energy weapon in 2014, the Laser Weapon System (LaWS) (Hoehn & Sayler, 2021). Lockheed Martin is currently testing prototypes of the Advanced Test High Energy Asset system (ATHENA), which is a laser system used to defend against and defeat threats such as UAS. ATHENA uses a 30-kilowatt spectral beam along with a fiber beam to provide one powerful, high-quality laser beam to destroy low-value targets, such as a swarm of inexpensive sUAS (Lockheed Martin, 2020). Boeing's Compact Laser Weapon System (CLWS) is small weapons system, weighing about 650 pounds, but can destroy targets up to 22 miles away with a 10-kilowatt energy beam. Figure 21 shows High Energy Laser with Integrated Optical-dazzler and Surveillance (HELIOS), a laser weapons systems currently in development, onboard a USN warship.

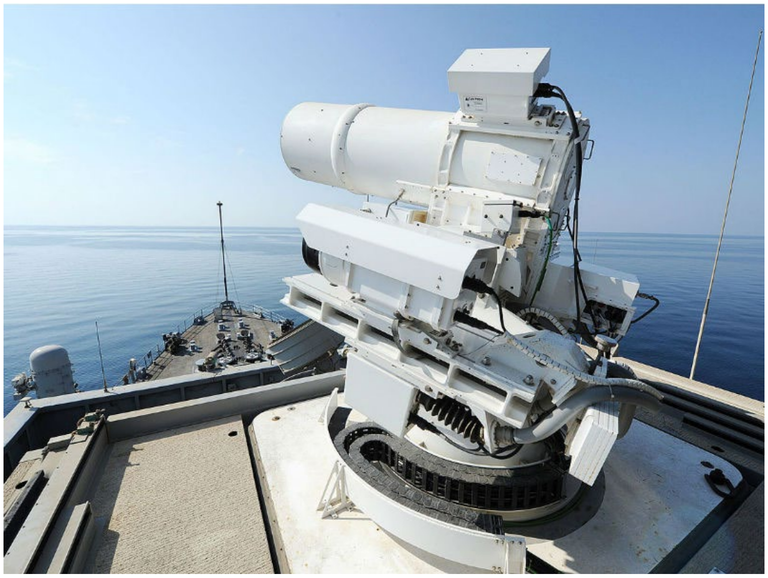


Figure 21. HELIOS, a Navy laser weapons system in development.
Source: Husseini (2019).

Laser weapons systems are fraught with challenges. Although a laser's aim is extremely accurate and discrete, lasers pose a threat to aircraft in the vicinity of the targeted UAS or swarm. Electromagnetic interference (EMI) is a small concern when utilizing lasers onboard a ship, because EMI has the potential to disrupt other electrical systems or sensors onboard the ship (Pappalardo, 2013). Depending on the power of the laser and the capabilities of the technology or system being used, the time required to lock onto and destroy a quickly moving sUAS swarm may make a laser system less suitable as a C-UAS method. Weather has a tremendous effect on the effectiveness of a laser. If there is precipitation, as there often is on the deck of a naval ship, the quality of the beam is diminished (Pappalardo, 2013).

e. Non-Nuclear Electromagnetic pulse (NNEMP)/High Power Microwave (HPM) weapons

Nuclear electromagnetic pulses (EMP) were originally discovered during the Cold War as a result of the detonation of nuclear weapons, but the damage was so widespread that the U.S. explored ways to use EMP in a non-nuclear capacity. NNEMP was developed to fill the need for a non-nuclear EMP option. NNEMP weapons have the ability to disrupt, deny and degrade the enemy's ability to use electronic equipment and damages critical infrastructure through bursts of EM energy. NNEMP weapons are highly destructive to UAS, because they destroy the electrical components and navigational sensors onboard. Similar to NNEMP, HPM uses directed energy in the form of RF or microwaves to disable electrical components and disrupt the electrical flow of UAS and UAS swarms.

Northrup Grumman Corporation formed an agreement with Epirus, Inc to incorporate Epirus' C-UAS EMP weapons system, Leonidas, into their C-UAS portfolio. Leonidas uses "solid-state commercial semiconductor technology to deliver capability with unprecedented reduction in size and weight" (Slayen, 2020, para. 4). It uses precision-focused EMP beams to incapacitate UAS, but the beam can be adjusted to tackle a large area, similar to a force field. Leonidas' C-UAS capabilities can be effective against an entire UAS swarm.

Raytheon's Phaser is an HPM system that focuses "a wide, arching energy beam on UAS that sends out a burst of EM energy, destroying their electronics and dropping them simultaneously" (Raytheon Technologies, 2020, para. 1). Phaser can disable UAS that weigh up to 55 pounds, approximately the size of the ScanEagle. A photo of Phaser is seen in Figure 22.

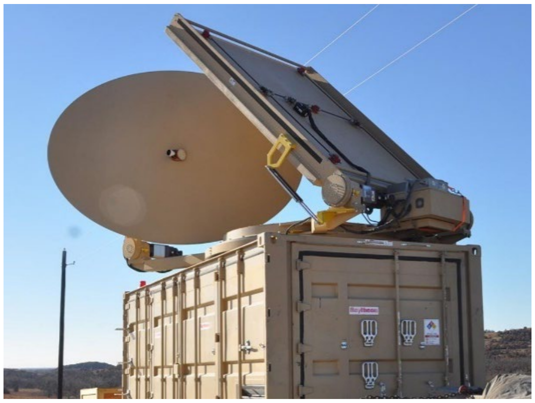


Figure 22. Phaser HPM system. Source: Raytheon Technologies (2020).

Tactical High Power Operational Responder (THOR) is similar in appearance to Phaser, but THOR was specifically developed for airbase defense as an electromagnetic weapon to engage multiple targets, such as UAS swarms. The Air Force Research Laboratory is developing a new weapon named Mjölnir, which is built on the technology of THOR but with improvements (Losey, 2022). Figure 23 is a photo of THOR.

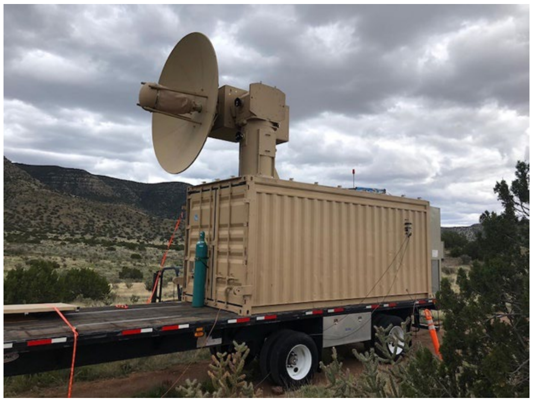


Figure 23. THOR. Source: Ripple (2019).

Although not threatening to human life, the limitations of NNEMP and HPM weapons lies in the unintended collateral damage that can occur. The effects on the population and equipment surrounding targeted UAS can be devastating, from disabling satellites to "destroying everything from a single smart phone to an entire continent's critical infrastructure, permanently and without possibility of repair" (Wilson, 2019, Under "EMP weapons," para. 3). Also, NNEMP and HPM weapons can be ineffective if the target is utilizing a Faraday cage. Faraday cages act as a shield to block EM fields, and are effective for protecting connected devices, such as a UAS or UAS swarm, against NNEMP attacks (English, 2019).

f. Swarm-on-swarm

Swarm-on-swarm warfare tactics is a newer method to counter hostile UAS swarms. A swarm of friendly UAS work together to target and track the enemy swarm, communicating data about the target swarm through wireless communications within the swarm. The swarm then maneuvers together to intercept and destroy the enemy swarm. The Pulse Newsletter summarizes swarm-on-swarm tactics and techniques as engaging "[numerous] aggressive combatants simultaneously" (TechLink, 2020, Under "Benefits").

Naval Postgraduate School's Consortium for Robotics and Unmanned Systems Education and Research (CRUSAR) coined the term xSwarm to describe massive UAS swarms under external control. Due to the exponential expansion of swarm technologies, CRUSAR is researching new tools to engage and counter xSwarms, such as aerial dogfights. In 2017, CRUSAR executed an aerial dogfight experiment at Camp Roberts in Monterey, California. The CRUSAR experiment demonstrated a collaborative autonomy amongst a UAS swarm to counter another UAS swarm through successful algorithms (Fox News, 2017). Figure 24 shows UAS maneuvering into a self-determined formation during the NPS experimentation at Camp Roberts. Also, the Navy has developed an airborne system to counter UAS swarms by dropping UAS from the air in canisters to intercept the hostile swarm with functioning maneuverability.

Figure 24. UAS moving into formation during Camp Roberts experiment. Source: Chagoya (2017).

Because C-UAS swarms are a new concept, the full range of challenges have not been experienced. However, it can be assumed that a future challenge will be to increase the size of the swarms from a few to 50 or more. New limitations and challenges will arise when the swarm-on-swarm C-UAS method is put to the test in various operational environments.

C. EXISTING DDG C-UAS SYSTEMS

The USN uses Northrup Grumman's Drone Restricted Access Using Known EW (DRAKE) to counter Group 1 UAS, those weighing less than 20 pounds. DRAKE repurposes a "mature counter-improvised explosive device technology" (Ball, M., 2016, para. 4) into a non-kinetic negation system that uses radio frequencies. Because DRAKE can counter hostile Group 1 UAS, it would be ideal for mitigating sUAS swarms in appropriate environments.

The MK MOD 0, also known as the Laser Weapon System Demonstrator (LWSD), is currently the most powerful laser outfitted onto a USN warship, the USS *Portland.* In a Popular Mechanics article, Mizokami states the LWSD is more destructive than the 30-kilowatt LaWS and has an output of up to 150-kilowatts, powerful enough to defend against the threat of rockets, artillery, mortars and especially UAS (2020). There is not much known about LWSD yet, such as its target range or potential for collateral damage.

In February 2020, the Navy installed an Optical Dazzling Indicator (ODIN), a C-UAS system that can track, identify and deny commercial UAS. ODIN is able to take control of the UAS, returning it to its operator or forcing the UAS to land (Phelps, 2018), while maintaining minimal risk for collateral damage. Mizokami writes that HELIOS, the 60- kilowatt laser system, is designed to shoot down UAS but can also prevent a UAS from performing its ISR mission by rendering its EO sensors useless (2019).

USN warships already utilize two weapons systems that can be used to defend against and destroy UAV threats: the MK 15 Phalanx Close-In Weapon System (CIWS) and RIM-116 Rolling Airframe Missile (RAM). Phalanx CIWS is described as a "fast-action, detect-through-engage, radar guided, 20-millimeter gun weapon system" (Office of Corporate Communication [OCC], 2021, Under "Description"), according to the Navy's official website. CIWS can autonomously detect, track, engage and eliminate enemy UAS with Armor-piercing discarding sabot (APDS) for longer range and optimized performance. RAM is known as a supersonic fire-and-forget, ship self-defense missile used to counter asymmetric air and surface threats (OCC, 2021).

The Naval Surface Warfare Center Dahlgren Division (NSWDD) developed a water method to defend warships against air attacks called the Water Barrier Ship Self Defense Concept. Although this method was not specifically designed to defend against UAS attacks, the Water Barrier Ship Self Defense Concept is a wall of water that can be used as an inexpensive and effective defense against low-flying threats such as UAS and UAS swarms (Higdon, 2000). The wall of water concept will protect the ship from debris from the destroyed target, unlike the CIWS which has the potential to cause severe target damage to the warship as debris from a damaged or destroyed UAS may still impact the ship.

Future Navy C-UAS plans include Counter-Remote Control Model Aircraft Integrated Air Defense Network (CORIAN). The capabilities that CORIAN provides are the detection, identification, tracking and mitigation of hostile UAS threats. CORIAN neutralizes sUAS threats with minimal fratricide to the RF spectrum and communications surrounding the target (CACI International Inc. [CACI], 2020). In October 2021, CACI International Inc. debuted CORIAN 2.0, a system intended to defend against "multiple, simultaneous threats from standoff distances and easily integrate with other systems, including command and control systems such as forward area air defense command and control" (CACI, 2021, para. 2).

D. CHALLENGES IN CURRENT C-UAS METHODS

The explosive growth of C-UAS technology is directly related to the increase in hostile uses of UAS. Based on the 2018 research report "Counter-UAV Systems," there are over 235 publicly-known C-UAS products sold by 155 different companies from 33 different countries (Michel, 2018). Despite the effectiveness in mitigating sUAS threats, each of these C-UAS systems have limitations and unintended consequences, and there is no perfect C-UAS system.

According to Michel, there is no interdiction system that is completely effective, and the advancement of UAS technology is continually moving forward (2018). Therefore, the C-UAS market will constantly need to develop new counter methods in an effort to keep up with the expanding UAS market. C-UAS technology must adapt to a growing number of targets, such as "large unmanned aircraft capable of carrying heavy payloads through to low-flying micro surveillance UAS that might only weigh a few grams" (Michel, 2018, p. 7). The future may see UAS specifically designed to counter the current C-UAS systems because C-UAS will likely be one step behind UAS development. For example, UAS may be designed to maneuver quietly in order to evade acoustic sensors, reduce radar signature to avoid detection, or use shielding to protect UAS from direct energy attacks.

E. SCOPE FOR THIS THESIS

Chapter II defined UAS swarm technology and the implications of the hostile use of UAS. UAS capabilities, vulnerabilities and classifications were highlighted, along with C2 methods in order to provide context for the introduction of C-UAS techniques in Chapter III. Although each C-UAS technique described in Chapter III can be used collectively to combat the enemy, it is evident from the additional information gathered that there are inherent limitations in current C-UAS methods. The current DDG C-UAS systems are ineffective in certain scenarios, such as the domestic environment of the San

Diego Harbor. Chapter IV will explore a mitigation technique using water that will be applicable to defending against enemy sUAS swarms in the San Diego Harbor. Chapter V concludes the thesis with future recommendations for furthering the research of water mitigation techniques.

IV. WATER MITIGATION STRATEGY

This chapter describes the feasibility of developing a successful, non-kinetic water mitigation strategy to defend against potential sUAS swarms. The scenario for this strategy will take place in the context of the San Diego Harbor where USN assets can leverage the existing firefighting and counter-piracy technologies of the USCG, San Diego fireboats and ECO tugboats in the event of a swarm attack. The following sections will describe the mitigation parameters, which includes the vehicles and their water capabilities, as well as describes the scenario and network integration needed to make the water mitigation strategy successful.

Water can be useful in countering UAS in multiple ways. First, impact with a water stream can physically knock some smaller commercial UAVs out of the sky. Some commercial UAVs would also be rendered inoperable through exposure of their electronics to water. Although this would not cause the vehicle to crash, it would still kill the mission for the UAV. A second impact is that surrounding a moving warship in a cloud of water makes targeting more difficult. If the UAV is using an onboard camera, it can essentially be blinded by the water cloud. If the UAV is being remotely operated, the remote operator may no longer be able to see specific target points on the vessel under attack. Finally, firefighting, washdown, and anti-piracy applications of water in the maritime environment means that such systems are already available and crews know how to employ them effectively.

A. MITIGATION PARAMETERS

1. Vehicles

The following section describes the physical characteristics of the vehicles available for a water mitigation strategy in the San Diego Harbor.

a. Tugboats

Six ECO tractor tugs, also known as C-tractors, are under long-term contract with the USN in the San Diego Harbor. During escort in and out of the harbor, the tugboats are directed by the pilots onboard the USN ships. Figure 25 is a photo of the ECO tugboats that are in use in the San Diego Harbor.

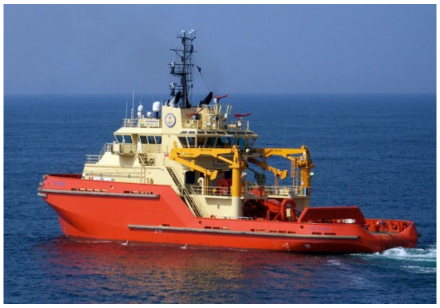


Figure 25. ECO tractor tug. Source: Edison Chouest (2018).

Each 90-foot tug is operated by a Tugboat Captain, a mariner trained by the USCG. The ECO tugboats operate under the direction of and can be dispatched by the USN, per the government contract. For example, the ECO tugboats were directed to respond as waterline firefighting support to the USS Bonhomme Richard fire in 2020 to help keep the hull of the ship cool for firefighters inside the ship, as seen in Figure 26.

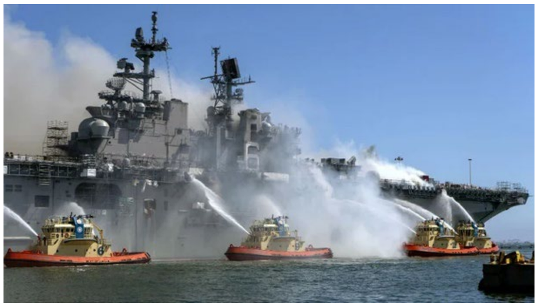


Figure 26. ECO tugboats assisting the USN during the USS Bonhomme Richard fire. Source: Mitchell (2020).

The tugboats escort USN ships as they enter and exit the harbor. With pre-planning and alteration of the government contract, ECO tugs could be directed to assist USN ships, such as a DDG, in a water mitigation strategy to defend against potential drone swarms.

Tugboats are listed as part of the marine craft available in the San Diego Harbor with firefighting capabilities (DON, 2012).

b. Fireboats

There are four fireboats available through the San Diego Port Authority that are able to aid the USN in fighting fires (MetalCraft Marine, 2021), as well as potentially assisting in shooting down sUAS swarms with seawater. The SDHP are a law enforcement entity and also trained marine firefighters. The crew is not USCG-certified. However, they receive "in-service field training [and] a 120-hour Department of Boating and Waterways marine firefighting course" (Ockerhausen et al., 2003, p. 21 footnote). The SDHP has five MetalCraft Firestorm 36 High-Speed Aluminum Fireboats in commission (MetalCraft Marine, 2021). Each fireboat is 39 feet 2 inches in length with maximum speeds of 38 knots. Figure 27 shows two SDHP fireboats docked in the San Diego Harbor.

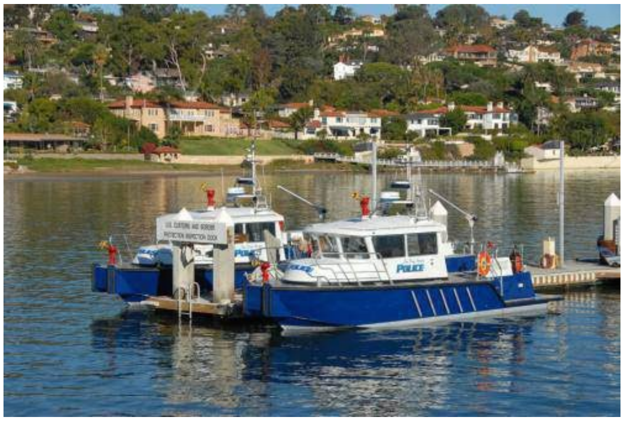


Figure 27. SDHP fireboats. Source: MetalCraft Marine (2021).

c. USCG

USCG Cutter (USCGC) *Petrel*, hull number WPB-87350, is a patrol boat in the Marine-Protector class homeported in the San Diego Harbor. The *USCGC Petrel* is 87 feet in length with a maximum speed of 25 knots (Department of Homeland Security [DHS], 2015). Figure 28 is a photo of the *USCGC Petrel.*

Figure 28. USCGC Petrel in the San Diego Harbor. Source: Flynn (2014).

2. Water Capabilities

The following section describes the water capabilities of the vehicles available for a water mitigation strategy in the San Diego Harbor.

a. Tugboats

Each ECO tugboat has two fire monitors onboard with an output of 3500 gallons per minute (GPM) and 360-degree coverage. Each fire monitor has a dedicated pump that couples to the generator that pumps an unlimited amount of sea water onto fires. Monitors can have their streams manually adjusted, from a thin stream for minimal, direct coverage to a fog-like output for maximum coverage. Figure 29 is a display of the water pumping capabilities of the ECO Tugboats.

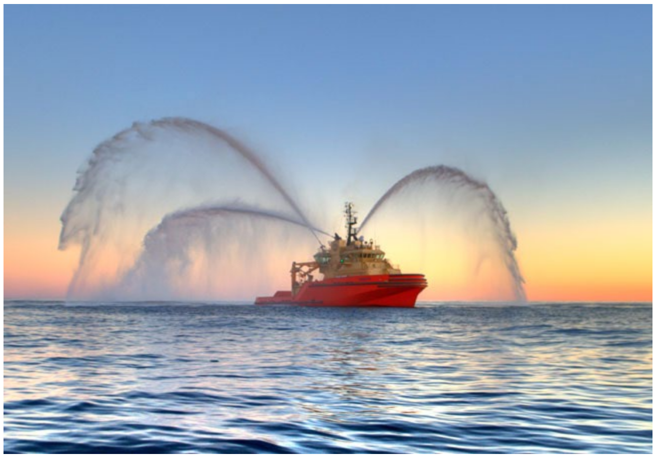


Figure 29. ECO Tugboat showcasing its fire monitor capabilities. Source: Mitchell (2020).

Figure 30 shows how the ECO tugboats escort USN warships to ensure safe passage through the harbor. The tugboats prevent grounding and collision with other vessels in the area. Although tugboats typically use their water cannons as a display to signal the ship's homecoming, these same water cannons can potentially be used the protect the ship from sUAS swarms.

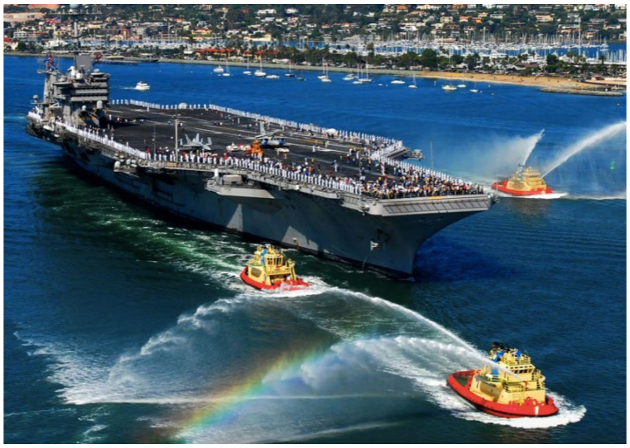


Figure 30. ECO tugboats escorting a USN aircraft carrier in the San Diego Harbor. Source: Mitchell (2020).

b. Fireboats

Each of the SDHP Firestorm 36 High-Speed Aluminum Fireboats are equipped with three Elkhart Master Stream standard water cannons for increased firefighting capabilities. The pumping capacity of each water cannon is approximately 1,750 GPM due to "a unique MetalCraft Marine proprietary designed sea chest" (MetalCraft Marine, 2021, Under "Fire Systems," para. 2). The large intake of water through the sea chest allows for a higher pumping capacity. The water cannons are located on top of the cabin, on the bow and in the aft of the boat, as seen in Figure 31.

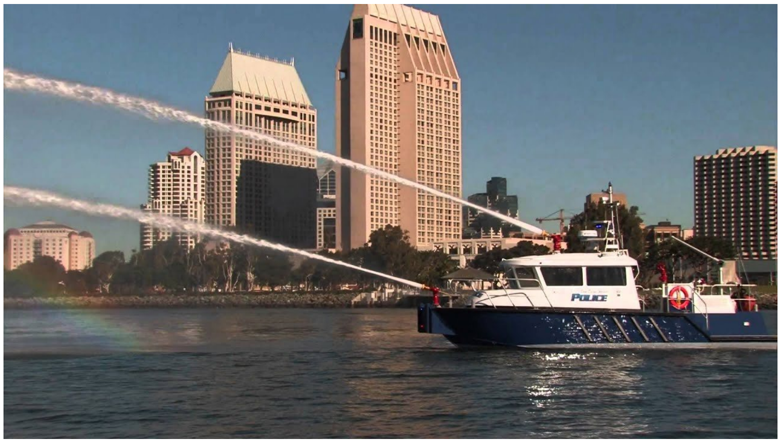


Figure 31. SDHP showing water cannon capabilities. Source: Port of San Diego (2012).

c. USCG

Currently, the *USCGC Petrel* does not have fire monitors onboard. However, the next section on network integration will highlight their role in communications for a UAS swarm mitigation strategy.

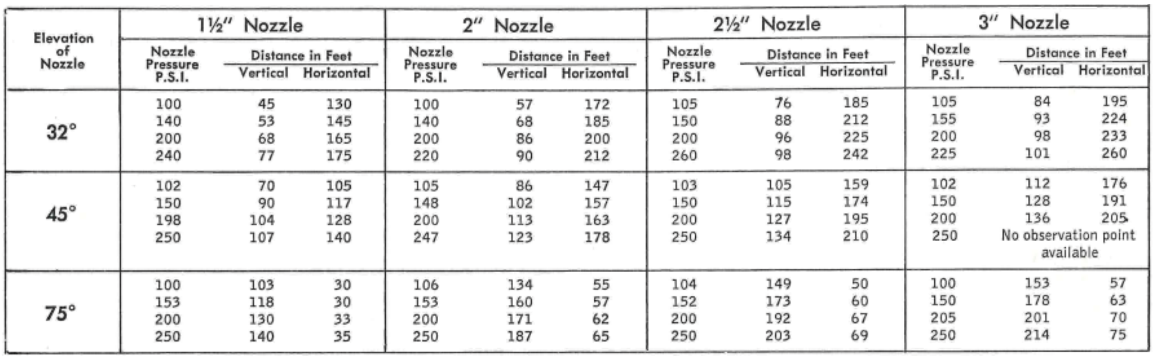
d. DDG

The firefighting capabilities of DDGs are listed in the COMNAVSURFPAC/ COMNAVSURFLANT Instruction 3504.1B (CNSP/CNSLINST 3504.1), referenced in the Joint Fleet Maintenance Manual (JFMM). This instruction identifies redline systems and "minimum equipment lists by ship class" (DON, 2012, p. 7). In order to be considered mission ready and deployable, each DDG must have at least three of six fire pumps in working order and functioning effectively (DON, 2012). All exterior hoses of a DDG are rated at 125 GPM for the 1.5-inch nozzles and 250 GPM for the 2.5-inch nozzles. The pumps are Elkhart, the nozzles are Elkhart brass and the hoses are generic. Figure 32 shows Sailors practicing using a fire hose during training aboard a DDG.

Figure 32. Fire hose practice using an Elkhart pump. Source: Keown (2019).

According to Elkhart, a water stream coming out of a 250 GPM fire hose with a 2.5-inch nozzle can effectively reach up to 203 feet in a vertical direction and 69 feet in a horizontal direction at a 75-degree angle. Table 7 depicts the effective reach of water streams for each nozzle size.

Table 7. Effective reach of water streams. Source: Elkhart (2021).



Elevation of Nozzle	1½″ Nozzle			2″ Nozzle			2½″ Nozzle			3″ Nozzle		
	Nozzle Pressure P.S.I.	Distance in Feet		Nozzle Pressure P.S.I.	Distance in Feet		Nozzle Pressure P.S.I.	Distance in Feet		Nozzle Pressure P.S.I.	Distance in Feet	
		Vertical	Horizontal		Vertical	Horizontal		Vertical	Horizontal		Vertical	Horizontal
32°	100	45	130	100	57	172	105	76	185	105	84	195
	140	53	145	140	68	185	150	88	212	155	93	224
	200	68	165	200	86	200	200	96	225	200	98	233
	240	77	175	220	90	212	260	98	242	225	101	260
45°	102	70	105	105	86	147	103	105	159	102	112	176
	150	90	117	148	102	157	150	115	174	150	128	191
	198	104	128	200	113	163	200	127	195	200	136	205
	250	107	140	247	123	178	250	134	210	250	No observation point available	
75°	100	103	30	106	134	55	104	149	50	100	153	57
	153	118	30	153	160	57	152	173	60	150	178	63
	200	130	33	200	171	62	200	192	67	205	201	70
	250	140	35	250	187	65	250	203	69	250	214	75

The Navy has developed the High Pressure Water Mist Fire Fighting Pump (WMFFP), a next generation fire-fighting system that is being used on multiple LHDs and the USS Zumwalt, a DDG 1000 Zumwalt Class multi-mission surface combatant homeported in San Diego (Leonardo DRS, 2021). According to Leonardo DRS, "the nozzles create a backpressure of up to 1,250 pounds per square inch (PSI) at a flow rate of 400 GPM" (2021, under "Highlights"). Instead of a direct stream, the system is designed to create a mist of water droplets to extinguish fires. The WMFFP water supply comes from a potable water tank. Therefore, the water supply is limited by the amount of water stored onboard the ship, unlike the unlimited seawater supply used by tugboats and fireboats.

Contrary to a stream of water, the water mist method would reduce the damage to ship equipment and would be effective in addressing a large swarm of UAS approaching a warship. The fire hoses onboard a DDG would be ineffective and insufficient during a water mitigation technique against a potential UAS swarm based on the distance the water can reach. However, communicating with the other entities in the harbor and coordinating a combined water mitigation strategy could be the most successful approach to defeating a UAS swarm.

B. NETWORK INTEGRATION

In order for a USN DDG to coordinate a UAS swarm mitigation strategy with local authorities in the San Diego Harbor, a Communications Plan (Comm Plan) would need to be established to ensure effective network integration. Comm Plan development is based on the local OPTASK Comm message put out by the Immediate Superior in Charge (ISIC). For a DDG, the ISIC is typically a Destroyer Squadron, more commonly referred to as a DESRON. OPTASK Comms are governed by a Regional Satellite Communications Support Center (RSSC), because they manage and own all of the radio frequencies in the region. Comm Plans are considered a mission vulnerability which requires operational frequencies to be classified.

Comm Plans are prepared by the Staff Communications Officer (Commo), along with instructions and other pertinent documents to carry out the missions or task. Typically, Comm Plans are published as “communications annexes to operational plans or orders” (DON, 2008, Sec. 1.3.13, para. 1), and they are tailored to specific tactical scenarios. When embarked to a USN ship, the Staff Commo works alongside the Ship Commo to ensure communications onboard are maintained effectively. The Ship Commo is also responsible for training, exercises and testing in the communications department to ensure the strike group is ready to deploy. This includes “informal quizzes to ensure system familiarity and drills to ensure proficiency in area of contingency communications” (DON, 2008, Sec. 1.6.3, para. 2). Comm Plans are disseminated to Radio, Bridge, Combat Information Center (CIC), the Commanding Officer (CO), Executive Officer (XO), etc.

The following sections explain the current communications available onboard each marine entity in the harbor, some of which will be used in the Comm Plan.

1. Tugboats

The primary means of tugboat communications is the bridge-to-bridge (B2B) radio. B2B radio is a Very High Frequency (VHF) stand-alone system used for short-range, nonsecure, voice communications with vessels in close proximity to each other (Sherman, 1999) or within LoS. B2B radio hardware can vary in appearance, but generally consists of a transceiver, handset, speakers and antenna, shown in Figure 33.

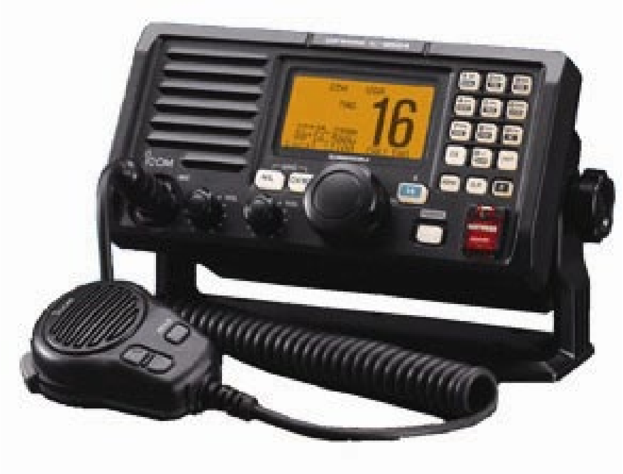


Figure 33. Marine VHF Radio. Source: Department of Energy and Environmental Protection (2022).

VHF Marine Channel 16 (156.8 MHz), also known as the national marine distress frequency, is a VHF radio frequency used on the B2B radio. This channel is monitored at all times by maritime vessels, including tugboats, to listen for “distress safety and calling...to get the attention of another station (calling) or in emergencies (distress and safety)” (Federal Communications Commission, 2021, Under “Type of Message”). Communications on this channel are not to exceed one minute to ensure timely reception of distress calls (Lees & Williamson, 2009). Once a vessel reaches out and establishes communications through channel 16, the two communicating vessels must switch to another working channel to maintain the conversation.

The Chouest tugboats in the San Diego Harbor use dedicated VHF frequencies 139.65, 139.725, 139.925, and 139.975 for communication between the tug captains and the harbor pilots. Along with Channel 16, the tugboats use the standard marine VHF channels 12, 13 and 14 for communication with other traffic in the area and for conducting port operations.

2. Fireboats

Fireboats communicate in the same manner as tugboats, using the B2B radio as the primary means of communication. To communicate with fireboats, the DDG bridge watchstander use Channel 16 to establish communications with the SDHP fireboats quickly in the event of an incoming UAS swarm. The Navy dispatcher would then call via the bridge sound-powered telephone or switch to a different channel to continue communicating with the SDHP fireboats.

The SDHP fireboats use a tracker called Blue Force Tracker. The purpose of this tracker is to “provide instantaneous intelligence on how an operation is unfolding in real time” (Ball, 2020) through GPS location. The Navy does not have access to this system. However, the Blue Force Tracker allows the fireboats to coordinate their locations in relation to each other to safely and effectively assist the DDGs with a wall of water to reduce the effectiveness of a swarm of commercial drones attacking the warship.

In 2002, the Port of San Diego established a Joint Harbor Operations Center to centralize police communications within the harbor. Police respond to incidents within the harbor in a timely manner because the SDHP dispatchers communicate with the civilian entities in the harbor to “facilitate information sharing” (Port of San Diego, 2012). The Joint Harbor Operations Center can be used to organize the SDHP fireboats and the tugboats to respond to an incoming UAS swarm threat and assist DDGs in the harbor with the water mitigation strategy.

3. USCGC

The primary means of communication for USCGC include Fleet Tactical Communication (FLT TAC) and B2B. FLT TAC resides on the unencrypted frequency 277.8 MHz and is known as plain voice communications (Department of Transportation, 1991). It would primarily be used by the USCGC and DDGs when there is no other prearranged frequency established. However, the Comm Plan would alleviate this issue by designating a specific tactical frequency for communications in the event of a UAS attack.

4. DDG

Similar to the USCGC, USN DDGs use FLT TAC while underway. FLT TAC is also used to navigate when visibility is low, primarily when entering and leaving a port. DDGs also use NAVY RED for secure voice communications. However, NAVY RED would not be used if a DDG was requesting assistance in the harbor from civilian or non-Navy vessels.

To communicate with other marine vessels in the harbor, DDGs utilize VHF LoS circuits, specifically B2B communications. Similar to a Citizens Band (CB) radio, each vessel typically uses a call sign. The DDG requests assistance by broadcasting over Channel 16, the distress channel that is continuously monitored by the USCGC, ECO tugboats and SDHP fireboats. Once communications are established on the general communications channel, the DDG and supporting unit(s) can switch to another channel to ensure Channel 16 remains clear. The Comm Plan establishes which channel is used for further conversations.

C. SCENARIO

The scenario for this thesis takes place in the San Diego Harbor, the location of Naval Base San Diego and the Pacific Fleet homeport to over 50 Naval ships. When a USN DDG is transiting the harbor, it is susceptible to UAS attacks launched from the land on three sides, shown in Figure 34. The crew onboard would respond to an incoming UAS threat in the same way they would respond to other incidents at sea. The Comm Plan would lay out the network integration for the DDG and supporting units in order to coordinate with local authorities during a UAS swarm attack.

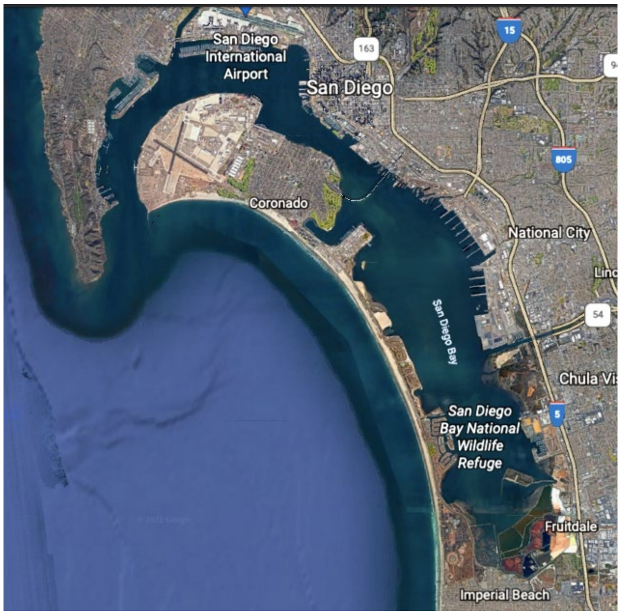


Figure 34. Satellite view of the San Diego Bay. Source: Google Earth (2021).

Defense on a DDG begins in CIC, the classified “tactical command center for most U.S. Navy ships” (Jessee & Reggia, 2020, para. 1). The CIC Watch Officer (CICWO) is in charge of CIC and its personnel. Inside of CIC, national mission data is monitored on the operator consoles and displays, called Common Display Systems (CDS). The data is received from various radars and sensors, which is then analyzed by sailors in the CIC. Figure 35 shows CIC sailors standing watch and monitoring CDS for external risks, hazards and threats.

Figure 35. CIC sailors monitoring CDS. Source: Jessee and Reggia (2020).

The pertinent information and intelligence of an incoming UAS swarm threat gathered from CIC would be reported to the Officer of the Deck (OOD) from the CICWO. According to Vandiver in *Task and Purpose*, the bridge watch team, led by a qualified OOD, mainly consists of a lesser experienced junior officer who is completing Under Instruction (U/I) watches, the Conning Officer who instructs the helmsman on the steering of the ship, the quartermaster who works to make sure the ship remains on the accurate path and maintain the correct speed, the boatswain's mate who manages the internal PA system and takes reports from the lookout sailors (Vandiver, 2017). When DDGs are executing particular maneuvers, such as pulling in and out of a port or harbor, the bridge team is assisted by roving watchstanders to oversee the safety of the ship.

Once the OOD receives intel from the CICWO about a sUAS swarm approaching, he or she informs the CO and XO, who are both required to be on the bridge when transiting dangerous areas, such as the San Diego Harbor. After notification of the CO and XO, the OOD would direct a watchstander on the bridge to pull an alarm to alert sailors onboard of the inbound swarm. Similar to the collision alarm used onboard USN ships, a UAS attack alarm would give the ship's crew information about the incoming threat and what defensive actions need to be taken.

The Comm Plan should be referenced when coordinating with external local authorities in the area if additional support is needed to defend against the drone swarm. For quick contact, the OOD would use the B2B radio to reach out to the other marine entities monitoring Channel 16. Once communications has been established with the USCGC, SDHP fireboats or the ECO tugboats, further communications would continue on a different, pre-established VHF frequency. The DDG would make requests for desired support based on the size of the threat.

V. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

A water mitigation technique is a viable counter-UAS swarm strategy that can be implemented immediately within current DDG operations in the San Diego Harbor. There are no known restrictions to using water as a defense strategy onboard DDGs. Because this strategy utilizes limitless sea water and existing DDG shipboard communications, it requires no alterations to the communications and equipment infrastructure onboard. This water mitigation technique can also potentially be used in conjunction with other C-UAS techniques outside of the harbor environment to defend against drones or drone swarms.

Although a water mitigation technique has the capability to be used immediately, development and testing of a Comm Plan must be conducted to determine the best way to implement the network integration needed to bring this C-UAS strategy to culmination. The communications onboard DDGs, USCG ships, fireboats and tugboats need pre-coordination in order to come together and be effective against a UAS swarm in the San Diego Harbor.

B. RECOMMENDATIONS FOR FUTURE WORK

Due to time constraints associated with executing this research in the middle of the COVID-19 pandemic, planned field experimentation of water mitigation techniques were unable to be conducted. Recommendations for future work include field experimentation to determine the degree to which kinetic kill and visual obscurity might impact the effectiveness of an incoming UAS swarm.

Future research to expound on this thesis would be creating and executing a Comm Plan involving a DDG, the ECO tugboats, the SDHP fireboats and the USCGC to determine whether a Comm Plan and UAS swarm water mitigation technique can be executed successfully. The performance of the Comm Plan would need to be thoroughly tested before the efficacy of a water mitigation technique can be tested. The Comm Plan and water mitigation strategy can be verified by simulating a sUAS swarm attack in the

San Diego Harbor utilizing a few small, autonomous drones. Another area for further study would be using the network integration established with this thesis to develop strategies to defeat UAS swarms in a harbor environment.

LIST OF REFERENCES

Airborne Drones. (2017, August 1). *Airborne drones discusses drones for commercial use- fixed wing or long range multi-rotor.* https://www.airbornedrones.co/fixed-wing-long-range-multi-rotor/

Ball, B. (2020, November 25). *Why blue force tracking and situational awareness require vertical positioning.* NEXTNAV. https://nextnav.com/blue-force-tracking/

Ball, M. (2016, October 6). *Northrup Grumman demonstrates counter-UAS technologies.* Unmanned Systems News. https://www.unmannedsystemstechnology.com/2016/10/northrop-grumman-demonstrates-counter-uas-technologies/

Bevelacqua, P. (2015). *Directivity.* Antenna Theory. http://www.antenna-theory.com/basics/directivity.php

Breeden, J. (2021, September 8). *Swarms may offer next level artificial intelligence.* Nextgov. https://www.nextgov.com/ideas/2021/09/swarms-may-offer-next-level-artificial-intelligence/185177/

Butcher, G., Mottar, J., Parkinson, C. L., & Wollack, E. J.(2011). *Tour of the Electromagnetic Spectrum.* National Aeronautics and Space Administration. https://smd-prod.s3.amazonaws.com/science-pink/s3fs-public/atoms/files/Tour-of-the-EMS-TAGGED-v7_0.pdf

Campion, M., Ranganathan, P., & Faruque, S. (2018). A review and future directions of UAV swarm communication architectures. *2018 IEEE International Conference on Electro/Information Technology (EIT).* https://doi.org/10.1109/EIT.2018.8500274

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

Castillo-Effen, M., Ippolito, C. A., Johnson, E., Ren, L., Takuma, N., Yoon, Y., & Yu, H. (2017). Small unmanned aircraft system (SUAS) categorization framework for low altitude traffic services. *2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC)*, 1–10. https://doi.org/10.1109/DASC.2017.8101996

Chagoya, J. (2017, February 22). *NPS, academic partners take to the skies in first-ever UAV swarm dogfight.* Naval Postgraduate School. https://nps.edu/-/nps-academic-partners-take-to-the-skies-in-first-ever-uav-swarm-dogfig-1

Chapman, A. (2019, December 18). *Types of UAVs: multi-rotor vs fixed-wing vs single rotor vs hybrid VTOL.* AUAV. https://www.auav.com.au/articles/drone-types/

CACI International Inc. (2020). *SkyTracker technology suite: CACI takes on the rapidly evolving global C-UAS threat.* https://www.caci.com/trending/skytrackerr-technology-suite-caci-takes-rapidly-evolving-global-c-uas-threat

CACI International Inc. (2021, October 11). *CACI debuts two new counter-unmanned aircraft system technologies.* https://investor.caci.com/news/news-details/2021/CACI-Debuts-Two-New-Counter-Unmanned-Aircraft-System-Technologies/default.aspx

Callahan, C. (2021, September 14). *Using drones for bird's eye view on search-and-rescue efforts*. Times Union. https://www.timesunion.com/hudsonvalley/outdoors/article/hudson-valley-drones-search-and-rescue-16455705.php

Corrigan, F. (2020, May 14). *How to secure your drone from hackers permanently.* DroneZon. https://www.dronezon.com/learn-about-drones-quadcopters/how-to-protect-your-drone-from-hackers-permanently/

Speicher, A. (2016, January 27). *What is the difference between a UAV and UAS?* DartDrones. https://www.dartdrones.com/difference-between-uav-and-uas/

Department of Defense. (2011). *Unmanned aircraft system airspace integration plan.* https://info.publicintelligence.net/DOD-UAS-AirspaceIntegration.pdf

Department of Energy and Environmental Protection. (2022). *Marine VHF radio: The basics.* https://portal.ct.gov/DEEP/Boating/Safety/Marine-VHF-Radio--The-Basics

Department of Homeland Security. (2015). *The cutters, boats, and aircraft of the U.S. Coast Guard.* https://www.uscg.mil/Portals/0/documents/CG_Cutters-Boats-Aircraft_2015-2016_edition.pdf?ver=2018-06-14-092150-230

Department of the Navy. (2008). *Naval Telecommunications Procedures 4(E).* https://info.publicintelligence.net/USNavy-NTP4E.pdf

Department of the Navy. (2012). REDLINES (COMNAVSURFPAC/COMNAVSURFLANT Instruction 3504.1B). http://www.dcfpnavymil.org/Library/tycom/3504%201B%20REDLINES.pdf

Department of the Navy. (2012). Naval Base San Diego (NBSD) information handbook. *Naval base San Diego instruction 5450.8Q.* https://www.cnic.navy.mil/content/dam/cnic/cnrsw/NBSD/5450.8Q.pdf

Department of the Navy. (2021, March 16). *Department of the Navy unmanned campaign framework.* https://www.navy.mil/Portals/1/Strategic/20210315%20Unmanned%20Campaign_Final_LowRes.pdf?ver=LtCZ-BPlWki6vCBTdgtDMA%3D%3D

Department of Transportation. (1991, May 08). *USCG radio frequency plan.* https://silo.tips/download/comdtinst-m24001f-8-may-1991

DJI. (2020). *Phantom 3 advanced - specs.* DJI. https://www.dji.com/phantom-3-adv/info

Dockrill, P. (2018, January 11). *First-ever UAV swarm attack has struck Russian military bases, sources claim*. Science Alert. https://www.sciencealert.com/swarm-home-made-drones-strike-military-base-first-attack-kind-russia-uavs

DroneShield. (2021). *DroneSentry-X.* https://www.droneshield.com/sentry-x

Edison Chouest Offshore. (n.d). *Highly Specialized Vessels for Job-Specific Tasks.* Edison Chouest Offshore. Retrieved June 7, 2022 from https://www.chouest.com/vessels.html

English, T. (2019, December 29). *Electromagnetic pulse weapons are used by militaries around the world.* Interesting Engineering. https://interestingengineering.com/what-are-emps-and-how-are-they-used-in-warfare

Federal Communications Commission. (2021). *Ship Radio Stations*. https://www.fcc.gov/ship-radio-stations

Fisher, D. (2013, December 03). *How to skyjack a UAV in an hour for less than $400.* Threat Post. https://threatpost.com/how-to-skyjack-UAVs-in-an-hour-for-less-than-400/103086/

Flynn, J. (2014, June 23). *U.S. Coast Guard small cutters and patrol boats.* https://media.defense.gov/2018/Apr/11/2001901931/-1/-1/0/FLYNN_SMALL_CUTTERS_WPBS-2014.PDF

Fox News. (2017, April 25). *Drone swarms deployed in aerial dogfight test.* https://www.foxnews.com/tech/drone-swarms-deployed-in-aerial-dogfight-test

Friedberg, S. (2019, April 19). *A primer on jamming, spoofing, and electronic interruption of a UAV*. Dedrone. https://www.dedrone.com/blog/primer-jamming-spoofing-and-electronic-interruption-of-a-drone

Gagaridis, A. (2022, January 5). *Warfare evolved: Drone swarms-analysis*. Eurasia Review. https://www.eurasiareview.com/05012022-warfare-evolved-drone-swarms-analysis/

Ganesan, R., Raajini, X., Nayyar, A., Sanjeevikumar, P., Hossain, E., & Ertas, A. (2020, June 01). *BOLD: Bio-inspired optimized leader election for multiple UAVs.* MDPI. https://www.mdpi.com/1424-8220/20/11/3134

Hartmann, K., & Giles, K. (2016). *UAV exploitation: A new domain for cyber power.* 2016 8th International Conference on Cyber Conflict (CyCon), 205–221. doi:10.1109/cycon.2016.7529436.

Higdon, C. E. (2000). Water barrier ship self defense lethality. *Naval Engineers Journal, 12*(4), 121–135. https://doi.org/10.1111/j.1559-3584.2000.tb03323.x

Hoehn, J. R., & Sayler, K. M. (2021). Department of Defense counter-unmanned aircraft systems (CRS Report No. IF11426 Version 10). Congressional Research Service. https://fas.org/sgp/crs/weapons/IF11426.pdf

Hughes, M. (2016, October 16). *Antenna basics: Radiation patterns, permittivity, directivity, and gain.* All About Circuits. https://www.allaboutcircuits.com/technical-articles/antenna-basics-field-radiation-patterns-permittivity-directivity-gain/

Husseini, T. (2019, April 1). *Navy laser weapon systems: Identifying the top five.* Naval Technology. https://www.naval-technology.com/features/navy-laser-weapon-systems/

Jessee, M.S., & Reggia, L.M. (2020). Building the combat information center of the future. *Johns Hopkins APL Technical Digest, 35*(2), 116–122. https://www.jhuapl.edu/Content/techdigest/pdf/V35-N02/35-02-Reggia.pdf

Joint Chiefs of Staff. (2012). Electronic Warfare (JP 3-13). https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf

Joint Chiefs of Staff. (2020). DOD dictionary of military and associated terms. https://irp.fas.org/doddir/dod/dictionary.pdf

Judson, J. (2020, August 03). *Raytheon and Rafael to build iron dome in U.S.* Defense News. https://www.defensenews.com/land/2020/08/03/raytheon-and-rafael-to-build-iron-dome-in-us/

Kallenborn, Z. (2018, October 24). *The era of the UAV swarm is coming, and we need to be ready for it.* Modern War Institute. https://mwi.usma.edu/era-drone-swarm-coming-need-ready/

Keown, L. (2019), August 4). [Mediterranean Sea]. All Hands Magazine of the U.S. Navy. https://allhands.navy.mil/Media/Gallery/igphoto/2002359112/

LaGrone, S. (2019, July 19). *Marines took out iranian UAV for the cost of a tank of gas.* USNI News. https://news.usni.org/2019/07/19/marines-took-out-iranian-drone-for-the-cost-of-a-tank-of-gas

Larson, C. (2021, July 13). *The U.S. Navy has a new weapon to defeat killer drone swarms.* 1945. https://www.19fortyfive.com/2021/07/the-u-s-navy-has-a-new-weapon-to-smash-stealth-drones-to-bits/

Lees, G., & Williamson, W. (2009). *Handbook for marine radio communication* (5th edition). Informa Law.

Leonardo DRS. (2021). *High pressure water mist fire fighting pump*. https://www.leonardodrs.com/what-we-do/products-and-services/water-mist-fire-fighting-pump-wmffp/

Liberatore, S. (2015, December 11). *Tokyo police reveal bizarre 'UAV catcher'*. Daily Mail. https://www.dailymail.co.uk/sciencetech/article-3356746/How-catch-UAV-BIGGER-UAV-giant-net-Tokyo-police-reveal-bizarre-UAV-catcher.html

Liebermann, O. (2021, October 20). *Drone attack targets U.S. troops at U.S. base in Syria, initial assessment suggests no U.S. injuries.* CNN. https://www.cnn.com/2021/10/20/politics/drone-attack-syria/index.html

Liptak, A. (2019, July 21). *A U.S. Navy ship used a new UAV-defense system to take down an Iranian UAV*. The Verge. https://www.theverge.com/2019/7/21/20700670/us-marines-mrzr-lmadis-iran-UAV-shoot-down-energy-weapon-uss-boxer

Lockheed Martin. (2020). *ATHENA laser weapon system prototype.* https://www.lockheedmartin.com/en-us/products/athena.html

Losey, S. (2022, February 28). *Killing drones with Thor's hammer: Air Force eyes counter-UAS 'Mjölnir' weapon*. DefenseNews. https://www.defensenews.com/air/2022/02/28/killing-drones-with-thors-hammer-air-force-eyes-counter-uas-mjolnir-weapon/

McMullan, T. (2019, March 16). *How swarming UAVs will change warfare.* BBC News. https://www.bbc.com/news/technology-47555588

McNeil, P. (2017, February 9). *Antenna gain and directivity-The basics.* Pasternick. https://blog.pasternack.com/antennas/antenna-gain-directivity-basics/

MetalCraft Marine (2021, August 28). *Firestorm 36 high-speed aluminum fireboat.* http://metalcraftmarine.com/html/firestorm_36.html

Michel, A. H. (2018, February). Counter-UAV Systems. The Center for the Study of the Drone at Bard College. https://dronecenter.bard.edu/files/2018/02/CSD-Counter-Drone-Systems-Report.pdf

Mitchell, E. (2020, July 16). *Navy puts out fires aboard USS Bonhomme Richard after four days of fighting blaze.* The Hill. https://thehill.com/policy/defense/507737-navy-puts-out-fires-aboard-uss-bonhomme-richard-after-four-days-of-fighting

Mizokami, K. (2019, March 21). *The Navy will put a laser gun on a destroyer by 2021.* Popular Mechanics. https://www.popularmechanics.com/military/weapons/a26898213/navy-laser-weapon-destroyer/

Mizokami, K. (2020, May 27). *The Navy just tests its most powerful laser yet*. Popular Mechanics. https://www.popularmechanics.com/military/navy-ships/a32676643/navy-laser-weapon-system-demonstrator-test/

Nichols, R. K., Ryan, J. J., Mumm, H. C., Lonstein, W. D., Carter, C., & Hood, J. P. (2018). *Unmanned aircraft systems in the cyber domain* (2nd ed.). New Prairie Press.

Nikolic, S. (2017). *An innovative response to commercial UAV menace: Anti-UAV falconry.* Vojno Delo, 69(4), 146–167. doi:10.5937/vojdelo1704146n

Ockerhausen, J., Stambaugh, H., & Kelly, S. (2003, May). Special report: Fireboats: Then and now. Report No. USFA-TR-146. Homeland Security. https://www.usfa.fema.gov/downloads/pdf/publications/tr-146.pdf

Office of Corporate Communication. (2021, September 20). *SeaRAM close-in weapon system (CIWS) Anti-ship missile defense system.* https://www.navy.mil/Resources/Fact-Files/Display-FactFiles/Article/2167555/searam-close-in-weapon-system-ciws-anti-ship-missile-defense-system/

Palmer, T. S., & Geis, J. P. (2017). Defeating small civilian unmanned aerial systems to maintain air superiority. Air & Space Power Journal, 102–118. https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-31_Issue-2/V-Palmer_Geis.pdf

Pappalardo, J. (2013, April 11). *Why the navy loves laser weapons*. Popular Mechanics. https://www.popularmechanics.com/military/weapons/a8825/why-the-navy-wants-to-fall-in-love-with-laser-weapons-15336997/

Pawlyk, O. (2020, January 15). *New Pentagon team will develop ways to fight enemy UAVs*. Military News. https://www.military.com/daily-news/2020/01/15/new-pentagon-team-will-develop-ways-fight-enemy-drones.html

Phelps, M. (2018, July 16). *SteelRock launches Odin counter-UAV system*. AIN Online. https://www.ainonline.com/aviation-news/aerospace/2018-07-16/steelrock-launches-odin-counter-uav-system

Pokrajac, I., Kozić, N., Čančarević, A., & Brusin, R. (2018). Jamming of GNSS signals. *Scientific Technical Review*, *68*(3), 18–24.

Port of San Diego. (2012, July 20). *San Diego Harbor Police: Both law enforcement officers and Marine firefighters* [Video]. https://www.youtube.com/watch?v=emb0oW1RVL4

sUAS News. (2022, March 10). *Drones help detect and prevent ever-increasing forest fires*. https://www.suasnews.com/2022/03/drones-help-detect-and-prevent-ever-increasing-forest-fires/?utm_source=DroneNewsDailyEmailMore&mc_cid=1a532ea601&mc_eid=206e234265

Rains, T. (2021, October 21). *Google's drone delivery company is partnering with Walgreens to deliver meds, food, and household items to customers in Dallas.* Business Insider. https://www.businessinsider.com/drone-delivery-company-partners-walgreens-store-door-air-delivery-service-2021-10

Rassoul, M. (2022, January 5). *Low-cost warfare: U.S. military battles with 'Costco drones'.* The Fifth Skill News. https://thefifthskill.com/low-cost-warfare-us-military-battles-with-costco-drones/

Raytheon Technologies. (2020). *Phaser high-power microwave system*. https://www.raytheonmissilesanddefense.com/capabilities/products/phaser-high-power-microwave

Ripple, B. (2019, September 24). *Enemy UAV operators may soon face the power of THOR.* Official United States Air Force website. https://www.wpafb.af.mil/News/Article-Display/Article/1969142/enemy-UAV-operators-may-soon-face-the-power-of-thor/

Safi, M. (2019, December 04). *Are UAV swarms the future of aerial warfare?* The Guardian. https://www.theguardian.com/news/2019/dec/04/are-drone-swarms-the-future-of-aerial-warfare

Shankland, S. (2022, April 19). *Ukraine is fighting Russia with drones and rewriting the rules of war.* CNET. https://www.cnet.com/news/ukraine-is-fighting-russia-with-drones-and-rewriting-the-rules-of-war/

Sherman, R. (1999). *Radio communications system*. https://man.fas.org/dod-101/sys/ship/weaps/radio.htm

Singh, M. (2018, July 14). *Countering the drone swarm.* All About Air Defence. http://www.airdefence.in/uncategorized/countering-the-drone-swarm/

Sisk, R. (2019, September 23). *Attacks on Saudi oil plants reveal weaknesses in US-made defenses.* Military News. https://www.military.com/daily-news/2019/09/23/attacks-saudi-oil-plants-reveal-weaknesses-us-made-defenses.html

Delft Dynamics. (2019, October 01). *DroneCatcher, Controlled Drone Interception*. Delft Dynamics. https://dronecatcher.nl/

Slayen, B. (2020, July 20). *Northrop Grumman taps Epirus for electromagnetic pulse C-UAS weapon system*. Northrup Grumman. https://news.northropgrumman.com/news/releases/northrop-grumman-taps-epirus-for-electromagnetic-pulse-c-uas-weapon-system

Sly, L. (2018, January 10). *Who is attacking Russia's bases in Syria? A new mystery emerges in the war*. The Washington Post. https://www.washingtonpost.com/world/who-is-attacking-russias-main-base-in-syria-a-new-mystery-emerges-in-the-war/2018/01/09/4fdaea70-f48d-11e7-9af7-a50bc3300042_story.html

Speicher, A. (2016, January 27). *What is the difference between a UAV and UAS?* DartDrones. https://www.dartdrones.com/difference-between-uav-and-uas/

Tahir, A., Böling, J., Haghbayan, M., Toivonen, H., & Plosila, J. (2019). Swarms of unmanned aerial vehicles - A survey. *Journal of Industrial Information Integration, 16*, 1–7. https://doi.org/10.1016/j.jii.2019.100106

TechLink. (2020). *Counter-swarm interception with self-organizing, sacrificial UAVs.* The Pulse Newsletter. https://techlinkcenter.org/technologies/counter-swarm-interception-with-self-organizing-sacrificial-uavs/55adbfd4-7fef-48eb-a6a1-ec4f54a7d898

Urban, B. (2021, August 6). *U.S. Central Command statement on the investigation into the attack on the motor tanker Mercer Street*. U.S. Central Command. https://www.centcom.mil/MEDIA/PRESS-RELEASES/Press-Release-View/Article/2722418/us-central-command-statement-on-the-investigation-into-the-attack-on-the-motor/

Vandiver, Shawn. (2017). *Here's how Navy crews watch for (and respond to) collisions at sea*. Task & Purpose. https://taskandpurpose.com/community/heres-navy-crews-watch-respond-collisions-sea/

Vattapparamban, E., Guvenc, I., Yurekli, A. I., Akkaya, K., & Uluagac, S. (2016). UAVs for smart cities: Issues in cybersecurity, privacy, and public safety. *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*, 216–221. doi:10.1109/iwcmc.2016.7577060

Watson, B. (2018, October 18). *Against the UAVs: How to stop weaponized consumer UAVs*. Defense One. https://www.defenseone.com/feature/against-the-drones/

Wilde, W. D., Cuypers, G., Sleewaegen, J., Deurloo, R., & Bougard, B. (n.d.). *GNSS interference in unmanned aerial systems (Tech.).* https://www.septentrio.com/sites/default/files/gnss_interference_in_unmanned_aerial_systems_final.pdf

Williams, Christopher. (2021, March 21). *Citadel defense secures new $5M counter drone contract from U.S. Department of Defense*. Business Wire. https://www.businesswire.com/news/home/20210330005011/en/Citadel-Defense-Secures-New-5M-Counter-Drone-Contract-from-U.S.-Department-of-Defense

Wilson, J. R. (2018, November 1). *The new world of counter-drone technology.* Military & Aerospace Electronics. https://www.militaryaerospace.com/unmanned/article/16707131/the-new-world-of-counterUAV-technology

Wilson, J. R. (2019, November 19). *The new era of high-power electromagnetic weapons.* Military & Aerospace Electronics. https://www.militaryaerospace.com/power/article/14072339/emp-high-power-electromagnetic-weapons-railguns-microwaves

Witherow, T. (2016, February 08). *Police set to use eagles to foil terrorist UAV attacks.* Daily Mail. https://www.dailymail.co.uk/news/article-3436572/Police-set-use-EAGLES-foil-terrorist-UAV-attacks-Scotland-Yard-confirms-birds-prey-used-intercept-aircraft-video-showed-one-plucked-sky.html

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