COUNTER UNMANNED AERIAL SYSTEM DEFENSE FOR HIGH VALUE UNITS AFLOAT PIERSIDE

by

Chris Hood

A Dissertation

Submitted to the Faculty of Purdue University
In Partial Fulfillment of the Requirements for the degree of

Doctor of Philosophy

Department of Computer and Information Technology
West Lafayette, Indiana
August 2021

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF COMMITTEE APPROVAL

Dr. Eric T. Matson, Chair
Computer and Information Technology

Dr. John Gallagher
Electrical Engineering and Computer Science
University of Cincinnati

Dr. J. Eric Dietz
Computer and Information Technology

Dr. John Springer
Computer and Information Technology

Approved by:
Dr. Kathryne Newton

Dedicated to Adler.

Never forget our three secrets:

I love you so much. I am so proud of you. I am so glad to be your Dad.

ACKNOWLEDGMENTS

Thank you Lesleay for not telling anyone that how much of a dumb dumb I really am when it comes to computers. I'm going to be a computer doctor thanks to you! These past three years have been the best ever. I love you forever. HIWTNSU!

Thank you to my family, especially to my parents, Terry and Shirley Hood, and to Bob and Teresa Workman. I can't even start to describe how you've influenced, pushed, and supported me through the years. I love you all so much.

Thank you Dr. Eric Matson for setting me up for success. Thank you for the invitation to the C-UAS project that really turned things around. You set me on my path. Thank you Dr. John Gallagher for always providing randomly-timed whimsical LOTR references to both distract me, and enable me to find my ticket. Thank you to my advisory committee. COVID made things interesting regarding how normal committee meetings and presentations take place. Thank you for being flexible.

Thank you Dr. J. Eric Dietz and David Hankins for this amazing opportunity via the Purdue Military Research Institute. Never in our wildest dreams did we think shore duty in Indiana would allow us to collectively achieve such great things. Thank you Purdue NROTC leadership for allowing me to fully integrate as a college student. Your flexibility and assistance was integral to my family striving through the COVID and life.

Thank you Austin Riegsecker for just about everything. You helped me set up my computer on Day 1 and with my model on Day 1001. Thank you for showing me how college works, 20 years after I graduated from high school. Thank you shipmate.

Thank you Duncan Mulgrew, Jeremy Frederick, and the boys for your subject matter expertise. Thank you for always wanting to help, providing a unique perspective on all things UAV, and for performing air shows for Adler.

Thank you Toy Andrews for always letting me know where you stood with your project. Thank you for the Fridays at Brockerage, the get-togethers with the wives and kiddos, and for the constant use of Navy vernacular while up in chat.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

AWS	Aegis Weapons System
C2	Command and Control
CIWS	Close-in Weapons System
C-sUAS	Counter small Unmanned Aerial System
C-UAS	Counter Unmanned Aerial System
C-UAV	Counter Unmanned Aerial Vehicle
DoD	Department of Defense
DHS	Department of Homeland Security
EM	Electro-magnetic
EMP	Electro-magnetic Pulse
EO	Electro-optical
FAA	Federal Aviation Authority
GNSS	Global Navigation Satellite Systems
GPS	Global Positioning System
HELIOS	High Energy Laser with Integrated Optical Dazzler and Surveillance
HPM	High Power Microwave
HVU	High Value Unit
IR	Infrared
ISR	Intelligence, Surveillance, and Reconnaissance
JCO	Joint Counter sUAS Office
LiDaR	Light Detection and Ranging
LoS	Line of Sight
NLFoS	Navy Laser Family of Systems
ODIN	Optical Dazzling Interdictor, Navy
RCS	Radar Cross-section
RF	Radio Frequency
RPA	Remote Piloted Aircraft
RTH	Return to Home

SECARMY	Secretary of the Army
SECDEF	Secretary of Defense
SM	Standard Missile
SME	Subject Matter Expert
SNLWS	Surface Navy Laser Weapons System
SoS	System-of-Systems
SSL	Steady State Laser
SSL-TM	Stead State Laser- Technology Maturation
sUAS	Small Unmanned Aerial System
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle

ABSTRACT

Counter Unmanned Aerial System (C-UAS) development and fielding has greatly accelerated over the last several years to protect against all classes of Unmanned Aerial System (UAS) threats. Integration of the detection and tracking systems, the engagement systems, and other portions of the kill chain including command and control (C2) is ongoing. A significant concern is that the majority of these developments are designed for defending ships at sea. Most of these technological advances cannot be used within restricted waters or in port, foreign or domestic, due to the potential of high collateral damages and the fact that they are not currently readily available for dissemination to the Fleet.

The problem addressed by this project is to determine how to defend high value units from the threat of weaponized UAVs while moored pier-side with currently in-place weapons systems. This study will take a parameter-driven approach based on existing technologies to determine if an enhanced fire-control system integrated with standard issue weaponry can increase watchstander accuracy required to safely defend a high value unit pierside.

1. PURPOSE AND PROBLEM

"The drone threat has been around for years, but the Navy has yet to prioritize defending against these easily acquired weapons. Amid preparations for a high-end fight, the Navy still is vulnerable to an adversary trading thousand-dollar drones for billion-dollar warships" [1].

1.1 Introduction

Man navigates towards water. People flock to the coasts, rivers, lakes, and oceans for the natural resources that it provides. Whether it be as a source for irrigation for farming, as a source of food from fishing, or as a source of recreation for fun or relaxation, the water has always been an attraction. Unfortunately, nefarious players also navigate to the water.

Legislation and regulations have been in place to keep these precious waterways safe from enemies, foreign and domestic. However, everything changed when the terrorists rammed suicide boats into American steel onboard USS Cole on 12 October 2000 in Yemen's Aden Harbor [2], [3], [4], [5]. The threat to our freedom has taken away a portion of our enjoyment of our maritime expeditions. Ever since the attack, civilian and military agencies have searched to counter maritime threats to maritime infrastructure and maritime assets [3].

Maritime security consists of securing and protecting military and domestic ports, piers, docks, and anchorages from threats [6]. Harbors and home ports are an integral part of any country's economic and military stability. These waterways are critical to the recreational and commercial activities that make up our maritime heritage. Additionally, the oceans, rivers, lakes and seas are a critical part of maritime infrastructure and require a certain level of thinking when regarding maritime security. These areas must be protected and secured at all times from enemies, foreign and domestic [7].

The events of September 11, 2001 had a profound impact on our society. Again, everything changed. The Department of Homeland Security (DHS) was created and made significant changes. First thoughts involved airline and airport security, but the changes did not stop there. DHS also implemented changes to secure another vital infrastructure, our maritime security via harbor defense [8]. Emphasis shifted to protecting our ships, crafts and harbors from attacks. Ships, military or civilian vessels, are essentially an extension of a state's territory. The fact that they carry flags of their country are an additional reason as to why maritime security is so important. The flags are potential terrorist targets [2].

1.2 The Problem

Counter Unmanned Aerial System (C-UAS) systems development and fielding has greatly accelerated over the last several years to protect against all classes of Unmanned Aerial System (UAS) threats. Integration of the detection and tracking systems, the engagement systems, and other portions of the kill chain including command and control (C2) is ongoing. A significant concern is that the majority of these developments are designed for defending ships at sea. Most of these technological advances cannot be used within restricted waters or in port, foreign or domestic, due to the potential of high collateral damages.

The problem addressed by this project is the lack of effective C-UAS defense for high value units from the threat of weaponized unmanned aerial vehicles (UAV) while moored pierside with minimal detection and countermeasures available. There is an emerging area of need for a system-of-systems (SoS) architecture that can incorporate shore and shipboard C-UAS capabilities as well as an effective last line of defense strategy. Until that SoS architecture is in place, something else must be implemented to enhance the C-UAS capabilities of the security forces or the typical Navy watch stander.

1.3 Significance

The harbor or port security mission is a significant application in the spectrum of maritime security. Warships, military craft, cruise ships, and maritime infrastructure are key assets that not only represent our maritime heritage, but our economic way of life.

Local anti-aircraft defenses are essentially non-existent these days. The air raid threat no longer exists based on the assumption of the guarantee of air superiority. This is no longer the case, due to the increased interest and advancements in unmanned technologies. Numerous technological advances have been made to attempt to counter the threat of UAVs, however these countermeasures consist of, but are not limited to steady state lasers, electronic attack/warfare (jamming or spoofing), and kinetic methods, all of which have a significantly high probability of collateral damages to the immediate environment. While this is not necessarily a problem when at sea on the open oceans, it is a serious concern within foreign and domestic ports of call or military bases. Essentially, countermeasures have been developed that simply cannot be used in port.

1.4 The Purpose

The purpose of this project is to address the lack of effectiveness of currently available C-UAS defenses, to identify the gaps in the current defense in depth protocols, and to determine the feasibility of an enhanced last line of defense countermeasure to protect vulnerable HVUs pier-side.

When afloat and at sea, high value units such as destroyers, cruisers and other surface combatants have their full arsenal at which to wage war against enemies. Ships at sea are equipped with the latest technology, optimized manning, and are ready for action. Their radars and sensors are operational and their weapons are uploaded. Ships in port are the exact opposite. When afloat pierside, ships may only have onboard one third of the ships compliment, with all radars and sensors offline and all weapons systems downloaded. The import duty section and topside watchstanders are responsible for the safety and security of the ship.

This research will attempt to give the ship and crew a fighting chance against threat UAVs by enhancing the watchstanders' accuracy and performance immediately. Waiting until a new, advanced technology, such as lasers, dazzlers, and the like, will take years to develop, implement and install on bases. The watchstanders need help now.

1.5 Research Questions

The research questions for this study include the following:

- Given a hypothetical system-of-systems (SoS) detection and alert architecture, can an advanced fire-control technology, installed on currently in-place, standard-issue weapons, enhance shipboard C-UAS defense capabilities and watch stander performance, accuracy, and effectiveness?

Specific research objectives include:

- Establish the framework and determine the metrics required to provide the response necessary to successfully defend a high value unit (HVU) positioned on a naval installation from an autonomous, weaponized small unmanned aerial vehicle (sUAV) attack?
- Effectively develop a simulation model with applicable metric(s) to determine how an enhanced, fire control system integrated onto existing weaponry could improve existing watch stander performance.
- Efficiently interpret the data to support or oppose the system's capability for successful C-UAS defense in future applications and strategies.

1.6 Assumptions

The assumptions for this study include the following:

- The data gathered from the UAV industry, from the Department of Defense (DoD), and from research teams will be accurate when discussing current characteristics and capabilities of the UAV/C-UAS technology in place.
- The use of an agent-based modeling simulation will accurately depict the expected conditions and environment of domestic or foreign port of call.
- The environmental norms will be based on an area or a location to be defined later, and will be an accurate average based on a given time frame.
- The use of data from prisons, cruise ship terminals, and airports will be a basis for the model's physical location and description during this research based on their similarities.

1.7 Delimitations

The delimitations for this study include the following:

- Threat aircrafts modeled will consists of quad-copter type sUAS, not fixed wing.
- Threat aircrafts modeled will consist of suicide attack aircraft, not missiles-carrying or grenade-launcher attachments.
- This study will only model one geographic map or harbor for testing mitigations.
- This study will only model a ship pierside, and therefore will not test the effectiveness of standard at-sea weaponry.

1.8 Limitations

The limitations for this study include the following:

- Due to the classification levels of information concerning Department of Defense, United States Naval Ships, and United States Naval Shore Installation capabilities, the researcher is unable to run the model in a classified environment using classified numbers for inputs.
- Probability of detection for sensor systems and probability of kill for weapons will be assumptions.

2. REVIEW OF LITERATURE

The general set of concepts to relative to this research are grouped into three main sections: the taxonomy of maritime threats, the current state of C-UAS technology, and lastly the current state of DoD C-UAS defense capability and strategy. The taxonomy of maritime threats includes the threat types, threat scenarios, and threat locations. The second section discusses the current state of C-UAS detection systems and mitigation methods. Lastly, the DoD C-UAS defense technology section pertains to the strategies, platforms available, and an overview of the sensor modalities and mitigation techniques currently used on or under development for vessels and at naval installations.

Many surveys have been conducted in the past three years that have significantly described the key technologies of UAV and subsequent C-UAV systems. H. Kang et al. [9] consolidated 343 references into a comprehensive paper that sufficiently details this topic. Arthur Holland Michel [10], [11] has additionally provided two in-depth reports on counter-drone systems that consist of the open-source research of reports, testimonies, manufacturer's information and much more. These documents provide a wealth of information that will be cited throughout this review of literature.

2.1 Taxonomy of Maritime Threats

Threats to maritime security come in various shapes, sizes, and colors. Radu et al [2] described categories pertaining to actual actions, to include terrorist attacks, bomb or hostage scenarios, piracy, trafficking of people or forbidden substances, and even threats to the environment. The vastness of the physical layouts of harbors or ports, the population's access to these areas, and the inability to monitor everything yields many openings and opportunities for terrorist plots, actions, and threats. Lastly, some of the most probable threat capabilities come from either divers, fast ships or small boats, mines, or other unforeseen attackers [2].

Muller and Brooks [12] took the discussion a step further and described detailed scenarios where these attacks may take place. Scenarios to be discussed include targets such as military ships, cargo ships, oil tankers, but are not limited to ships. Maritime infrastructures such as piers, warehouses, pilings and even the channels themselves are subject to dangerous and illegal activities. Locations of these scenarios include above and below the waterline by coordinated attacks, divers, swimmers, small boats, or even unmanned delivery vehicles capable of carrying significant payloads. Additionally, Muller and Brooks [12] did not rule out attacks from airborne adversaries and other types of conventional weaponry. It is this the threat of airborne adversarial attacks that will be discussed in this research.

2.1.1 Threat UAS

The small unmanned aircraft systems (sUAS) field continues its rapid development of new technology, thereby creating new, exciting, and readily accessible applications for hobbyists, commercial industry, and military users [9], [13], [14], [15]. The advancement in computing power and the miniaturization of components has improved the functionality for legitimate applications across the globe [14]. These legitimate applications include uses such as agricultural applications, disaster management, photography and movie films, and simple recreational fun [9], [13], [14], [16].

The improvement on legitimate sUAS applications simultaneously creates new risks and the potential for state, non-state, and nefarious actors to utilize drones for operations that could be hazardous to not only Department of Defense (DoD) personnel and facilities, but also to airports, prisons, nuclear facilities and other components of critical infrastructure [13], [14], [17], [18].

Examples of nefarious or negligent sUAS applications include, but are not limited to the following:

1. harassment and protest of German Chancellor Merkel in 2013 [9] ;
2. accidental crash-landing of DJI quadcopter on White House lawn in 2015 [9], [14];
3. radioactive sand carrying drone from Fukushima nuclear power plant in 2017 [9];
4. assassination attempt of Venezuelan President Maduro in 2018 [9], [14];
5. rogue drones interrupting airport operations [9];
6. contraband delivery drones in prisons [9], [14];

7. explosive-carrying drones in the Middle East [19].

There are multiple factors that go into how threatening a sUAS can or will be. These factors include the skill and competency of the user, the type and purpose of sUAS being utilized, and the method at which the sUAS is being guided or controlled. The continued review will address these factors.

The threat from which to model for this research is assumed to be a threat that is impervious to most current C-UAS methods. The price will be within reason, however it is assumed that the user has access to advanced technology with a high level of knowledge in all things regarding autonomous flight behavior, software understanding, and weaponry.

UAV Threat Operator Skill Level

The drone operator's skills and overall level of knowledge have been categorized multiple times. Humphreys [20] breaks operators down into two main categories: Sophisticated and Unsophisticated operators. These unsophisticated operators have the minimal operational experience or knowledge and may inadvertently violate air space restrictions and no-fly zones, resulting in accidental trespassing. Additionally, unsophisticated operators could slightly modify drones to intentionally violate rules and regulations and even trespass. The sophisticated operators, on the other hand, have the capability to piece make UAVs and manipulate the internal components of the drone, rendering it possible to make sophisticated and intentional intrusions [20]. It is the sophisticated operator that will be addressed and analyzed in this study, with their ability to potentially weaponize a drone.

Another categorization of threat operator skill level has four categories. Mike Hopmeier of Unconventional Concepts, Inc. described these four levels in Washington, DC in 2016 as follow [21]:

1. Level I ("Christmas morning")

   These operators consist of individuals that simply purchase a drone off the internet, insert a battery, and start flying. These are the most common types of operators and the price point is relatively low, entry cost being a few hundred dollars or less. These operators could be placed into the negligent or reckless operator category and still create potential risk [13], [21].

2. Level II (“13 year old son”)

   These operators consist of individuals that have slightly more advanced capabilities and could be considered hobbyists. The operators purchase parts from the internet and integrate their own knowledge into manufacturing drones, similar to model building. There is no real understanding of the science or the engineering, and the price point ranges from hundreds to thousands of dollars. Not necessarily considered threats, however they could still fall into the negligent or reckless operator category when near air, land, and maritime domains [13], [21].

3. Level III (“Dr. Evil”)

   These operators actually design, build and test new capabilities and have an in-depth knowledge of multiple technical fields. These operators a technically-sophisticated and not necessarily limited to commercial available components and parts. If persuaded, these operators have the potential to be nefarious [20], [21].

4. Level IV (“Axis of Evil”)

   The last level consists of operators from state or non-state actors and possibly terrorists. These operators are easily considered major strategic and national security threats based on their potential to weaponize drones for kamikaze-style attacks against sensitive targets. This is a significant problem and consists of the operator that this study intends to focus on [20], [21].

The sophisticated, Level IV (Axis of Evil) operator utilizing a sophisticated drone is the significant problem that this study intends to address.

UAV Threat Types

Yaacoub et al. [22] provided a security analysis of drone systems in 2020 that classified drones into three main types. These types of drones are categorized based on their flying mechanisms, whether it be multi-rotor drones, fixed-wing drones, or hybrid-wing drones. These classifications are described below:

1. Multi-Rotor Drones, or rotary-wing drones, perform vertical take-off and landings similar to helicopters. These drones have both advantages and disadvantages. While they have the ability to hover and maintain a constant cellular coverage over a fixed location, they lack advanced mobility and do not have extended stay times [22], [23].
2. Fixed-Wing Drones are either runway/catapult launched or hand-tossed and are significantly more energy efficient than other types of drones. Instead of hovering, these drones flying mechanism is that similar to airplanes and have the ability to glide. Advantages include high speeds, while disadvantages include landing and take-off capabilities and pricey internal computer configurations [22], [23].
3. Hybrid-Wing Drones are essentially combinations of the previous classification types. These drones have the ability to both glide and hover, thereby combing the two advantages of the previous types: ability to travel fast and ability to maintain hover [22], [23].

UAV Threat Control

Yaacoub et al. [22] provided a security analysis of drone systems in 2020 that classified UAV controlling methods. UAV can be controlled remotely, autonomously, or a combination of the two, and fall into three main categories. These categories are described below:

1. Remote Pilot Control is as simple as it sounds. The operator uses some sort of controller, which can consist of anything from a store bought remote, to a cell phone, to a laptop or tablet. The operator, or pilot, uses the controller and is responsible for every maneuver the remote piloted aircraft (RPA) makes [22].
2. Remote Supervised Control is a hybrid version of the Remote Pilot Control. The operator, or pilot, has the ability to intervene when necessary. However, the drone utilizes adaptive automation, meaning that UAV can perform missions independently

of human control or interaction. Way-point or GPS/GNSS guidance enables the UAV to follow pre-programmed routes [22].

3. Full Autonomous Control is the final category and consists of mission operations without any human intervention. This is known as system static automation and allows the device to make decisions independent of human control or interaction [22]. This particular controlling method is largest concern for the researcher and will be addressed further throughout this study.

Demirhan et al [24] developed a camera-based positioning system that automates the landing process for quad-copters. While harmless research and definitely the future of parcel delivery, this type of functionality creates risks and opportunities for nefarious actors to manipulate and weapons drones that could now operate independently, while being impervious to standard mitigation methods to be discussed in later sections [24].

2.1.2 Maritime Threat Scenarios

The threat scenarios, detailing how and where an actual attack may take place, were described by Muller [12] in 2010. These possible threat scenarios are summarized in the list below.

- Surface attack via suicide boat or truck;
- Surface attack via coordinated small boat swarm attack;
- Surface attack via rocket propelled grenade from a unmarked vessel;
- Subsurface attack via diver with improvised explosives;
- Subsurface attack via swimmer delivery vehicle;
- Subsurface attack via unmanned vehicle;
- Subsurface attack via mines;
- Kamikaze attack via small manned aircraft;

- Kamikaze attack via unmanned small aircraft.
- Coordinated air attack by small unmanned aircraft launched from berthed or anchored ship;

These threat scenarios are not limited to ships inside the harbor, but could also be used on pilings and quays in port, or potentially on the hulls of ships at anchor outside the harbor [25]. These categories and attack scenarios must be broken down further by describing the actual threat types that are potentially carrying out these actions.

UAS Threat Scenarios

Enemy unmanned vehicles pose a significant threat to many aspects of maritime security and safety. Not only can they potentially deliver payloads to inflict damage themselves, but they can be used to study, research, and gather data in efforts to properly plan for such an attack. Multiple penetrations by unmanned surveillance crafts ensure that enough data is gathered and analyzed to pull off a successful attack by knowing the assets routines [26].

Unmanned vehicles, from any medium, are just as effective to terrorist groups or organized crime networks as they are to security industries as they do have potentially significant advantages. Unmanned vehicles provide criminals or terrorist groups with these advantages as described by Patterson [26] in 2010:

- stand-off distance for potential targets;
- significantly outnumbering via swarm attacks;
- the ability to deploy unmanned vehicles at varying times to distract and overwhelm authorities;
- small size and relatively cheap to produce;
- flexibility to change the plan during the attack.

Unmanned vehicles could easily carry enough explosives to inflict enough damage or fear. Weaponizing smaller unmanned surface crafts or UAVs could cause serious damage to the actual assets or simply cause an economic chain reaction based on fear of what could be next. The assets do not have to be warships or cruise ships or cargo ships, they could be critical infrastructure or anything that throws off the normal, everyday routine of the harbor. Additionally, the size of explosive payload depends on the size of the vessel being used. Using a remote controlled small boat could render huge damages based on the amount of C-4 or radioactive material it can carry, as to where a weaponized UAV would carry a significantly smaller payload [26], [27].

2.1.3 Maritime Threat Locations

Harbors and ports, both military and civilian, require constant supervision and security due to the nature of their high value units. Military ships and structures are normally protected somewhat separately from the rest of the harbor and civilian traffic. Non-military bases, harbors or ports also have high value units, to include cargo ships and cruise ships, both of which require open water protection [28].

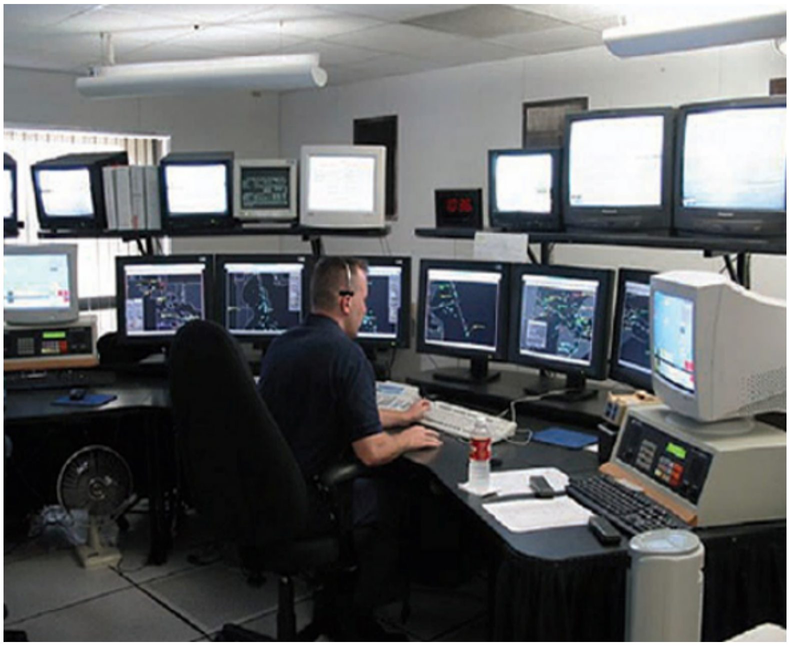


Figure 2.1. Typical layout of port authorities control center [29]

The physical layout of a harbor or port differs from place to place. These ports are monitored by port authorities as seen Figure 2.1 in a control station [29]. Generally speaking, they consist of a large area of water with a multitude of maritime infrastructure platforms, to include piers, dock, warehouses, boat launches, etc. These structures represent multiple businesses, properties, and boundaries. The harbor surface has been physically characterized by Radu [2] as follows:

- Perimeter boundary fences;
- Access control points;
- Infrastructure (transport, communications, public utilities, maritime flow command and control installations, etc.);
- Harbor basin;
- Berths (operative and technical) providing the ship-port interface (with a maximum admitted tonnage at berths, maximum depth at berth determines a certain operation capacity, which in turn determines which ship types are admitted);
- Banks protecting the berths against sea waves;
- Port operators providing various services (pilotage, towing, berthing and releasing ships, supply, operation);
- Merchandise storage.

The common maritime infrastructure as we know it is vulnerable to a wide array of threats. The vastness of the physical layout, the population's access to the area, and the inability to monitor everything leaves many openings and opportunities for terrorist plots, threats, and actions [2]. For these reasons, maritime security must continuously be analyzed and plans must be further developed to ensure security.

This paper has primarily addressed only the harbor makeup during times of least vulnerability. Maritime security does exist, and it exists with a layered defense. Warships in particular, are well protected. Normally within a harbor there will be a navy base that has its own protective services. Restricted waters, sectioned off from the civilian population, are

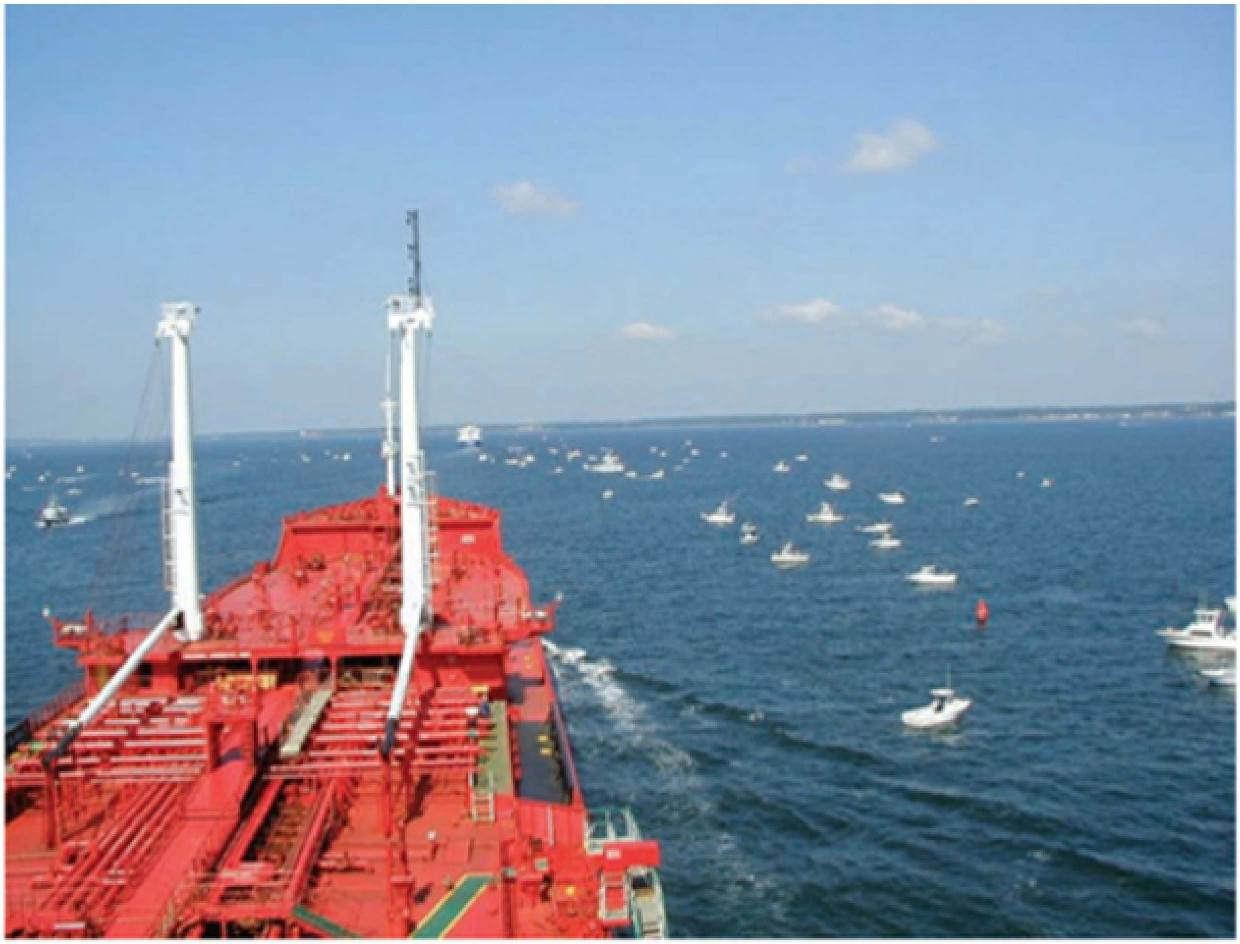


Figure 2.2. An example of harbor or channel traffic[29]

usually protected by multiple security boats patrolling inside a fixed or movable barrier and marked as such on paper and electronic charts.

However, there are times when even warships and crafts are vulnerable. These times of heightened vulnerability were addressed by Muller [12] in 2010 and are listed below:

- Berthed in harbor;
- At anchor;
- During an in-harbor evolution;
- Leaving or entering the harbor;
- In confined passages like a channel.

Additionally, the majority of this document has discussed the maritime attacks from threats taking placing within the confines of harbors, ports, and inland waterways. However, maritime threat locations are not limited to these areas. Unmanned surface vessels could also be used to thwart maritime threats in other areas of vulnerability outside the harbor and coastal waterways. Rivers, straits, vital choke points, and near shore littorals also pose as potential targets for maritime security threats.

Straits and Choke Points

Three particular straits or choke points come to mind when considering vulnerability to maritime security and potential attacks: The Strait of Hormuz, the Strait of Malacca, and the Bab-el-Mandeb Strait. These three straits are critical ”pinch points” that shipping uses to transit extreme quantities of oil and natural gas everyday from the Middle East [30]. These straits are extremely vulnerable to terrorist attacks.

The Strait of Hormuz is the jumping off point for oil transportation from the Middle East. Roughly 17 million barrels of oil transit this strait daily [30]. From there, the shipping diverges to either the Bab-el-Mandeb Strait and the Strait of Malacca.

The Bab-el-Mandeb Strait, from Stevenson [31] in 2018, links the Gulf of Aden to the Red Sea. From the Red Sea, shipping transits the Suez Canal to enter the Mediterranean Sea and beyond. The Strait of Malacca is the major path through which the Far East relies on for oil transport. Shipping transits the Indian Ocean and proceeds to the Strait of Malacca and onward to support economic powerhouses such as China [32], [30].

Littorals

The littoral waters, or those waters just off a state’s coast or shore line, also require maritime security measures. Littorals, as well as straits and choke points, are vulnerable to many types of threats, some only mentioned briefly in this paper. Littoral waters just off coastlines are challenged to defend against piracy, smuggling, drug trafficking and mine warfare in the maritime security spectrum [6].

Many countries continue to attempt to counter terrorist activities in their littoral waters [32]. These littoral threats could be another opportunity for unmanned surface vessels to prove their worth. By successfully employing unmanned surface vessels, these unique threats could easily be neutralized while minimizing the threat to humans [28].

2.2 C-UAS Technology

The rapid expansion of the UAV market has unfortunately resulted in the need to rapidly expand the C-UAS market. The nefarious actors have the capability to cheaply perform malicious acts based on the commonality of inexpensive UAV components and the increasingly accessibility to potential explosive materials [9]. The C-UAS technology is rapidly developing to counter the weaponized threat, but unfortunately there is no ”silver bullet” to thwart the offenders.

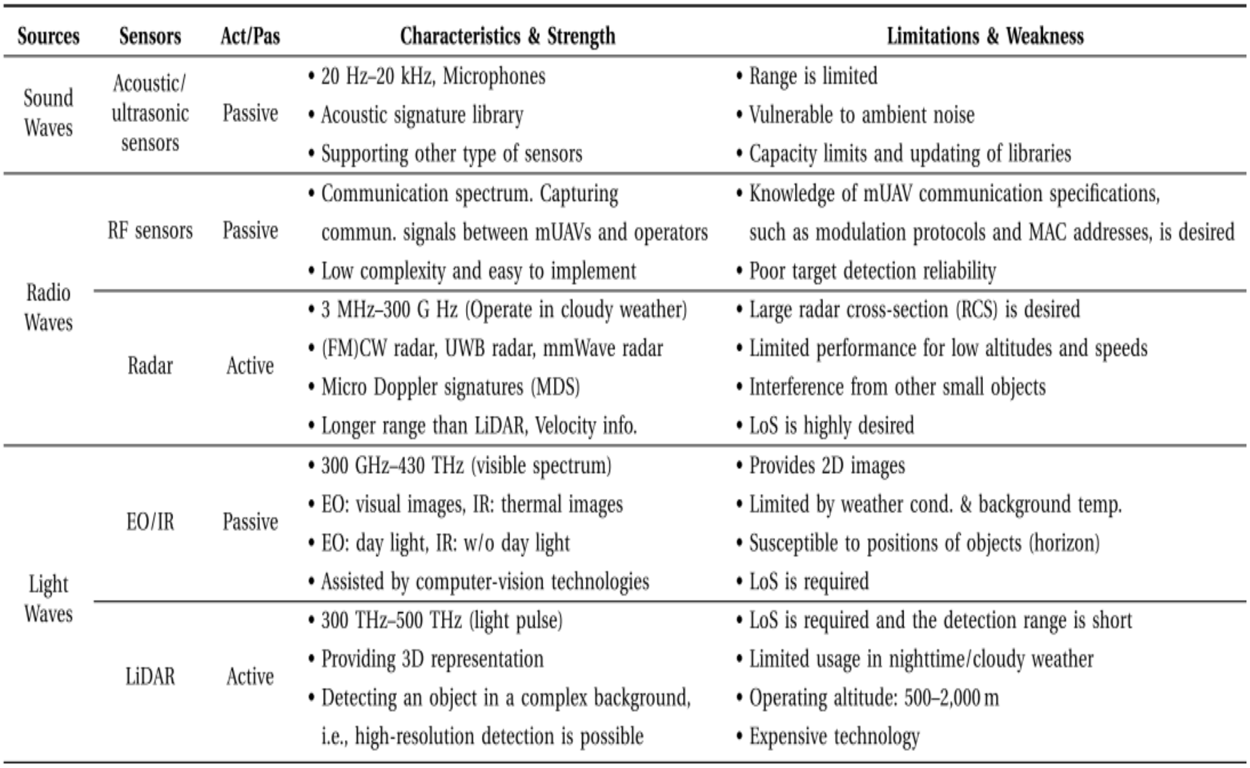
C-UAS technology can be loosely broken down into three categories, consisting of detection or sensing systems, mitigation or interdiction systems, and integration or command and control (C2) systems [9], [11].

2.2.1 Detection and Sensors

Detection systems consist of both active and passive sensors used to gather changes in the environment from sound, radio, and light waves. Acoustic, radio-frequency (RF), radar, electro-optic/infrared (EO/IR), and light detection and ranging (LiDaR). Additionally, S. Park et al. [33] and S. Siewert et al. [34] proposed system that combine sensors utilizing radar, EO/IR and acoustic data respectively. Figure 2.3 from Kang et al [9] shows applicable detection characteristics.

Acoustic

Acoustic sensing systems passively uses microphone or microphone arrays to detect the presence of drones and estimate the direction of arrival [35]. These systems convert sound waves to electrical signals that can be used to not only detect the presence of drones, but quite possibly identify the type of drone based on the acoustic signature. Often the motors produce



Sources	Sensors	Act/Pas	Characteristics & Strength	Limitations & Weakness
Sound Waves	Acoustic/ ultrasonic sensors	Passive	• 20 Hz–20 kHz, Microphones • Acoustic signature library • Supporting other type of sensors	• Range is limited • Vulnerable to ambient noise • Capacity limits and updating of libraries
Radio Waves	RF sensors	Passive	• Communication spectrum. Capturing commun. signals between mUAVs and operators • Low complexity and easy to implement	• Knowledge of mUAV communication specifications, such as modulation protocols and MAC addresses, is desired • Poor target detection reliability
	Radar	Active	• 3 MHz–300 G Hz (Operate in cloudy weather) • (FM)CW radar, UWB radar, mmWave radar • Micro Doppler signatures (MDS) • Longer range than LiDAR, Velocity info.	• Large radar cross-section (RCS) is desired • Limited performance for low altitudes and speeds • Interference from other small objects • LoS is highly desired
Light Waves	EO/IR	Passive	• 300 GHz–430 THz (visible spectrum) • EO: visual images, IR: thermal images • EO: day light, IR: w/o day light • Assisted by computer-vision technologies	• Provides 2D images • Limited by weather cond. & background temp. • Susceptible to positions of objects (horizon) • LoS is required
	LiDAR	Active	• 300 THz–500 THz (light pulse) • Providing 3D representation • Detecting an object in a complex background, i.e., high-resolution detection is possible	• LoS is required and the detection range is short • Limited usage in nighttime/cloudy weather • Operating altitude: 500–2,000 m • Expensive technology

Figure 2.3. Sensor and Detector Characteristics [9]

sounds that can be recognized and many systems attempt to gather the signatures of drones and place them into a database or library [11]. The libraries can be used to not only detect the drone, but attempt to classify them for potential threat analysis and mitigation efforts. While simplicity of microphones and pressure transducers can be beneficial, the limitations include their dependence on weather, ambient noise, and detection range. Additionally , the drone libraries and databases do not have the ability to distinguish all types of drones. These libraries could have difficulties classifying drones in their libraries if they have been altered or are carrying a payload, altering the acoustic signature [9], [11], [14].

Electro-optical and Infrared

Electro-optical and infrared (EO/IR) devices passively detect light waves via EO sensors or heat signatures via thermal cameras that can be utilized in either daylight or at low-light conditions. These sensors have the ability to give either visual images or thermal images of drones in flight and can be assisted by computer-vision technologies [11]. The limitations of this type of detection consist of degraded performance during poor weather conditions or based on background temperatures. Also, the images provided are two-dimensional (2D), limited by line of sight (LoS) and the horizon, and require multiple cameras and sensors to improve the quality and multi-directional detection [9]. F. Christnacher et al. [36] have developed a combination acoustic and optical detection system can better enhance the overall picture better than simply one detection source alone.

Radio Frequency

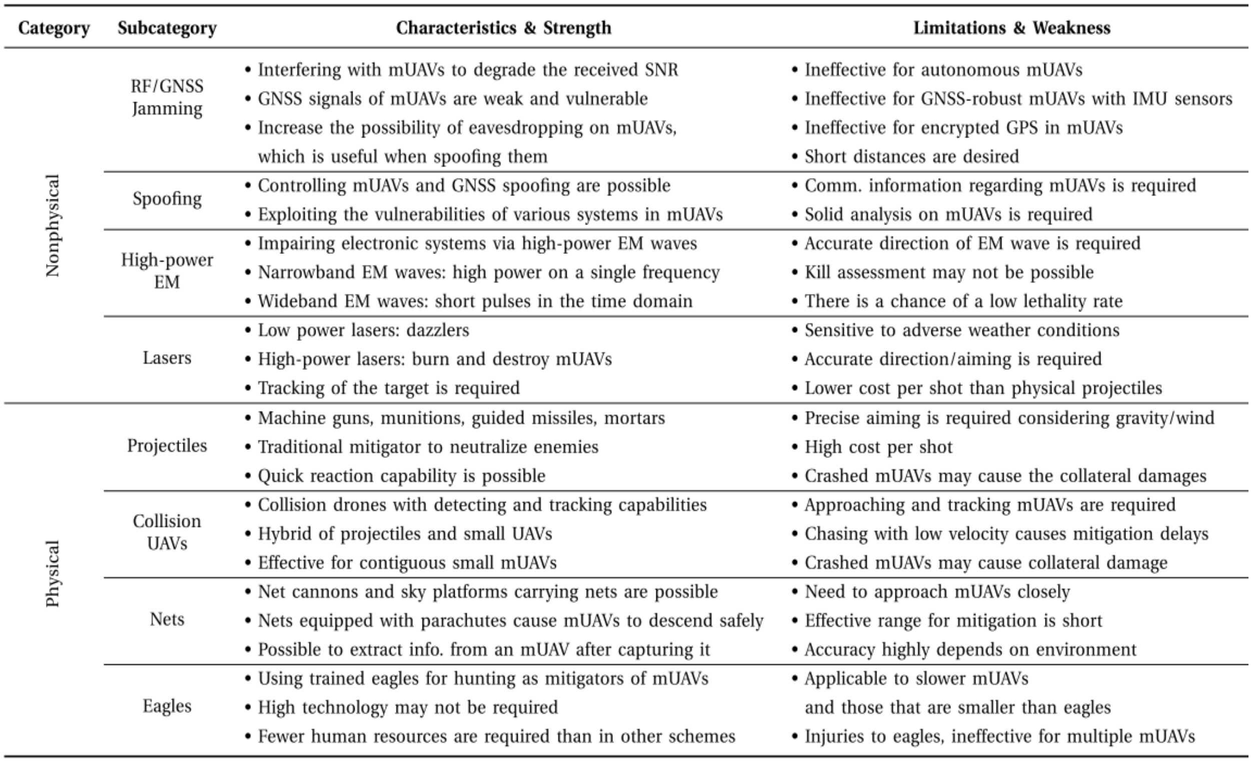
Due to their low computational complexity and relatively easy implementation, radio-frequency (RF) sensors are quite common in all drone detection and mitigation systems. RF sensors passively gather the electro-magnetic (EM) signals and scan for frequencies passed between the drone and the remote controllers [11]. The operators use the EM from the drones for data transfer and maneuvering capabilities. While simple to implement, RF sensors are limited based on their inability to determine range, their poor target detection reliability, high false alarm rates, and the environment's EM interference [9].

Radar

Traditionally designed to detect large manned aircraft at high speeds, radar systems are now being used to attempt to identify drones and their small radar cross-sections (RCS) and slower speeds [9]. Radar is an active process that consists of sending pulses of radio frequency (RF) out towards and object and measuring the reflected signal returns [11]. Radar has the ability to utilize Doppler signatures to detect the presence of drones via false alarms such as birds. The system has a longer range than LiDaR, however clutter is a problem. Other limitations include degraded performance for low altitudes and low speeds [9].

LiDaR

LiDaR sensors provide high-resolution and 3D detection in complex backgrounds. It mirrors radar in application except that it utilizes laser light vice radio frequency. This



Category	Subcategory	Characteristics & Strength	Limitations & Weakness
Nonphysical	RF/GNSS Jamming	• Interfering with mUAVs to degrade the received SNR • GNSS signals of mUAVs are weak and vulnerable • Increase the possibility of eavesdropping on mUAVs, which is useful when spoofing them	• Ineffective for autonomous mUAVs • Ineffective for GNSS-robust mUAVs with IMU sensors • Ineffective for encrypted GPS in mUAVs • Short distances are desired
	Spoofing	• Controlling mUAVs and GNSS spoofing are possible • Exploiting the vulnerabilities of various systems in mUAVs	• Comm. information regarding mUAVs is required • Solid analysis on mUAVs is required
	High-power EM	• Impairing electronic systems via high-power EM waves • Narrowband EM waves: high power on a single frequency • Wideband EM waves: short pulses in the time domain	• Accurate direction of EM wave is required • Kill assessment may not be possible • There is a chance of a low lethality rate
	Lasers	• Low power lasers: dazzlers • High-power lasers: burn and destroy mUAVs • Tracking of the target is required	• Sensitive to adverse weather conditions • Accurate direction/aiming is required • Lower cost per shot than physical projectiles
Physical	Projectiles	• Machine guns, munitions, guided missiles, mortars • Traditional mitigator to neutralize enemies • Quick reaction capability is possible	• Precise aiming is required considering gravity/wind • High cost per shot • Crashed mUAVs may cause the collateral damages
	Collision UAVs	• Collision drones with detecting and tracking capabilities • Hybrid of projectiles and small UAVs • Effective for contiguous small mUAVs	• Approaching and tracking mUAVs are required • Chasing with low velocity causes mitigation delays • Crashed mUAVs may cause collateral damage
	Nets	• Net cannons and sky platforms carrying nets are possible • Nets equipped with parachutes cause mUAVs to descend safely • Possible to extract info. from an mUAV after capturing it	• Need to approach mUAVs closely • Effective range for mitigation is short • Accuracy highly depends on environment
	Eagles	• Using trained eagles for hunting as mitigators of mUAVs • High technology may not be required • Fewer human resources are required than in other schemes	• Applicable to slower mUAVs and those that are smaller than eagles • Injuries to eagles, ineffective for multiple mUAVs

Figure 2.4. Mitigation and Interdiction Characteristics [9]

method of detection is limited in range, is expensive, and is severely limited during almost any negative weather situation. Additionally, line of sight (LoS) is required [9].

2.2.2 Mitigation and Interdiction

Mitigation, some cases referred to as interdiction, consists of intervening in the flight path or mission of threatening sUAS [14]. Mitigation methods consist of either physical or non-physical systems that utilize the EM/RF spectrum, a physical approach, or a combination of the two [9], [11] in an attempt to deny the drone access to vital locations. Kang et al [9] described mitigation and interdiction characteristics and are shown in Figure 2.4.

Non-physical interdiction requires no physical contact. These methods consist of, but are not limited to RF jamming, global positioning system or global navigation satellite system (GPS/GNSS) jamming, spoofing, and directing energy [9], [11]. While these interdiction methods are considered non-physical, they are not entirely low regret. Removing the radio frequency links or other communication capacities can cause the drone to operate in a manner that the mitigator or the drone operator was not expecting. These operations could result in hovering until battery drain, return to home (RTH) over potentially secure facilities, or simply landing/crashing in an undesirable location. These non-physical methods will be discussed throughout this study, weighing both pros and cons.

RF Jamming

RF jamming breaks the communication chain between the sUAS and its operator. This can be completed by multiple methods consists of spot jamming, sweep jamming, or barrage jamming. These methods vary the way that the disruption or disabling occurs. Once the link between the operator and the drone is removed, the drone will complete one of a handful of preset responses, which can include hovering until frequency regained, perform RTH response, or landing in place [9].

RF jamming is an effective way to mitigate standard, commercial-off-the-shelf (COTS) drones being used by inexperienced or negligent operators. However, RF jamming should be considered ineffective against semi-autonomous and fully-autonomous drones that follow waypoint guided routes via GPS/GNSS.[9].

GPS/GNSS Jamming

Similar to RF jamming, GPS jamming disrupts the communication link between the drone and its controlling station. This time, however, the controlling station is via a satellite link that the drone uses for navigation. Sever the link, the drone should again perform certain responses, to include landing, hovering, or performing a RTH functions [10].

While effective against the jamming satellite signals, GPS jammers are vulnerable to drones that possess additional customizations. These customizations can include inertial measurement unit (IMU) sensors and could navigate based on encrypted signals [9]. Many mitigation and interdiction systems utilize a combination of RF/GPS jamming capabilities.

Spoofing

Spoofing enables a mitigation or interdiction system to gain access to and take control of the sUAS. Also known as protocol manipulation, spoof is performed for the purpose of removing the drone from a secure or protected area [11], possibly with or without the operator knowing that it has happened. Spoofing is completed via hijacking either the RF or GPS link, and either manually operating the drone with fake RF signals, or entering spoofed GPS coordinates that the drone and operator unknowingly follow [9].

Spoofing is a great way to exploit the vulnerabilities of various sUAS systems, however the technology required to perform this function must be solid. Much analysis and knowledge of the operating systems is required to not only hack into the drone's systems, but then be able to safely control, guide, or remove the threat from a potentially threatening situation or protected area [9].

Directed Energy

Directed energy toes the line between non-physical and physical mitigation. While technically under the non-physical category, directed energy can physically alter, burn, and destroy a drone. The directed energy category consists of lasers and high power microwaves or electro-magnetic pulses [9].

Lasers consist of both high-power and low-power varieties. Low-power varieties, often call dazzlers, have the ability to disrupt the EO/IR sensors, cameras, and components, rendering that capability useless. High-power lasers, utilizing extremely large amounts of energy, have the capability of burning holes through sensitive components of a drone and causing crash landings [10]. Lasers, however, perform poorly in adverse weather conditions, require both accuracy and time on target, are a significant investment in time and research [9].

High-power microwaves (HPM) and electro-magnetic pulses (EMP) have the ability to impair the electronic components of a drone, disabling them. HPMs fall into two categories, narrow-band and wide-band EM waves. Narrow-band waves are extremely powerful and result in internal failure of the drone and ultimate crash landings. Wide-band waves consist of short pulses of energy that may not produce as high of a lethality rate as the narrow-band waves. These methods require accuracy and appropriate equipment to perform correctly [9].

Kinetic

Kinetic, or physical mitigators, are the exact opposite of non-physical mitigators. These kinetic mitigators require effective, accurate, and lethal physical interactions with the drone to neutralize or destroy the threat. There are multiple methods in use, many more in development, and consist of projectiles, nets, collision-UAVs, and even birds of prey [9], [11].

C-UAV UAVs are an effective way to mitigate threat sUAVs. These mitigators have the ability to dogfight with threatening drones, can perform collision-type mitigations, can launch or drag nets and entangle the rotors of the threat UAV [10], [37], and can even launch projectiles to destroy the drone.

Projectiles, such as machine guns, munitions, mortars, or guided missiles can be employed to destroy drones, however these techniques require accuracy and precision and have a high cost rate, and a high risk of collateral damage if used incorrectly [9], [10].

Eagles or other birds of prey can be used as kinetic means to disable drones. These eagles must be highly-trained and are susceptible to injuries. Additionally, they move slower that other kinetic mitigators [9].

2.3 Department of Defense C-UAS Strategy

In November 2019, based in response to the challenges created by the emergence of sUAS and the associated risks, the Secretary of Defense (SECDEF) placed the Secretary of the Army (SECARMY) as Executive Agent for C-UAS across all activities within the DoD. This appointment enabled SECARMY to establish the Joint C-sUAS Office (JCO) to specifically address all challenges and direct C-sUAS activities. In this role, the JCO will develop a holistic strategy for countering sUAS threats and hazards, streamlining the efforts already in progress by the service branches [13]. The Department of Defense's Counter-Small Unmanned Aircraft Systems Strategy [13] provides Figure 2.5 below.

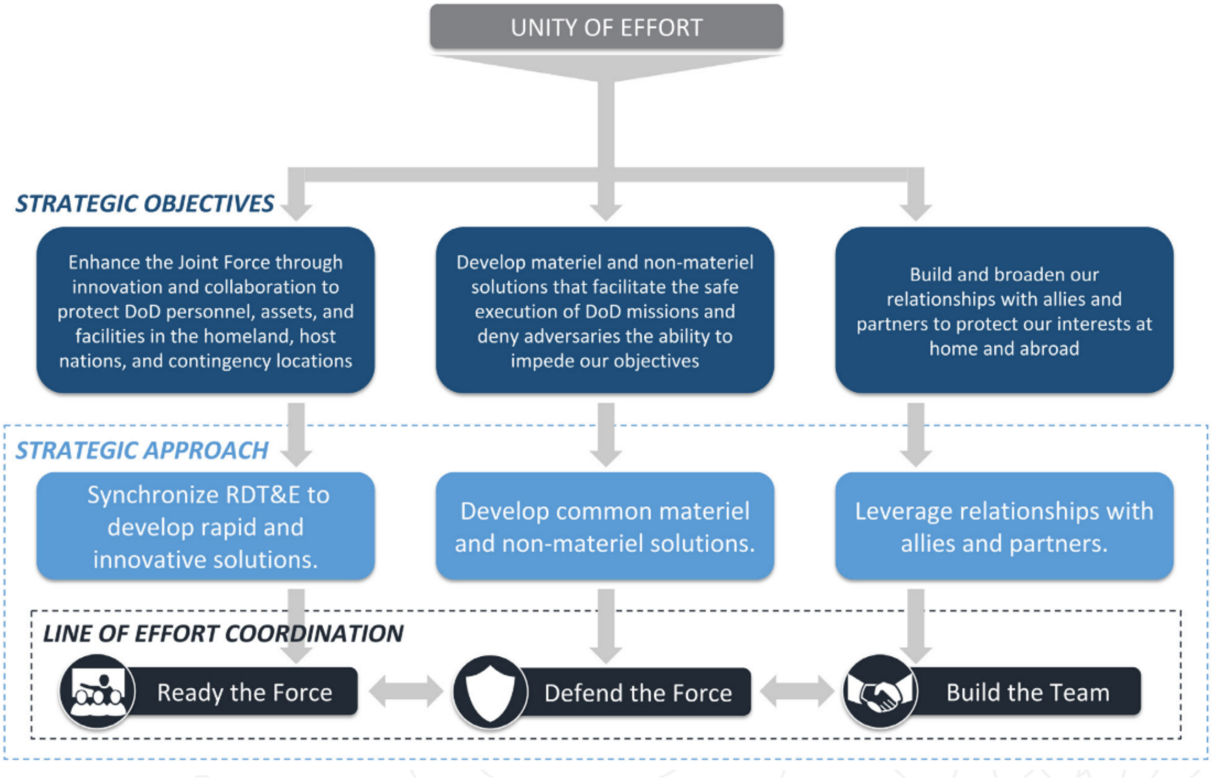

UNITY OF EFFORT
STRATEGIC OBJECTIVES
Enhance the Joint Force through innovation and collaboration to protect DoD personnel, assets, and facilities in the homeland, host nations, and contingency locations
Develop materiel and non-materiel solutions that facilitate the safe execution of DoD missions and deny adversaries the ability to impede our objectives
Build and broaden our relationships with allies and partners to protect our interests at home and abroad
STRATEGIC APPROACH
Synchronize RDT&E to develop rapid and innovative solutions.
Develop common materiel and non-materiel solutions.
Leverage relationships with allies and partners.
LINE OF EFFORT COORDINATION
Ready the Force
Defend the Force
Build the Team

Figure 2.5. C-sUAS Unity of Effort Matrix [13]

2.3.1 Afloat Strategy for Ships

Navy surface combatants are more than capable of defending themselves against enemy threats. These warships are battle-tested and continue to adapt to the ever-changing technological revolutions going on in advanced warfare and weaponry. That being said, there are concerns about the survive-ability of surface ships during a conflict with a near-peer adversaries with advanced weaponry, to include a surplus missile inventory, drone or swarm strategy, and the opportunity [38].

There are concerns regarding the size of naval ships, the distribution of naval ships in the fleets, and the danger of operating in waters where adversaries have the ability to overwhelm air defense platforms with missiles and sUAS. Additionally, the defense of surface ships is limited by the depth of magazines and by extremely unfavorable cost exchange ratios [38]. The enemy must simply have one more drone that the defender has missiles, birds, lasers, etc. Similar to challenges presented to the commercial C-UAV market, sUAVs are relatively cheap and C-UAV systems are expensive and always one step behind the threat. Trading million-dollar missiles for thousand-dollar drones will bankrupt a country.

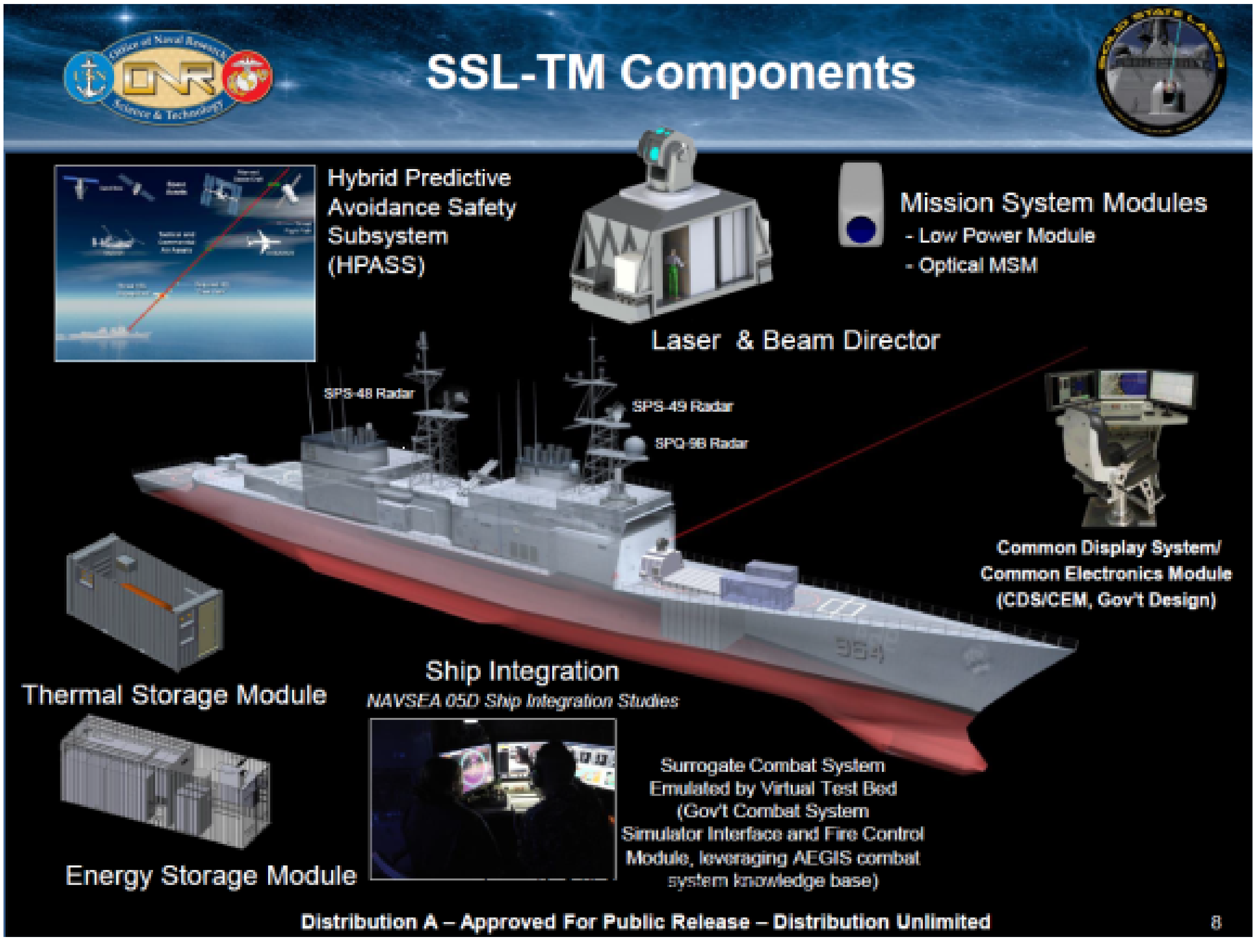
These concerns have caused the Navy to find a way to extend the depth of magazines and lessen the tab per shot required to counter missiles and sUAVs. The significant efforts to employ high-energy steady-state lasers (SSL) onboard Navy ships is coming to fruition. The Navy is attempting to combat threat UAVs by multiple methods to include, but not limited to dazzling intelligence, surveillance, and reconnaissance (ISR) sensors, to physically destroying sUAVs or small boats, and potentially even using lasers for countering enemy missiles [38].

Shipboard Systems in Development

Many current systems onboard United States Navy's surface ships are more than capable of combating a threat from sUAVs, but there is a significant gap in the capabilities and questions regarding whether or not they should be used for that purpose [39]. The Navy currently has three lasers in production and with attempts and trials onboard Navy ships happening at this time. These three more-capable lasers include the Solid State Laser Technology Maturation (SSL-TM) effort; the Optical Dazzling Interdictor, Navy (ODIN); the Surface Navy Laser Weapon System (SNLWS) Increment 1, also known as the high-energy laser with integrated optical dazzler and surveillance (HELIOS). These three efforts above are included in what the Navy calls the Navy Laser Family of Systems (NLFoS) effort and will be discussed in greater detail below. [38].

SSL-TM

The Navy's Steady State Laser- Technology Maturation (SSL-TM) Program has provided the fleet with a new capability that can combat UAV at sea without utilizing the traditional weapons used to defend the ship. The use of traditional ship self-defense weapons such as the Close-in Weapons System (CIWS) and Standard Missiles (SM) are not recommend for use against drones due to the unfavorable cost exchange and due to the depth of magazines



SSL-TM Components

Hybrid Predictive Avoidance Safety Subsystem (HPASS)

Laser & Beam Director

Mission System Modules
- Low Power Module
- Optical MSM

SPS-48 Radar

SPS-49 Radar

SPQ-9B Radar

Common Display System/
Common Electronics Module
(CDS/CEM, Gov't Design)

Thermal Storage Module

Ship Integration
NAVSEA 05D Ship Integration Studies

Energy Storage Module

Surrogate Combat System
Emulated by Virtual Test Bed
(Gov't Combat System
Simulator Interface and Fire Control
Module, leveraging AEGIS combat
system knowledge base)

Distribution A – Approved For Public Release – Distribution Unlimited 8

Figure 2.6. Steady State Laser- Technology Maturation Components [38]

onboard the ships. SSM-TM has the potential to be the go-to weapon against asymmetric threats, such as sUAS, small boats, and other ISR threats [38]

The 150-kilowatt weapon was installed onboard USS PORTLAND (LPD 27) in 2019 and has successfully disabled a UAV during an at-sea test in 2020. The platform and program will inform future acquisition strategies, system designs, integration architectures, and fielding plans for laser weapon systems [38]. Figure 2.6 is a graphic describing SSL-TM components from O'Rourke [38].

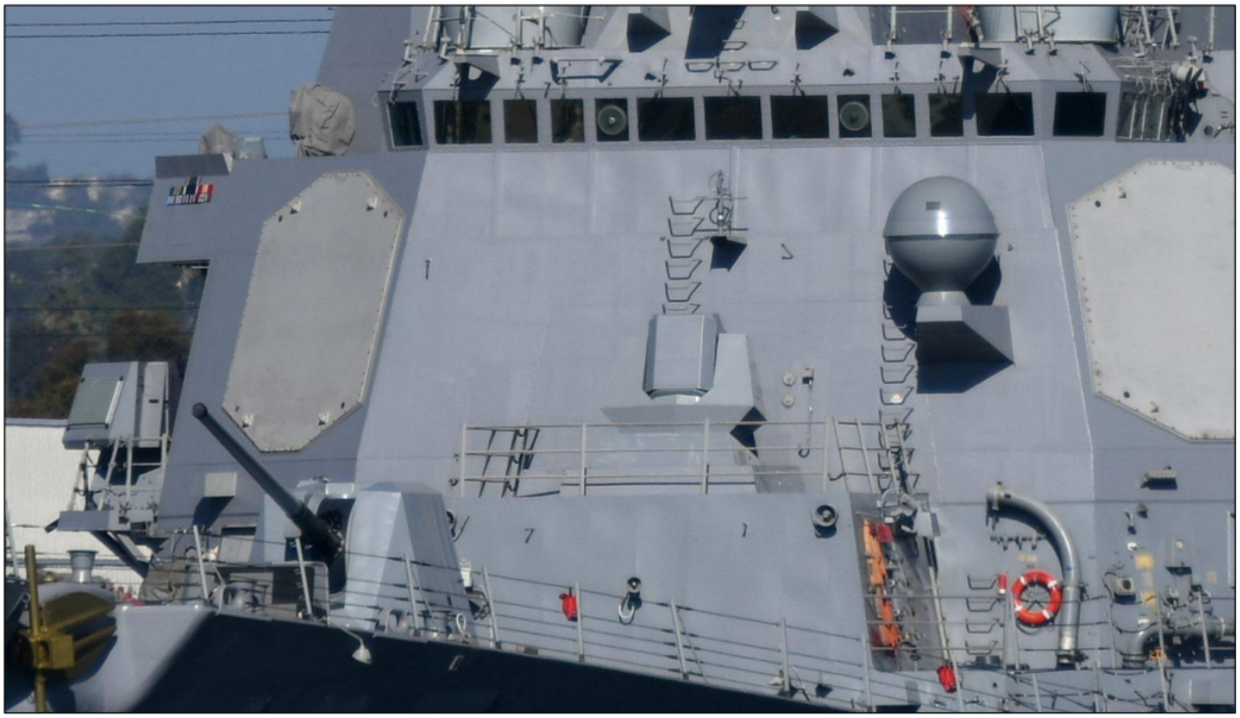


Figure 2.7. ODIN onboard USS DEWEY (DDG 105) [38]

ODIN

Unlike SSL-TM, Optical Dazzling Interdictor, Navy (ODIN), is a laser dazzler that degrades the ISR capabilities of UAVs. This is not a weapon that disables or destroys a drone. This system degrades or scrambles the optical sensors of a sUAV, thereby rendering it useless for its intended use. Without the ability to gather intelligence, navigate, or target, the threat UAV will loses its way and ultimately crash [38].

ODIN was installed aboard an active destroyer, USS DEWEY, DDG 105, in 2019 as seen in Figure 2.7 by O'Rourke [38]. This system is the first operation deployment of a laser dazzle as a stand-alone system. This program will also inform the leaders for future acquisitions and C-UAS strategies [38].

HELIOS

The Surface Navy Laser Weapon System (SNLWS) Increment 1, also known as the high-energy laser with integrated optical dazzler and surveillance (HELIOS), is somewhat of a combination of both SSL-TM and ODIN. HELIOS is currently focused on fielding a high-energy laser and dazzler integrated system. The ability to both dazzle and destroy sUAV, small boats, and ISR sensors solves issues with the capability gaps of current onboard systems [38].

One significant difference with this program and weapons system is that it is integrated into current shipboard combat systems. The fact that it is not a stand alone system ensures that the combat identification and battle damage assessments can give commanding officers a better picture of the current battle situation and enable them to make educated decisions. The expected delivery of the HELIOS system to the fleet will be late 2021 onboard an operational DDG-51 Class Destroyer as shown in Figure 2.8 by O'Rourke [38].

2.3.2 Ashore Strategy for Ships

The majority of this study will be conducted determining the ashore strategy for ships in port. At the present time, there are not many options for watchstanders onboard naval vessels while pierside. Small arms, such as M4 rifles, 12 gauge shotguns, and 9mm Beretta handguns make up the standard arsenal available for import duty watchstanders.

M4

The standard M4 service rifle is the long-range weapon of choice for top-side watchstanders onboard US Navy vessels. The effective range of this rifle is 500 - 600 meters. Standard shooters can expect to successfully engage targets from 25 - 300 meters, while military personnel with adequate marksmanship training should be capable of reaching out and touching something at closer to 600 meters, given the right environmentals [40]

This rifle has multiple modes of operational fire, to include semi-automatic mode, three round burst mode, and automatic mode. The M4 is fairly lightweight, especially when

Figure 2.8. HELIOS System on DDG-51 Destroyer [38]

compared to its predecessor, the M16. Multiple configurations and attachments can be installed, to include optics, illuminators, and the fire-control systems, to be discussed in the next section [40].

Smart Shooter - SMASH

An Israeli-based company named Smart Shooter has successfully created SMASH, a state-of-the-art fire-control system that can mount on to standard weapons to significantly improve the successful engagement of hard to kill drone threats. The system is designed to improve watch stander accuracy and minimize collateral damages to friendlies and civilians alike [41].

Functionally, the system operates by gaining a fire control solution and firing when ready to ensure a ”one shot, one kill” solution. The watch stander will gain the threat in the

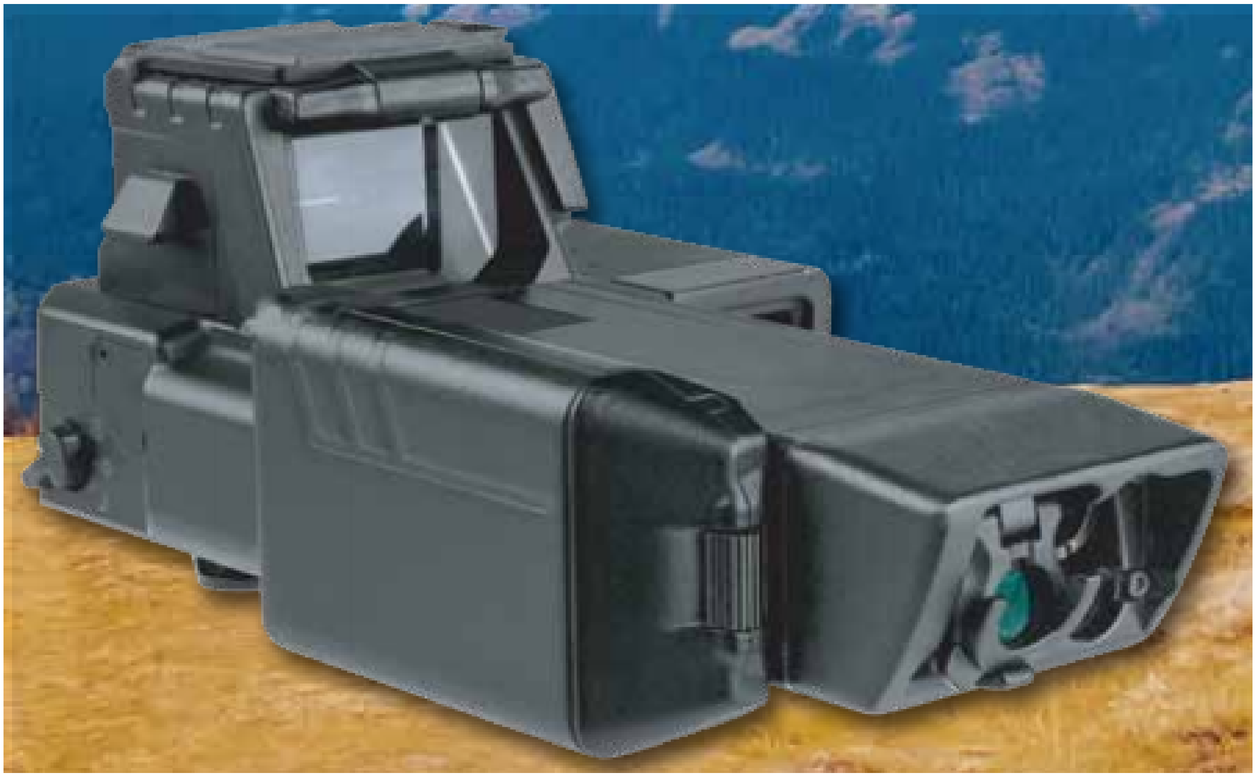
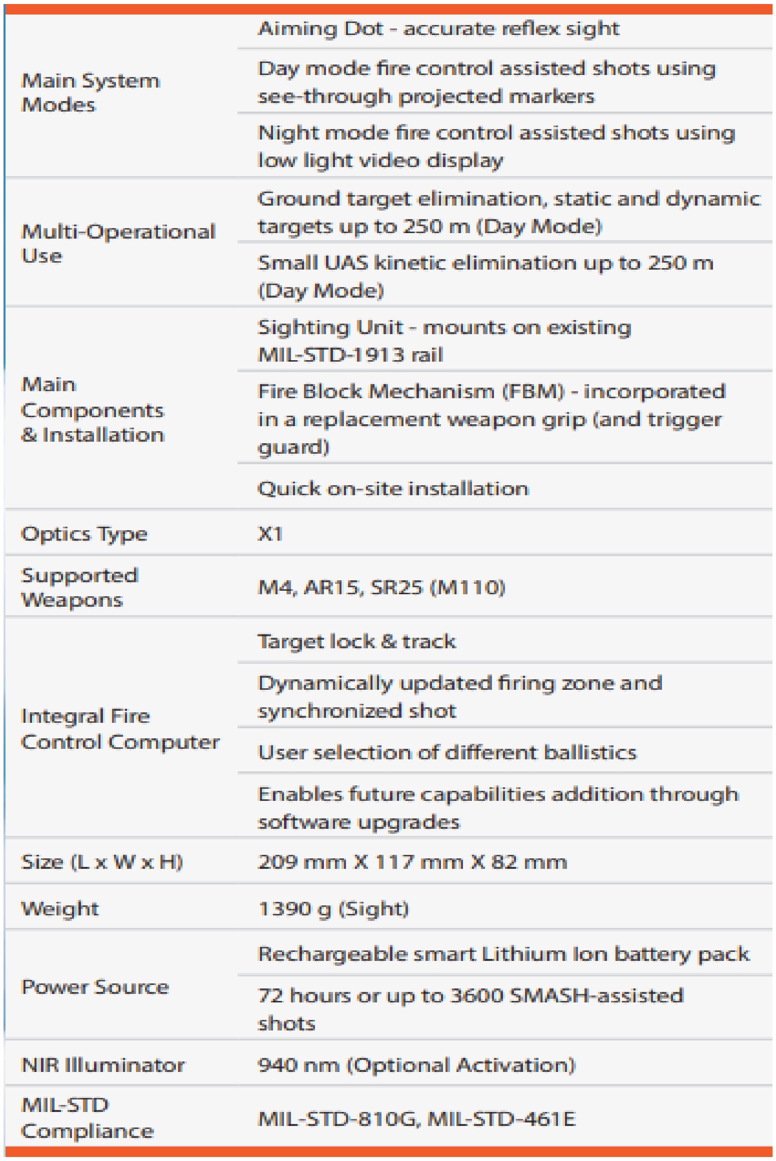


Figure 2.9. SMASH [41]

detection system and pull the trigger. A piston holds the trigger in place until a correct solution can be processed. Upon confirmation of a believed-successful mitigation, also known as ”locking on,” the piston clears, enabling the trigger to be pulled, thereby firing the rifle [41].

In 2020, the US Army and Secretary of Defense conducted supervised live fire testing of the Smart Shooter technology [42] and later announced that they had selected the system as an interim C-UAS moving forward based on previous assessment results. Smart Shooter technology was one of three dismounted or handheld systems selected in an attempt to further develop the a systematic defense against threat UAVs [43].

A goal of this study is to determine the effectiveness of low-regret, low collateral damage weapons to arm watchstanders with in order to protect the ship with little to no time to react. The Israeli company Smart Shooter has a fire-control system that enables small arms to become more effective via their proprietary target acquisition and tracking algorithms.



Main System Modes	Aiming Dot - accurate reflex sight
	Day mode fire control assisted shots using see-through projected markers
	Night mode fire control assisted shots using low light video display
Multi-Operational Use	Ground target elimination, static and dynamic targets up to 250 m (Day Mode)
	Small UAS kinetic elimination up to 250 m (Day Mode)
Main Components & Installation	Sighting Unit - mounts on existing MIL-STD-1913 rail
	Fire Block Mechanism (FBM) - incorporated in a replacement weapon grip (and trigger guard)
	Quick on-site installation
Optics Type	X1
Supported Weapons	M4, AR15, SR25 (M110)
Integral Fire Control Computer	Target lock & track
	Dynamically updated firing zone and synchronized shot
	User selection of different ballistics
	Enables future capabilities addition through software upgrades
Size (L x W x H)	209 mm X 117 mm X 82 mm
Weight	1390 g (Sight)
Power Source	Rechargeable smart Lithium Ion battery pack
	72 hours or up to 3600 SMASH-assisted shots
NIR Illuminator	940 nm (Optional Activation)
MIL-STD Compliance	MIL-STD-810G, MIL-STD-461E

Figure 2.10. SMASH Data [41]

These solutions potentially give watchstanders the ability to maximize effectiveness during time-critical situations and can easily be implemented onto existing Navy weapons.

Other options for import ship self-defense include potentially novel ideas, to include but not limited to shoulder/hand-held RF devices, confetti cannons, water jets, camouflage, Mylar netting with weather balloon or projectile assistance.

Installation/Base Systems

Navy bases and installations currently do not have the capability to defend against sUAS effectively. Commercially available sUAS are a significant threat to military bases in the United States and abroad. Military bases are not prepared to combat these threats simply because they bases were not designed or prepared for such an asymmetric threat. Long gone are the days of anti-aircraft weapons due to the fact that our bases maintain air superiority. That may not be the case anymore with the emergence of sUAS [44].

The fact that there is no ”silver bullet” to combat sUAS threats requires a layered defense, or defense in depth [44]. Geo-fencing is a preventive measure currently used at naval bases, airports, and prisons, but it is easily defeated an should not be considered as effective. It is a deterrent to negligent and accidental access at best. Improved detection, organized command and control systems (C2), and cost-effective mitigation or interdiction techniques must be utilized to extend the perimeter of any base or facility [45].

Naval bases and installations typically have either security towers or air traffic controlling towers with which the base can have an understanding of what is going on in the air space. This is either used to control, protect, and safely operate aircraft. These systems are not prepared or capable of defending or protecting the operations, facilities, and personnel from sUAS threats without a rapid adoption and capability improvements of C-UAS systems. The technological advances and capabilities of sUAS requires immediate attention [44].

2.4 AnyLogic Simulation Modeling Software

AnyLogic is a simulation modeling software that enables real world problems to be addressed quickly and efficiently. Instead of performing actual experiments that can be too expensive, too dangerous, or too time consuming, AnyLogic allows the users to create abstract models that accurately represent the original systems.

There are two types of models used currently, analytical and simulation models. Analytical models can be sometimes be referred to as spread-sheet based modeling, using software such as Microsoft Excel. This system can work for many experiments, but lacks the dynamic aspects of simulation modeling. Simulation modeling, such as what is used in AnyLogic, provides executable models or experiments that utilize multiple functions to produce the user's desired outputs.

Inside the simulation aspects of AnyLogic, the software utilizes three "methods" or frameworks for model development. These methods are system dynamics, discrete event modeling, and agent-based modeling. Grigoryev [46] illustrated these methods in Figure 2.11 and shows the varying amount of abstraction as chosen by the user. It is the simulation method referred to as agent-based modeling that will be addressed further [46].

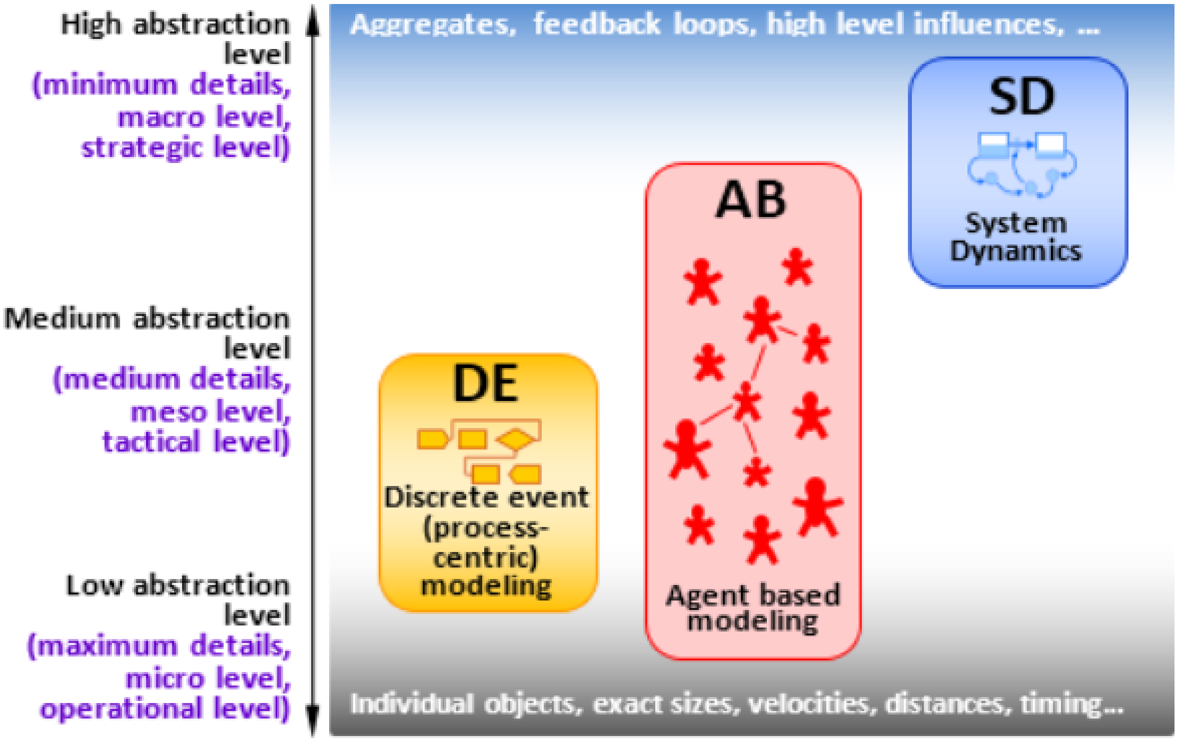

High abstraction level
(minimum details, macro level, strategic level)
Medium abstraction level
(medium details, meso level, tactical level)
Low abstraction level
(maximum details, micro level, operational level)
Aggregates, feedback loops, high level influences, ...
SD
System Dynamics
AB
Agent based modeling
DE
Discrete event (process-centric) modeling
Individual objects, exact sizes, velocities, distances, timing...

Figure 2.11. Methods of simulation modeling [46]

2.4.1 Agent-based Modeling

Agent-based modeling is a fairly new type of event modeling and has become relevant due to the improvements in computer sciences, mainly the advances in computer processors and memory. Agent-based modeling using agents, state charts, flowcharts, and other various functions to make experiments based on defined sets of rules created by the users [46].

Agent-based modeling can serve as an appropriate venue to test maritime security policies and techniques. Technical data can be inserted into a model to represent sensors, threat capabilities, unmanned aerial vehicles, and different harbors, ports, and facilities. Modeling would serve to validate which type of system mix may be most beneficial based on threats. Additionally, the models provide data to further revise current maritime security policy involving maritime threat characteristics and locations. Once a model is built, it can be used to validate the security procedures of a port, harbor, or base, while different scenarios can be used to test and refine security policy and C-UAS defenses.

2.4.2 Previous C-UAS Research using AnyLogic

There have been instances of AnyLogic simulation modeling being used in the past to research C-UAS defense. The work was performed by Cline and Dietz [14] from Purdue University in an attempt to assess the capabilities of a C-UAS system's ability to deter threatening drones in and about prison yards. The threat drones were being utilized to drop drugs, cell phones, and paraphernalia over the fences of the prisons for the prisoners to pickup without the authorities detection. Figure 2.12 shows the physical prison representation from that model.

The authors were able to utilize several assumptions from hypothetical detection and mitigation systems as inputs into the model. Once the model was developed, randomized flight paths and flight speed dependent variables were inserted to test their hypothesis. The authors were able to analyze the outputs and determine the probability of interdiction resulting from increasing the speed of a C-UAV UAV against the static speed of the threat UAV [14].

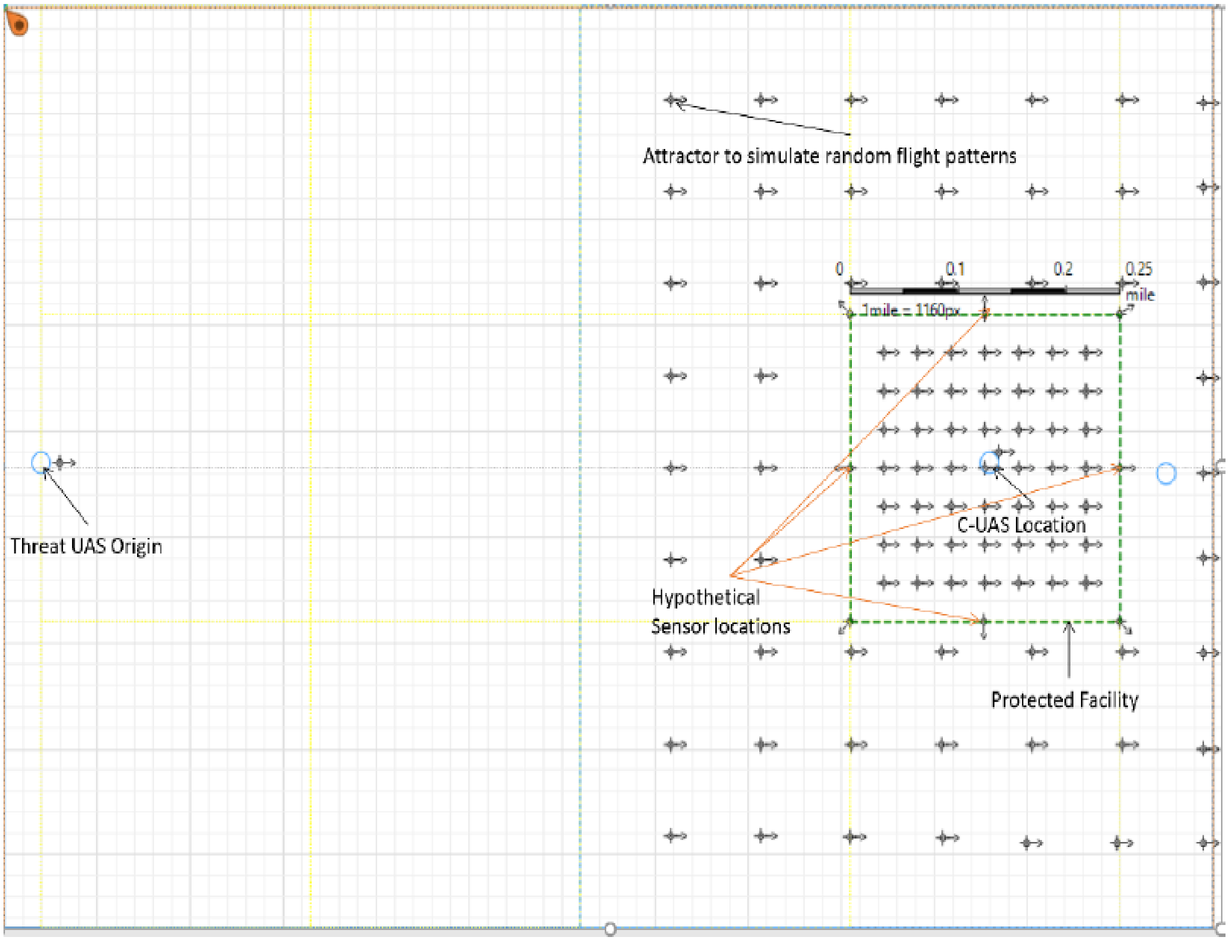


Figure 2.12. Example of previous work using AnyLogic for C-UAS [14]

3. METHODOLOGY

3.1 Research Framework

This research utilizes a parametric-driven approach based on a hypothetical detection system and enhanced watch stander capability to successfully defend a high value unit (HVU) positioned on a naval installation from attack from an autonomous sUAV.

This research paper will utilize agent-based modeling software for adjusting and determining parameters that could lead to successful maritime security or port security defenses. This research will assume naval installation detection platforms and mitigation techniques based on proposed sensor data and developmental and in-place interdiction systems. The inability to field test a comprehensive detection, tracking, and interdiction system for threats is the reason AnyLogic modeling software will be used. Expense, risk and time are essentially unrealistic when attempting to perform these tests live [47]. This software can affordably, effectively, and quickly assist in the development of real-time solutions to real-time problems.

The model will be based on the hypothetical harbor monitoring sensor performance data and an assumed autonomous, weaponized sUAV threat. Variables within these simulations will consist of altering the speed and approach trajectories of a weaponized sUAV threat. Additionally, variable watchstander response times will potentially influence the success rate. The mitigation method utilized by watchstanders will be of the kinetic variety and will consist of standard-issue M4 rifles and standard-issue M4 rifles with Smart Shooter's SMASH system integration. This high likelihood of success with low likelihood of collateral damage makes the M4 SMASH system a viable option for C-UAS defense.

Since the autonomous, weaponized sUAV will be in fact weaponized, the goal of the simulation is to detect and safely mitigate the drone prior to reaching the high value unit (HVU). The simulation will provide data to include time to detection, mitigation success, time to mitigation, time of watch stander response, and distance to ship before mitigation, if applicable. The AnyLogic model project, from which all modeling and configuring was performed, can be seen in Figure 3.1

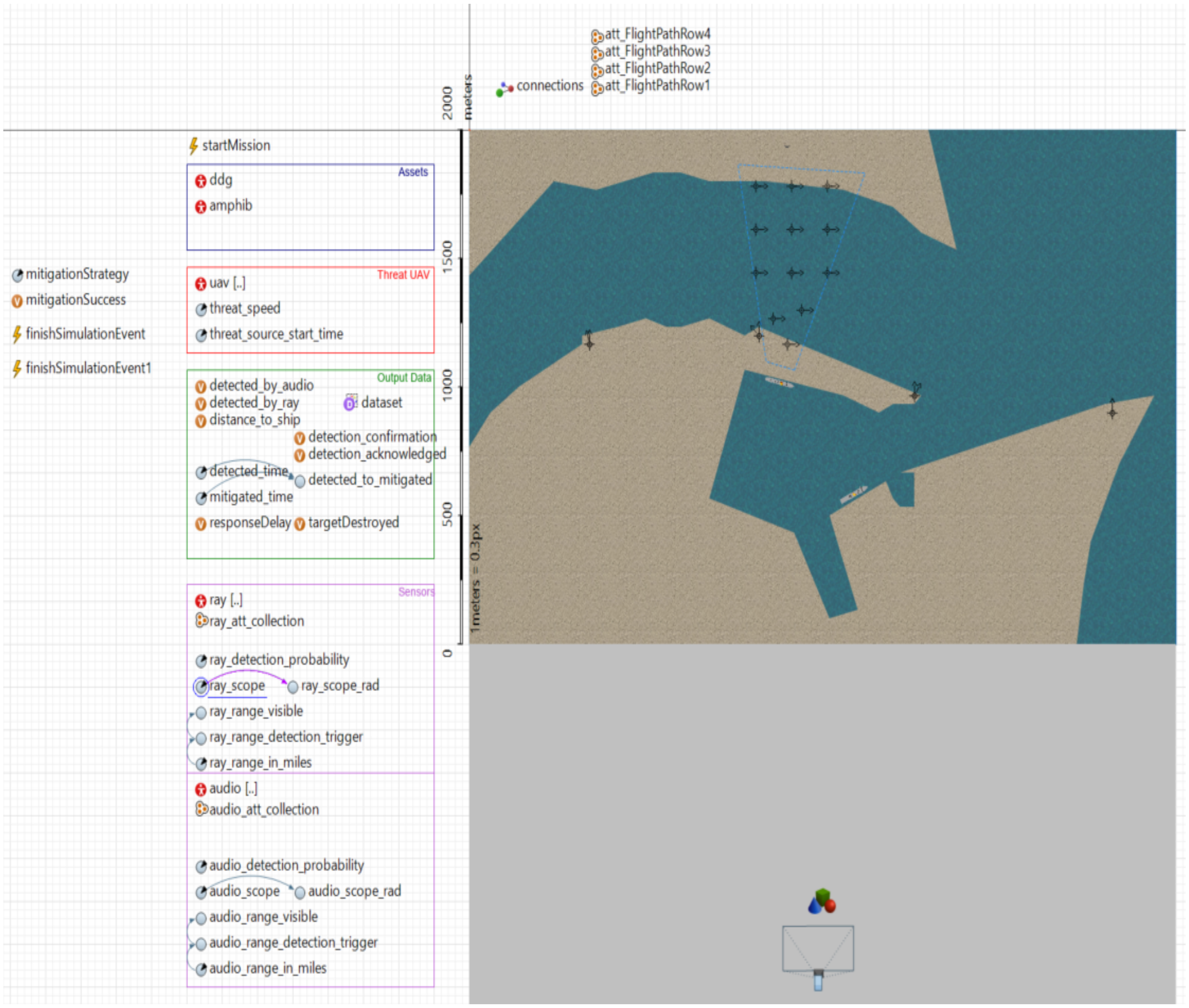


Figure 3.1. AnyLogic simulation model project [48]

3.2 Simulation Attributes

The model characteristics are determined via extensive literature review, subject matter expert (SME) consulting, and real-life, real-time field data gathered. Additionally, some assumptions will be made based on the lack of white paper material, classification levels, and accessibility. The model will use performance metrics that are have been utilized in the past to measure system effectiveness. The probabilities, times, and locations of detection, tracking, assessment, and mitigation will be utilized to evaluate the performance of the model [49].

3.2.1 Harbor Simulation Attributes

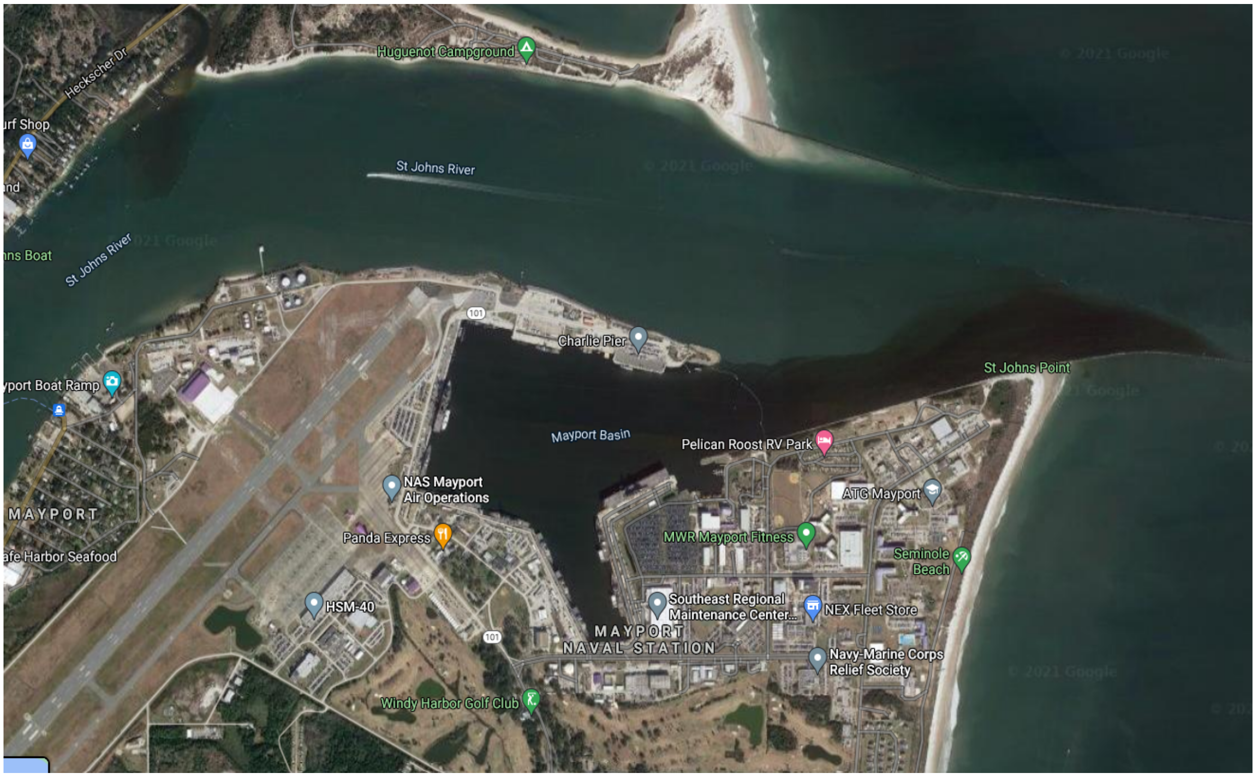


Figure 3.2. Naval Station Mayport [48]

The physical location in which the harbor model will be based on will be Naval Station Mayport, located 15 miles east of Jacksonville, Florida. A satellite image of Naval Station Mayport can be seen in Figure 3.2. Naval Station Mayport performs as both a naval seaport, as well as an air facility. The base is home to several operational and logistical support commands, as well as approximately 15 home-ported ships from the United States Navy, United States Coast Guard, and the Military Sealift Command [50].

There are several possible sites just outside of base for nefarious actors to take launch from, to include nearby beaches, restaurants, and the St. Johns River. The St. Johns River shares the open ocean access point with the ships basin. This close proximity to cargo, shipping, and leisure vessels provides additional threats. The AnyLogic Model representation of Naval Station Mayport can be seen in Figure 3.3.

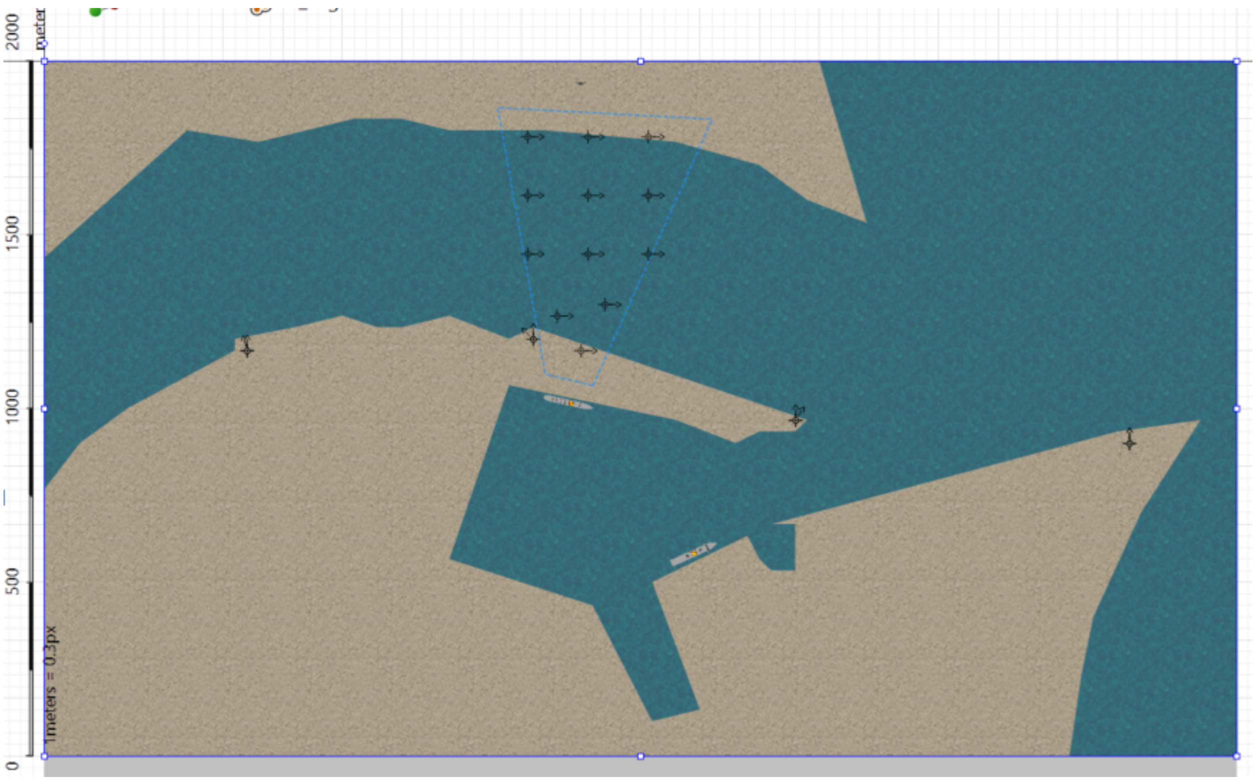


Figure 3.3. Naval Station Mayport Main Agent Replication

3.2.2 Drone Simulation Attributes

The threat quadcopter was chosen as a representation of how a non-COTS, cheap, easy to construct, autonomous-capable platform would perform under given variables. To build and operate an equivalent platform would require at minimum a 500 dollars material cost and a high school level of education. The fact that this drone can be effective while being created mostly via parts made from a 3D printer should be a cause for concern. COTS drones have the ability to be traced via receipts, credit card transactions, FAA-required drone registration, and even commercial surveillance cameras.

The threat specifications include a maximum autonomous speed of 40 mph, 915 mHz control link proven to 30+ miles of range, approximately two pound payload capacity, and flight time of anywhere between 5-15 minutes, dependent on the environmentals and mission variables. These threat characteristics are comparable to drones utilized in similar studies.

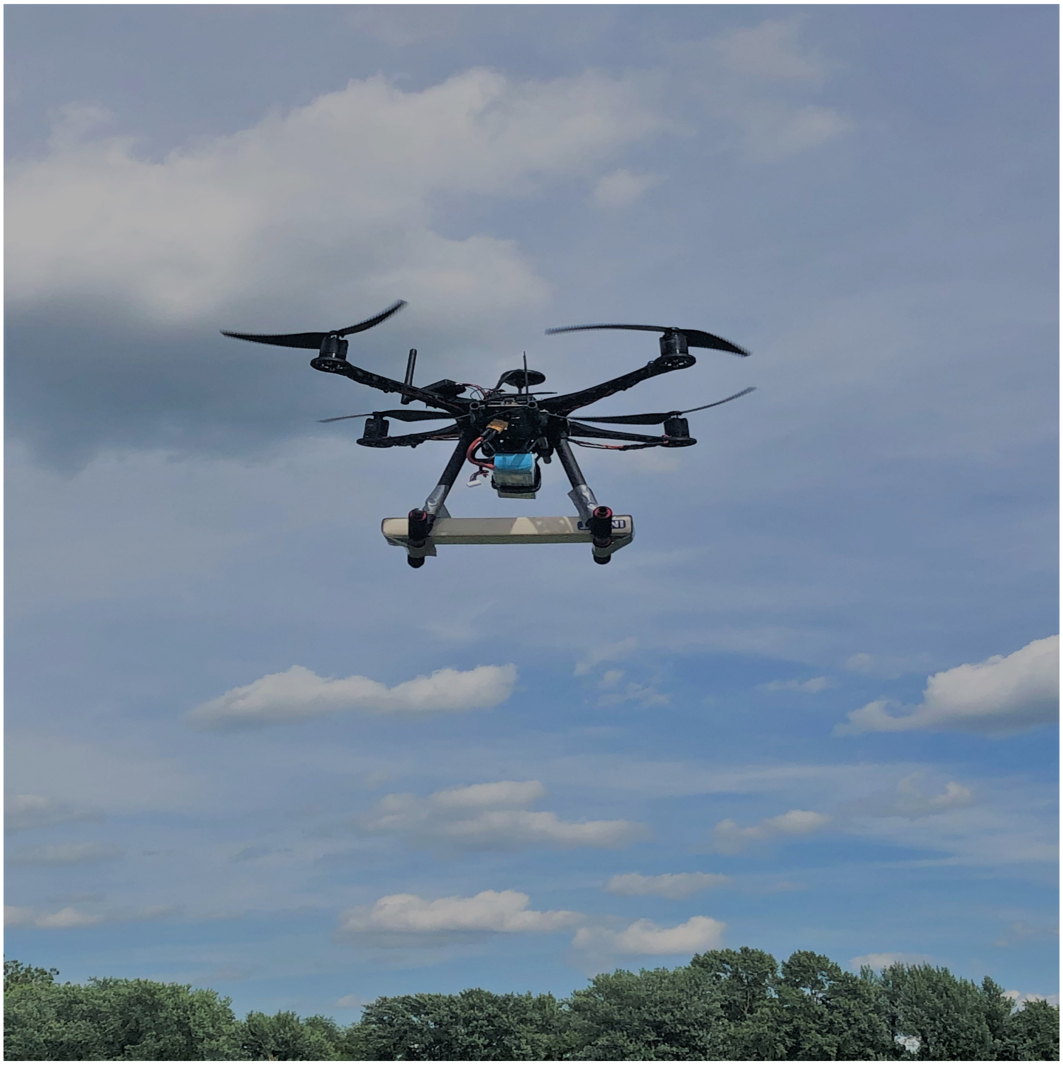


Figure 3.4. Weaponized threat UAV in flight

Physical dimensions, speed, and payload capacity are consist with what subject matter experts believe would be a viable threat.

The aircraft is capable of waypoint navigation, and could be simply modified to run off computer vision-based navigation. The aircraft is capable of autonomously launches. With no operator input, the threat could strike a target greater than three miles away with relatively high accuracy. The threat quadcopter can be see in Figure 3.4.

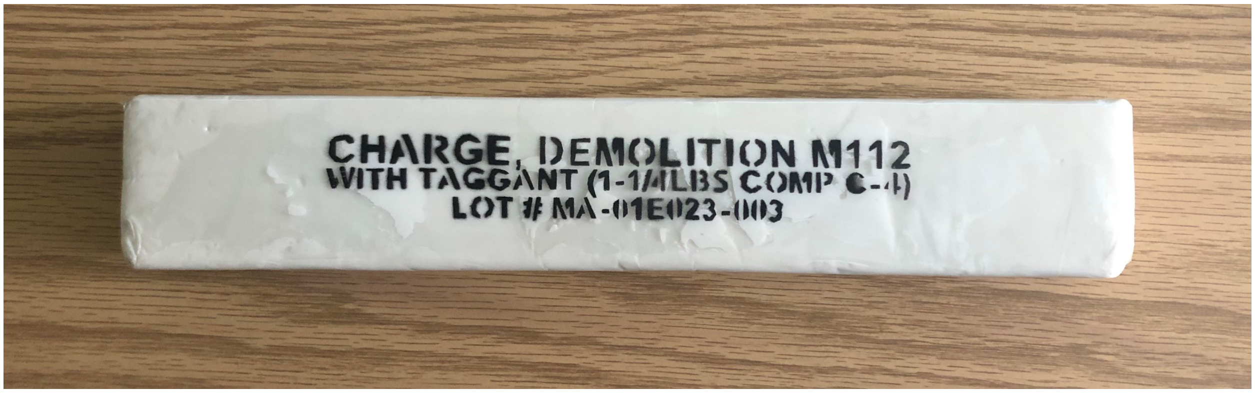


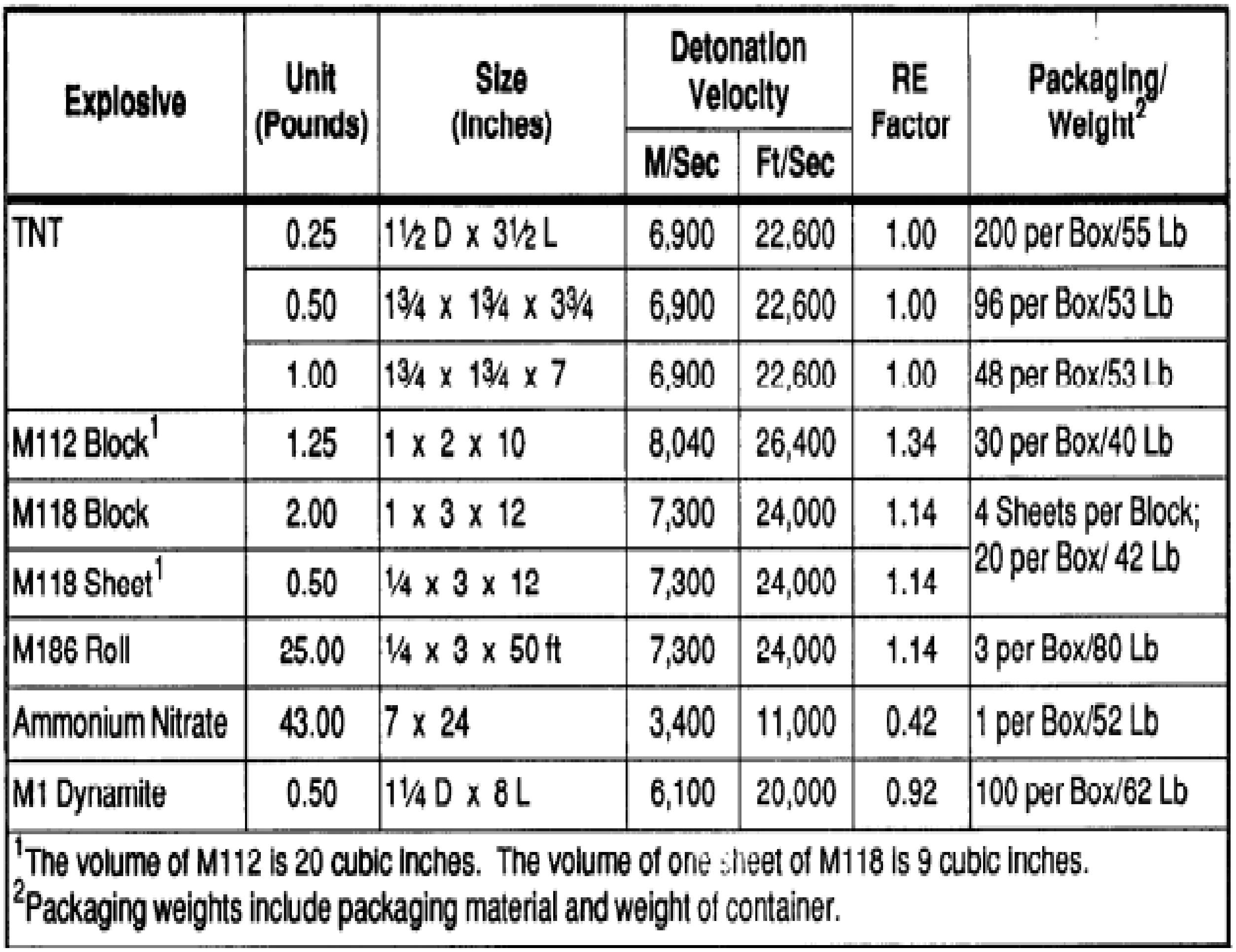
Figure 3.5. M112 block demolition charge

Drone Haul

Composition C4 (C4) has been the explosive of choice for terrorists for many years. Examples include the 2018 assassination attempt of Venezuelan President Maduro [9], [14] and multiple Mexican cartel attacks along the United States' southern border. The method of attack for the assassination attempt was a DJI M600 drone carrying C4 explosives. The Mexican cartel uses C4 with ball bearings to provide the effect of an enormous shotgun blast [51].

C4 is a fairly common and accessible composite explosive that when used appropriately, is extremely effective for general demolition purposes. The standard M112 block demolition charge, as seen in Figure 3.5 and characterized in Figure 3.6, is malleable, more intense than TNT, and can be cut and shaped for uses such as blowing bridges and cutting steel [52]. This steel cutting capability and the fact that the M112 charge is readily available are reasons why they are being utilized in attacks, and this study.

In this simulation, either one or two M112 block demolition charges, allowing variables for different attack speeds, will be attached to the bottom of the drone and will make up the threat payload for the suicide drone.



Explosive	Unit (Pounds)	Size (Inches)	Detonation Velocity		RE Factor	Packaging/ Weight[2]
			M/Sec	Ft/Sec		
TNT	0.25	1½ D x 3½ L	6,900	22,600	1.00	200 per Box/55 Lb
	0.50	1¾ x 1¾ x 3¾	6,900	22,600	1.00	96 per Box/53 Lb
	1.00	1¾ x 1¾ x 7	6,900	22,600	1.00	48 per Box/53 Lb
M112 Block[1]	1.25	1 x 2 x 10	8,040	26,400	1.34	30 per Box/40 Lb
M118 Block	2.00	1 x 3 x 12	7,300	24,000	1.14	4 Sheets per Block; 20 per Box/ 42 Lb
M118 Sheet[1]	0.50	¼ x 3 x 12	7,300	24,000	1.14	
M186 Roll	25.00	¼ x 3 x 50 ft	7,300	24,000	1.14	3 per Box/80 Lb
Ammonium Nitrate	43.00	7 x 24	3,400	11,000	0.42	1 per Box/52 Lb
M1 Dynamite	0.50	1¼ D x 8 L	6,100	20,000	0.92	100 per Box/62 Lb

[1]The volume of M112 is 20 cubic inches. The volume of one sheet of M118 is 9 cubic inches.
[2]Packaging weights include packaging material and weight of container.

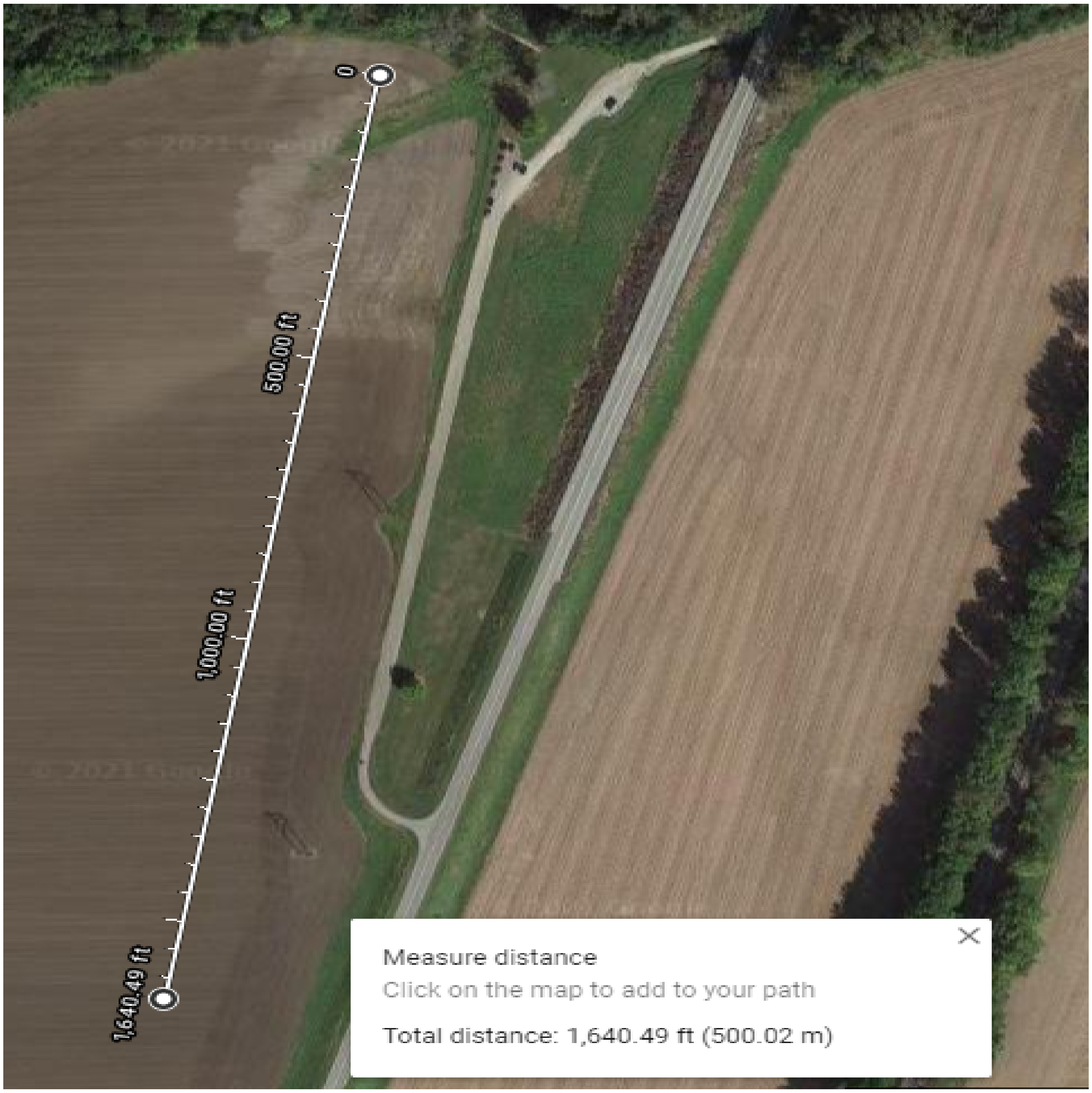
Figure 3.6. Characteristics of block demolition charges [52]

Drone Maneuverability Trial

Drone stability and maneuverability trials were conducted to determine the speed, distance of travel, and length of time airborne based on battery discharge with variably-weighted payloads. As seen in Figure 3.7, an open-field was used to test the flight plan. An area of approximately 500 meters was used to deduce the overall effectiveness and characteristics of the weaponized threat.

Top speed received without any payload was noted at 19.6 m/s, or 44 mph. Upon addition of one 1.25 lb M112 block demolition charge, the stability and speed was slightly reduced to 18.1 m/s, or 40.5 mph. The addition of a second M112 charge rendered the drone less evasive and maneuverable.

The overall flight was still successful with top speed reaching 15.5 m/s, or 35 mph; however, the significant drain on the battery seemed to make operational flight time not nearly as long. Battery discharge and life was extended when speed was reduced to 13.5 m/s, or 30 mph. This extended battery life would preclude possible launch points from farther sites. These three speeds, 40mph, 35 mph, and 30 mph, make up the foundation for the simulation speeds to be researched and analyzed.



Measure distance
Click on the map to add to your path
Total distance: 1,640.49 ft (500.02 m)

Figure 3.7. Drone maneuverability trial path [48]

Drone Simulation Construction

The weaponized drone threat will launch from just north of the St. John's River, approximately 1 km from the target vessel, as previously seen in Figure 3.3. The drone will travel at speeds of 30, 35, and 40 mph based on data gathered from field testing. 1000 simulations will be performed for each speed against each mitigation system, SMASH M4 and iron-sighted M4. Upon initiation, the drone will follow randomized flight paths, following appropriately placed attractors in the AnyLogic system. As the drone travels southbound, it will navigate through Flight Rows 1-4, as seen in Figure 3.8 and funnel towards the target for collision. The drone will hone in on an integral fire-control system on the port side of the ship. This collision would render the ship unable to carry out primary missions.

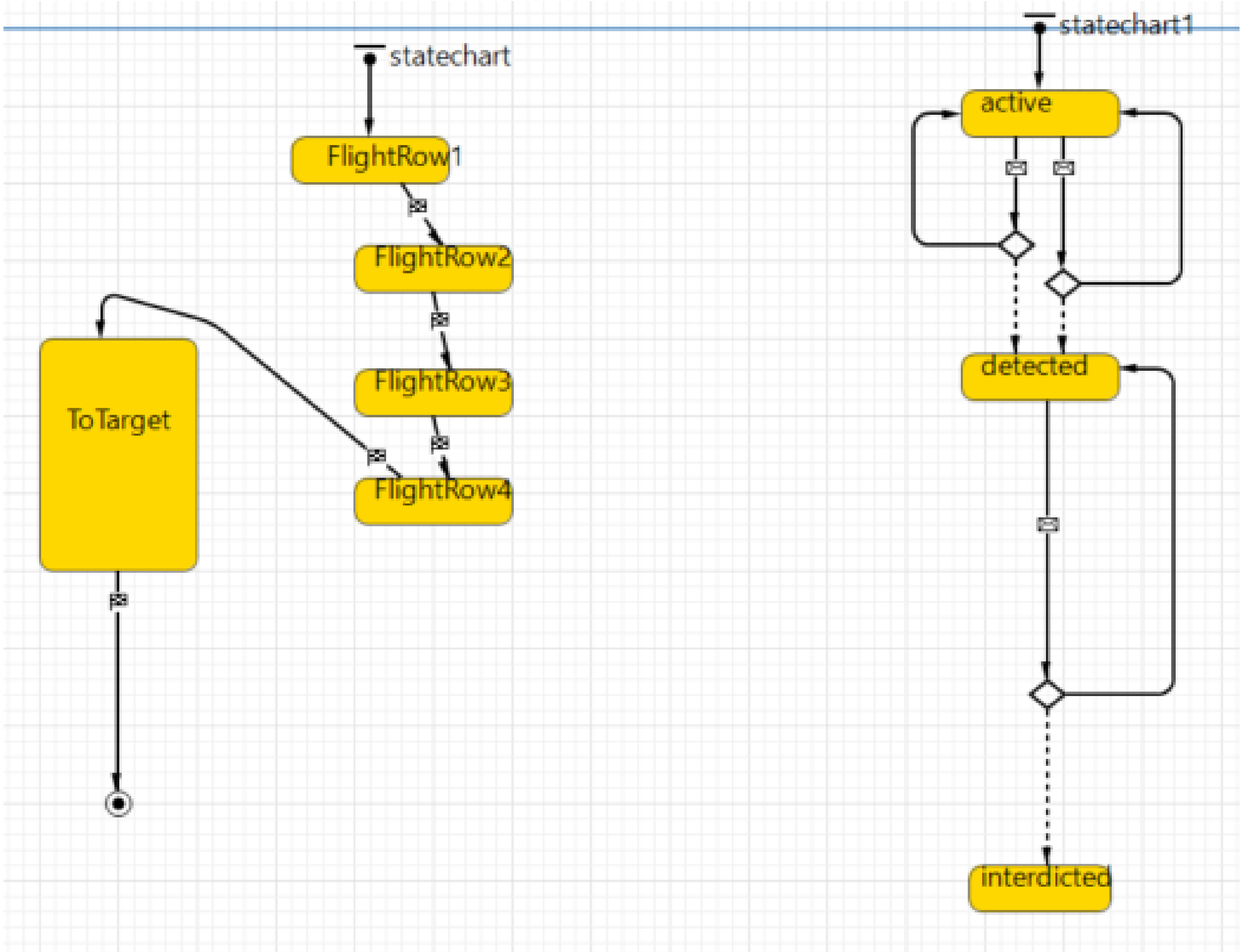
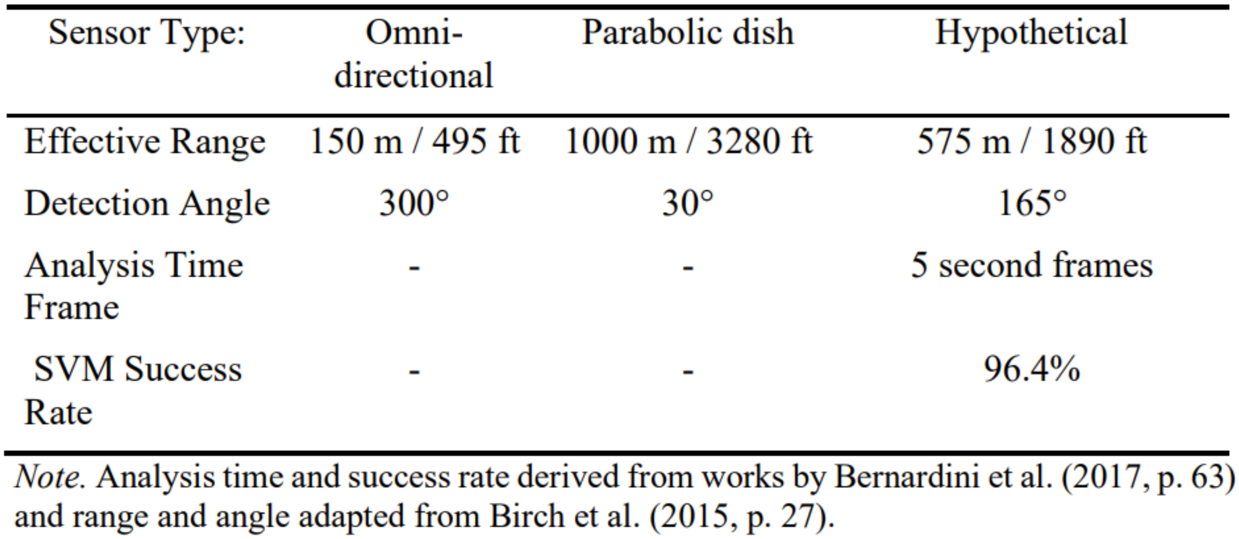


Figure 3.8. Drone Agent Statechart

3.2.3 Detection Simulation Attributes

Cline et al. [14] utilized a hypothetical sensor that will be used for modeling based on his C-UAV prison study. The average of performance characteristics of Bernardini et al. [53] and listed specifications of DroneShield as reported by Birch et al. [54] for ranging and success probability will be utilized in this study. The parameters and values of the hypothetical sensors are listed in Figure 3.9 [14]. The sensor consists of a combination of acoustic and radar detection systems. Upon detection and the resulting fix, an immediate ”all call” warning signal is sent to base and ship security forces, alerting them of the location of the impending threat.



Sensor Type:	Omni-directional	Parabolic dish	Hypothetical
Effective Range	150 m / 495 ft	1000 m / 3280 ft	575 m / 1890 ft
Detection Angle	300°	30°	165°
Analysis Time Frame	-	-	5 second frames
SVM Success Rate	-	-	96.4%

Note. Analysis time and success rate derived from works by Bernardini et al. (2017, p. 63) and range and angle adapted from Birch et al. (2015, p. 27).

Figure 3.9. Hypothetical Sensor Model Parameters and Values [14]

Four hypothetical sensors are strategically placed along the edge of the St. Johns River with overlapping coverage to the north of Naval Station Mayport. With a single threat coming from the north, only four sensors were utilized. It should be noted that any facility would provide full coverage in all cardinal directions, but that grand strategic plan is for future work and not relevant to this experiment.

3.2.4 Mitigation Simulation Attributes

The C-UAS mitigation occurs via topside watchstanders with either standard issue M4, or with standard issue M4 with SMASH system integration as seen in Figure 3.10. These watchstanders will standing watch topside, either on the bow, amidships, and near the stern of the high value unit. Once the sUAV is detected by the hypothetical sensors, the high value unit and all other base assets will be notified of impending threat. Upon notification of impending threat, watchstanders will respond within 0-10 seconds to the threat, locate it visually, and position themselves in preparation for engagement.

Within this agent of AnyLogic, watch stander response and delay occurs, probability of successfully mitigating the drone via iron sights M4 occurs, and probability of mitigating the drone via SMASH M4 occurs. This is also where the successful mitigation animation is generated, as well as experiment complete logic.

Table 3.1. C-UAS Mitigation Probabilities

Distance from ship (m)	SMASH Mitigate Probability	Iron Sighted Mitigate Probability
>500	0	0
>400	.01	.01
>300	.05	.05
>200	.10	.10
>150	.33	.15
>100	.50	.20
>50	.66	.25
>0	.90	.33

The standard issue M4 mitigation probability is the same as the SMASH M4 until drone location falls inside the SMASH system's maximum effective range of 250 meters. From 250-500 meters, both M4s have the same probability of successful mitigation. It is within 200 meters where the SMASH system delivers. The probability increases to 90 percent inside 50 meters for SMASH M4, while iron sights M4 never gets above 33 percent. Both success rates at the applicable ranges are represented in Table 3.1. The actual model logic can be seen in Figures 3.11 and 3.12.

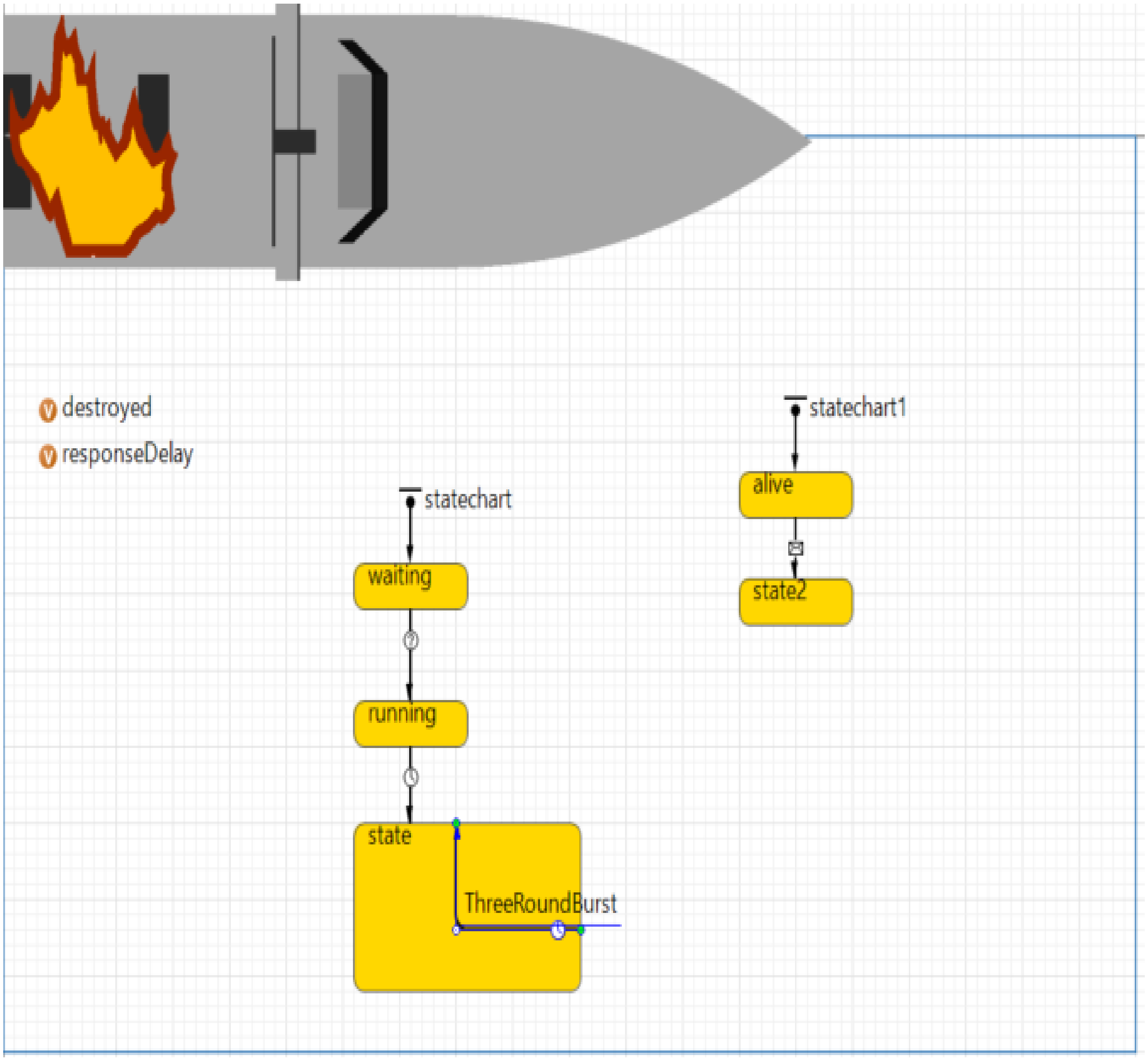
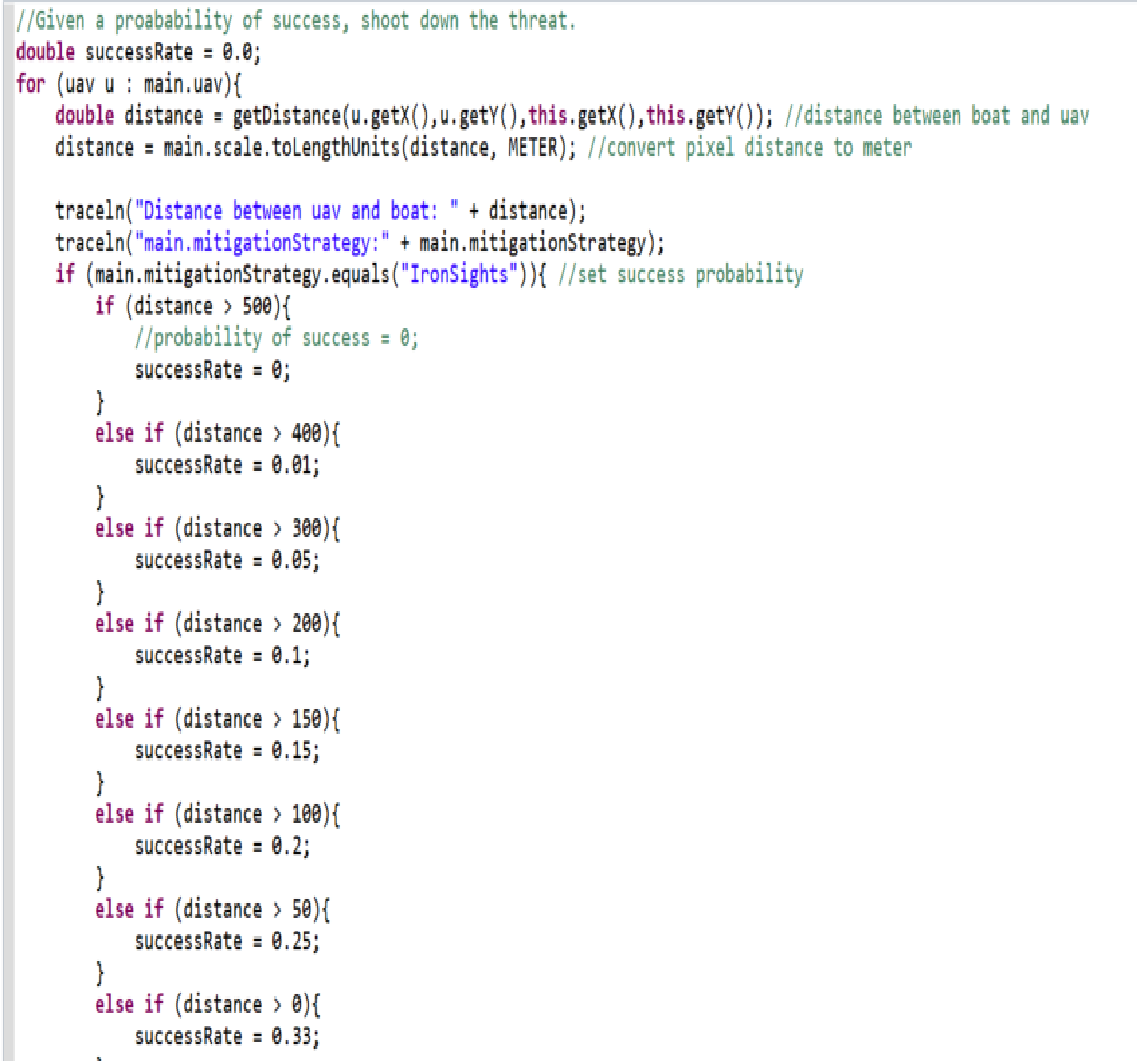


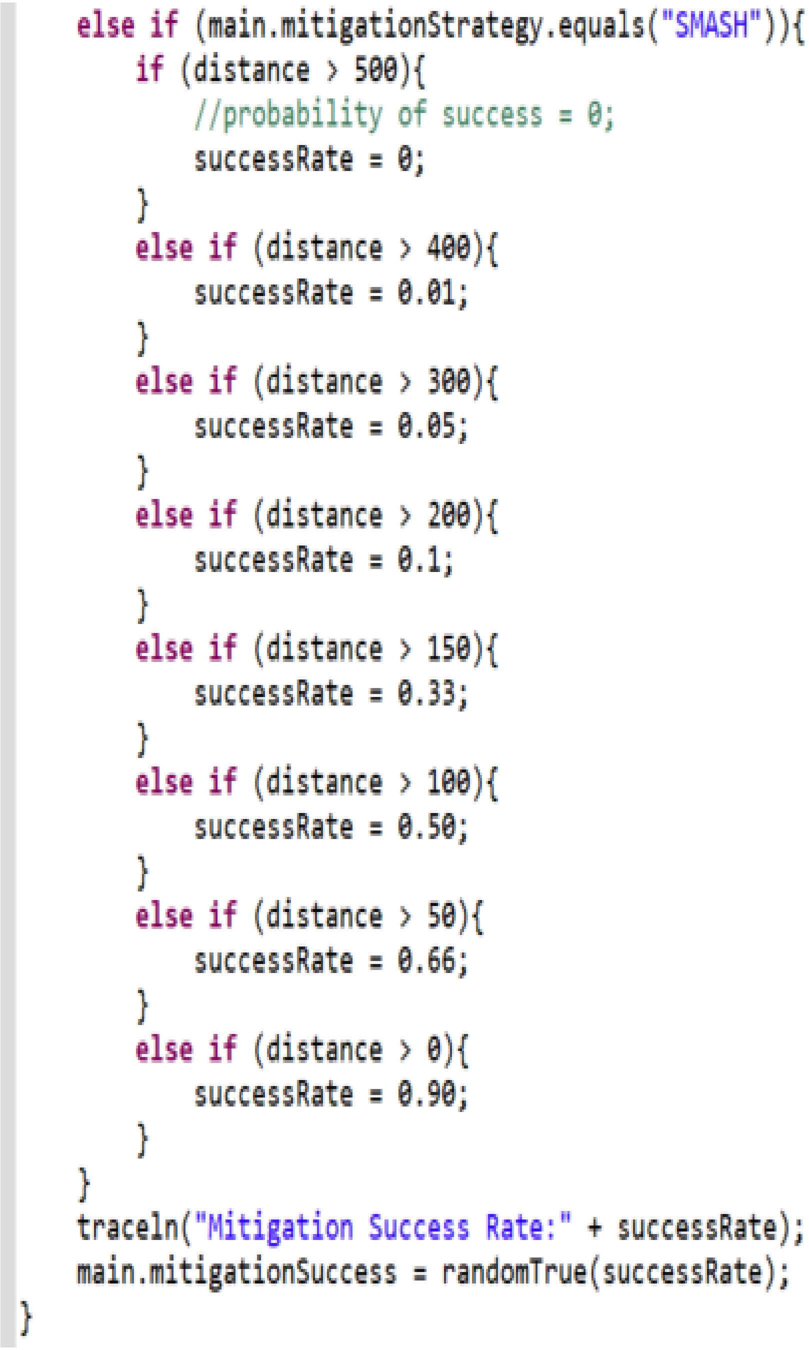
Figure 3.10. Mitigation Agent Statechart



```
//Given a proabability of success, shoot down the threat.
double successRate = 0.0;
for (uav u : main.uav){
    double distance = getDistance(u.getX(),u.getY(),this.getX(),this.getY()); //distance between boat and uav
    distance = main.scale.toLengthUnits(distance, METER); //convert pixel distance to meter

    traceln("Distance between uav and boat: " + distance);
    traceln("main.mitigationStrategy:" + main.mitigationStrategy);
    if (main.mitigationStrategy.equals("IronSights")){ //set success probability
        if (distance > 500){
            //probability of success = 0;
            successRate = 0;
        }
        else if (distance > 400){
            successRate = 0.01;
        }
        else if (distance > 300){
            successRate = 0.05;
        }
        else if (distance > 200){
            successRate = 0.1;
        }
        else if (distance > 150){
            successRate = 0.15;
        }
        else if (distance > 100){
            successRate = 0.2;
        }
        else if (distance > 50){
            successRate = 0.25;
        }
        else if (distance > 0){
            successRate = 0.33;
```

Figure 3.11. Iron Sights M4 Probability Logic



```
    else if (main.mitigationStrategy.equals("SMASH")){
        if (distance > 500){
            //probability of success = 0;
            successRate = 0;
        }
        else if (distance > 400){
            successRate = 0.01;
        }
        else if (distance > 300){
            successRate = 0.05;
        }
        else if (distance > 200){
            successRate = 0.1;
        }
        else if (distance > 150){
            successRate = 0.33;
        }
        else if (distance > 100){
            successRate = 0.50;
        }
        else if (distance > 50){
            successRate = 0.66;
        }
        else if (distance > 0){
            successRate = 0.90;
        }
    }
    traceln("Mitigation Success Rate:" + successRate);
    main.mitigationSuccess = randomTrue(successRate);
}
```

Figure 3.12. SMASH M4 Probability Logic

4. RESULTS AND DATA ANALYSIS

Chapter 4 details the summarized outcomes from the AnyLogic modeling simulations based on facts and assumptions gathered from intensive literature review, field testing, and subject matter expert recommendations and analysis. Complete data can was too large to include in the appendices, but can be reviewed upon request.

4.1 Data Review

The modeling software system AnyLogic was utilized to calculate the results of 6000 trial experiments. These experiments consisted of launching a threat aircraft from across the St. Johns River near Naval Station Mayport in Jacksonville, Florida. The targets consisted of surface warfare combatants stationed and physically moored pierside within two kilometers from the threat launch point. Multiple randomized flight paths were used, as well as randomized delay responses from the topside watchstanders onboard the ships. The watchstanders were given one of two mitigation technologies, either a standard iron-sighted M4 rifle, or an M4 rifle with SMASH technology integration. The weaponized threat speed was the only dependent variable, and was set a speeds of 30, 35, or 40 MPH based on previous field-testing data. The results of the data are displayed in charts and tables throughout the following section.

Initial Data

As seen in Table 4.1, the innovative and enhanced technology out-performed the traditional methods. With the SMASH system integrated onto the M4 rifle, the threat drone traveling at the two slowest measured speeds of 30 and 35 MPH was only able to reach the desired target four times each out of the 1000 simulation runs. The threat reached the target 11 times each in the 40 MPH simulation experiments. The iron-sighted M4 was expected to perform poorly when compared to the SMASH M4 integration system, and did not fail to live up to those expectations. The most dangerous threat, the 40 MPH drone against a watch stander supporting an iron-sighted M4 was successful at penetrating the defenses

232 times. The watch stander versus the 35MPH and 30MPH threat did not perform much better, allowing penetrations 199 and 125 times out of 1000 simulation runs respectively.

Table 4.1. C-UAS Mitigation Data Summary

Speed	Weapon System	M-D Time	Strikes/1000 attempts	Mean Distance to Ship
30	SMASH	48.7	4	201.4
35	SMASH	42.6	4	186.3
40	SMASH	37.7	11	182.6
30	IRON	48.6	125	173.4
35	IRON	42.4	199	147.9
40	IRON	37.1	232	140.8

Mitigation Times Data

The distribution comparisons between the times to mitigate provides data stating that the SMASH M4 times are slightly less that that required to mitigate via iron sights. The average time for the SMASH M4 to mitigate was right at one minute at 59.9 seconds, while the average time for iron sighted M4 to mitigate was 62.9 seconds. Granted, three seconds may not seem like much time, but it would at the absolute least provide one more three-round burst to occur prior to a target strike. The fact that 3rd quartile numbers are significantly lower cannot be overlooked either. On average, the Q3 mitigation time on SMASH M4 was 65.6 seconds, while traditional M4 sights averaged 69.9 seconds. The SMASH M4 was able to engage and deter the threat at least 1-2 three-round bursts faster than the traditional M4.

Table 4.2. Time to mitigate data

	SMASH40	SMASH35	SMASH 30	IRON40	IRON35	IRON30
Mean	52.4	59.3	68	54.2	64.6	69.8
Min	34.5	37.8	42.3	29.2	34.8	37.3
Q1	48	53.9	61.7	48.3	55.1	62.1
Median	53	60.3	69.1	55.6	62.6	70.5
Q3	57.2	64.9	74.7	61.4	69	79.2
Max	70.2	81.3	92.7	72.3	82.7	96.4

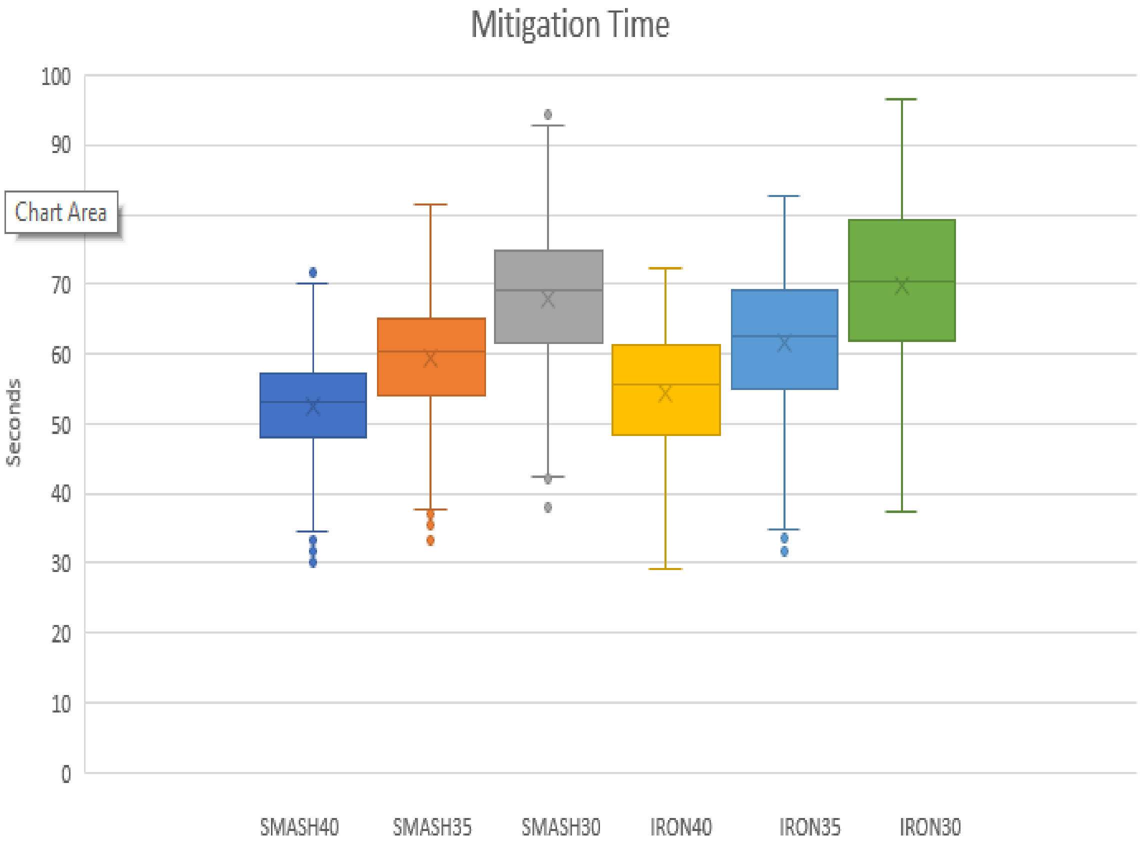


Figure 4.1. Time to mitigate boxplot

Distance to Ship Data

Based on the improved accuracy of the SMASH M4, the watch stander was able to mitigate the threat UAV much farther out from the ship that with traditional iron sights. Once the drone was able to penetrate within 250 meters of the ship, the SMASH M4 mitigation percentages increased dramatically, resulting in both fewer overall target strikes and at an increased range from the ship at which the drones were mitigated. The SMASH system against the threat at any speed was able to mitigate on an average of 190.1 meters, while traditional iron sights performed average mitigations at a range of 154 meters.

While not necessarily an overwhelming amount with merely a 36 meter difference, the frequency of close calls is evident when looking at the statistical first quartile (Q1) ranges. The average distance to the ship when mitigated based on the three speeds at the Q1 data

Table 4.3. Distance to ship data

	SMASH40	SMASH35	SMASH 30	IRON40	IRON35	IRON30
Mean	182.6	186.3	201.4	140.8	147.9	173.4
Min	0	0	0	0	0	0
Q1	109.8	113.9	125	7	26.7	58.4
Median	165	167.5	179.2	112.4	133.3	160.8
Q3	251.1	258.7	271.9	241	240.7	274
Max	462.6	463.9	491.6	498.2	493.9	491.8

measure shows that the SMASH M4 systems mitigated at 116.2 meters, while standard iron sights mitigated at 30.7 meters. This can be better visually represented by the bar graphs below illustrating the frequency of at which the threat was mitigated, based on distance to the ship.

Clearly the distribution is significantly skewed left during the review of the iron sights data, thereby alluding that the 36 meter difference in the average distance does not show how effective the SMASH system actually is. By mitigating more targets at a farther distance, the SMASH system provides a greater distance of target elimination and more room for errors pending other environmental variables.

4.2 Inferential Statistical Analysis

In order to demonstrate that the results of the experiments were due to decided variations vice random chance, testing for statistical significance was completed via the Mann-Whitney U Test. This non-parametric test compared two groups in which the dependent variable are not necessarily normally distributed, as in the case of the differences between the SMASH system and the traditional iron sighted M4. The data was collected and bundled to compare the populations in the categories consisting of mitigation times, detection times, watchstander response delay times, and distance from ship at time of mitigation.

For the performance claim that this document is making, significance tests were done in two parts. First, all pooled data, independent of speed from the two mitigation systems, were collected and compared. Secondly, the individual speeds for each mitigation system were

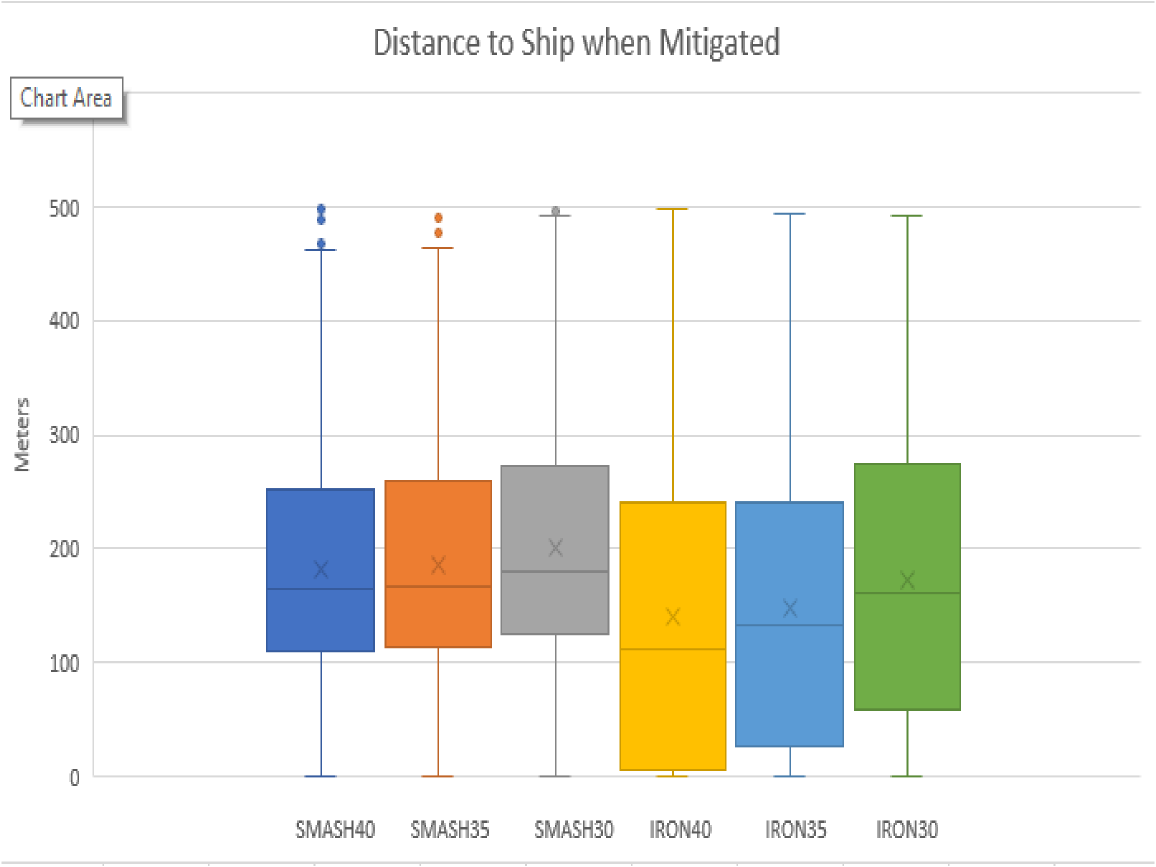


Figure 4.2. Distance to ship boxplot

compared to their counterpart for 30, 35, and 40 MPH respectively. The results provides the evidence that the difference in averages is significant across all effects tested.

Approximately 12,000 simulation iterations of pooled data were compared between SMASH system and Iron Sights, resulting in a p-value of 0.00674. Additionally, significance tests were conducted were based on the two mitigation techniques, SMASH and Iron Sights, and the mean distances to the ship at which they were mitigated, dependent on speed. The SMASH system probabilities changes from the standard M4 traditional Iron sights once the threat moves within 200 meters from the target. When SMASH at 30 MPH was compared to Iron Sights at 30 MPH within 200 meters, the p-value was 2.22e-16. When SMASH at 35 MPH was compared to Iron Sights at 35 MPH within 200 meters, the p-value was 1.56e-8. When SMASH at 40 MPH was compared to Iron Sights at 40 MPH within 200 meters, the p-value was 2.442e-15.

4.3 Data Summary

Understanding that an enhanced version of the traditional M4 must provide improvement upon the likelihood on threat mitigation is a given. Understanding how or where the improvements will come from is another. It is evident that the increased threat mitigation percentages inside 200 yards is where the benefit lies. The increased distance from the ship of threat mitigation cannot be understated. Lastly, the fact that a total of 26 threats were able to penetrate the defenses in 3000 simulations, compared to the 556 successful target strikes in 3000 simulation against traditional M4 sights emphasizes the need for implementation into the fleet.

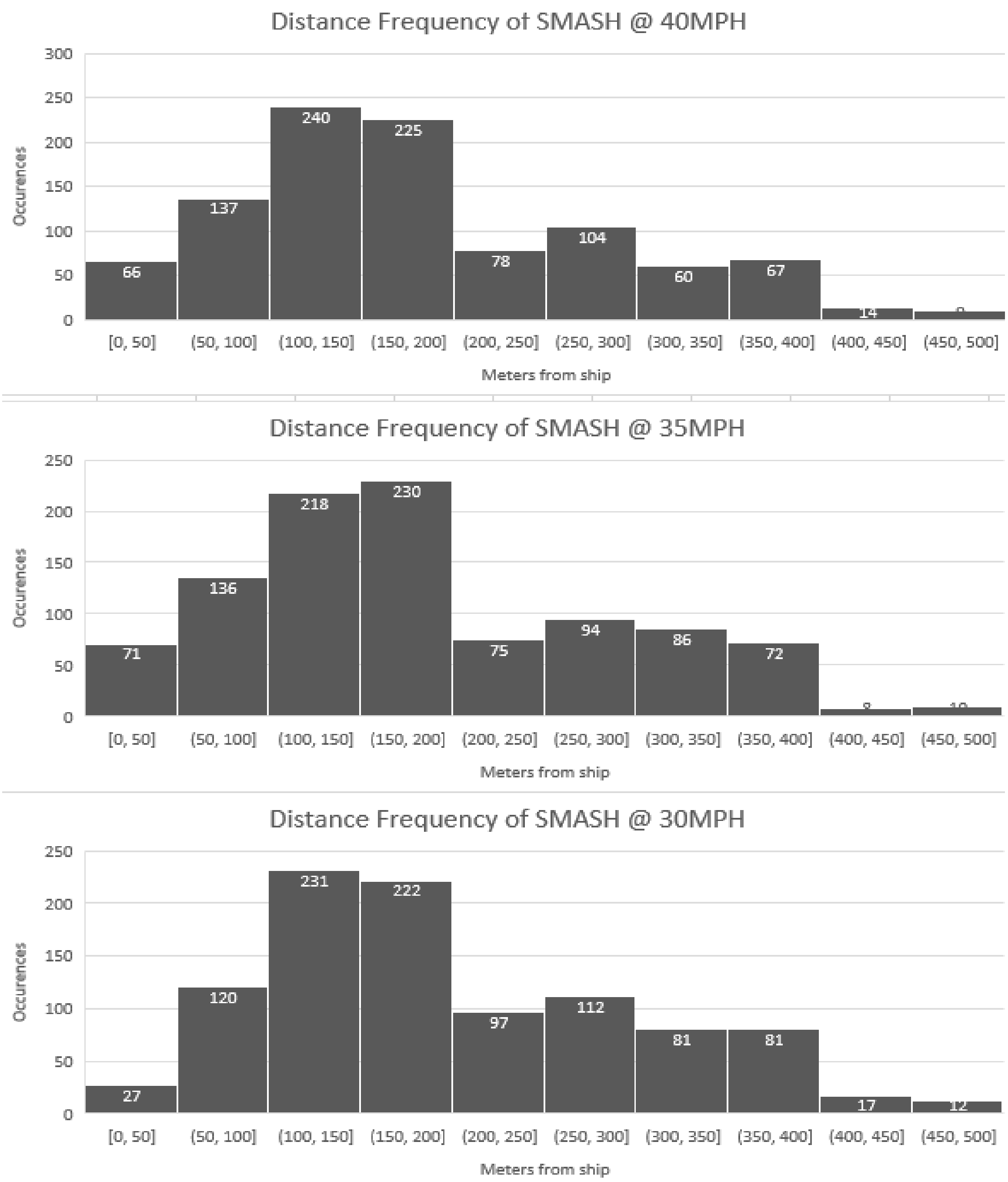


Figure 4.3. Frequency distance SMASH

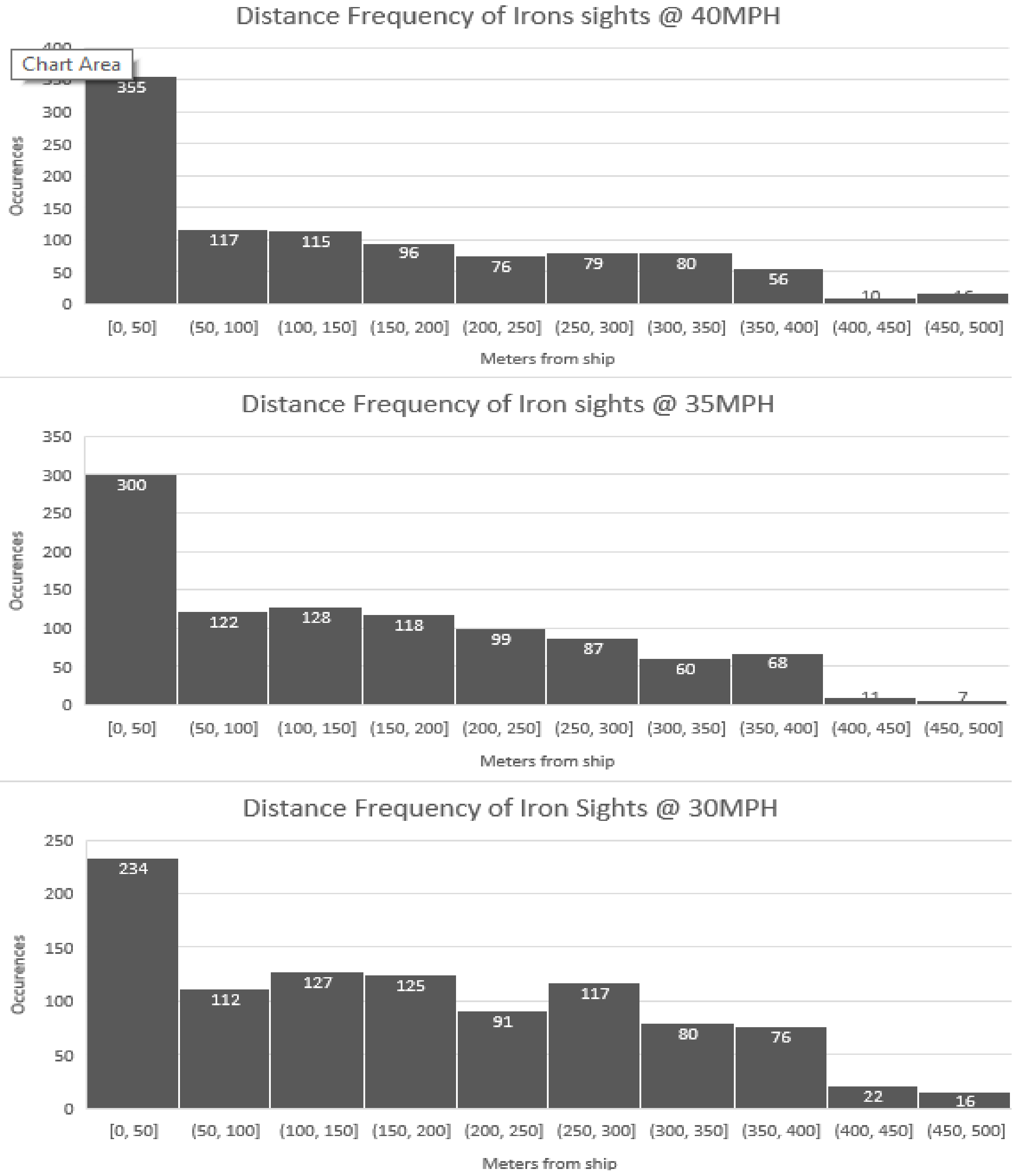


Figure 4.4. Frequency distance Iron Sights

5. CONCLUSIONS, DISCUSSIONS, AND RECOMMENDATIONS

5.1 Introduction

The purpose of this project was to address the lack of effectiveness of currently available C-UAS defenses, to identify the gaps in the current defense in depth protocols, and to determine the feasibility of an enhanced last line of defense countermeasure to protect vulnerable HVUs pier-side.

This experiment consisted of defending high value units afloat pierside at Mayport Naval Station in Jacksonville, Florida, from a weaponized drone. The weaponized drone was based on an autonomous drone, flying randomized flight paths at speeds ranging from 30-40MPH based on internal flight control computing systems. This threat drone is assumed to be impervious to traditional jamming, spoofing and dazzling techniques and can only be taken down kinetically.

The defense consisted of a hypothetical detection and alert system with 96.4 percent detection rates from acoustic and radar sensors. Upon detection, the hypothetical sensor would trigger an ”all-call” alert system, similar to what is already implemented at naval base security centers, notifying authorities, ships, and watch standers of an impending threat, its location and vector. Upon notification of the threat, topside watch standers would have anywhere from immediate response to a ten second delay to react and position themselves to a location to accurately intercept and mitigate the threat.

Watch standers were supplied with either a traditional, iron-sighted M4 rifle or an enhanced M4 model, implemented with the SMASH, a fire control-enabled, ballistic-assisted system that provides an ”one shot, one kill” hit probability. Mitigation probability percentages were assumed based on maximum effective ranges of both the M4 rifle and the SMASH-enabled M4 rifle.

5.2 Conclusions

6000 simulation runs were conducted using AnyLogic modeling software to determine how effective the SMASH system can be when compared to traditional iron-sighted M4s. It is evident from the data given that the SMASH system provides a higher probability of success in the defense of high value units in port while afloat pierside.

The SMASH system only allowed 26 penetrations through the defenses in 3000 simulation runs at various drone speeds. The most difficult threats, the 35 and 40MPH weaponized drones allowed 11 target strikes in each of their 1000 runs; 30MPH threat only allowed 4 strikes of the high value unit. The SMASH system was 99 percent effective in drone mitigation.

The iron-sighted M4 allowed 125, 199, and 232 strikes in each of their 1000 simulations based on speeds of 30, 35, and 40MPH respectively. The traditional M4 allowed strikes 556 times out of the 3000 attempts, for enabling the drone to be successful 18.5 percent of the time.

Distance from the ship when mitigation occurred was a significant observation made during the modeling. The watch standers utilizing the SMASH system were able to mitigate the threat at an average range of 190 meters away from the ship, while the watch standers wielding traditional iron-sighted M4s allowed the threat to penetrate to within 154 meters, on average, before mitigation. The most lethal drone, traveling at 40MPH against the iron-sighted M4 was mitigated on average only 140.8 meters from the ship. That being said, that particular threat again struck the high value unit 23.2 percent of the time.

The frequency at which the drones were able to penetrate within 50 meters was quite astounding. 889 occurrences out of 3000 simulations resulted in either target strike or mitigations within 50 meters. This is far too close to the ship for any base commander or ship captain to feel comfortable with. The 29.6 percent mitigation or strike percentage within 50 meters must be addressed. Environmental concerns such as weather visibility or increased watch stander response delays greater than 10 seconds would only increase this percentage.

5.3 Future Work

Accurate numbers, not valid assumptions, need to be inserted into the model to provide a better overall picture and accurate assessment of the SMASH system's ability to compete with the traditional iron-sighted M4s. Field testing of standard M4 rifles and SMASH-enable M4 rifles against drones at various speeds, heights, and evasive action flight paths will provide the data required to perform a more accurate model.

Once the model becomes more accurate, it can be disseminated and implemented to existing naval bases to more precisely prepare defenses and doctrine against drone threats. The knowledge of knowing what type of threat drone the base would be up against is essential. The defenses, to include detection and notification systems, can be based on the time needed to effectively defeat a weaponized drones.

The model could be improved in various ways. The model could use better detection and alert systems. The model could be run again with multiple watch standers, using combinations of traditional and enhanced M4 systems, as well as run with multiple SMASH systems to provide even better mitigation percentages, as well as mitigation from the ship distances.

Additionally, threat generation or launch points could also provide better randomization, as well well as threats development enhancements. Instead of using a quadcopter, perhaps a fixed wing threat based on quickness vice being impervious to countermeasures could provide additional simulations and experiments.

This model represents a static target with watch standers using various M4 rifles. Another possibility or future use of the model would be to implement the use of the SMASH system integrated onto crew-served weapons while entering or leaving port. This is a potential possibility to better defend the ship while transiting straits, channels or other restricted water locations. Additionally, these enhanced crew-served weapons could be used when the risk of collateral damages to civilian and friendly populations are lower.

Throughout this research there was zero discussion about the upkeep and maintenance required to keep these systems functional. There should be a discussion regarding how many units should be provided to ships or bases. Training watch standers to use and maintain the weapon should be fairly simple based on the fact that these system will be implemented onto existing M4 rifles. There was no discussion about the cost-benefit analysis and procurement of the systems. These are but a few items needs to be discussed in the future.

5.4 Final Thoughts

SMASH is a proactive approach to improve C-UAS defenses. This option is better than traditional iron sights and is better than utilizing a reactive approach. It is clearly an inexpensive option that should be discussed and implemented as lasers, dazzlers, and other defenses of the future are developed, at a cost. Additionally, implementing SMASH systems onto already existing M4s enables Sailors to easy to train for these inevitable scenarios. These systems can be taken to sea to test on open ocean shooting ranges. Maintenance and upkeep of these handheld devices .

The simulation modeling experiment, when integrated with accurately field tested ballistic data, could easily be replicated at any number of naval, army, and coast guard bases. This replication can give an estimated timeline into how to best defend high value units across all branches of service. By running this model, base commanders could improve training, drills, sensor locations, and weak points or gaps within current doctrine for defending against this threat. By knowing the threat, and assuming speeds and distances to assets, base commanders can actually prepare and be proactive in this escalating arms race between UAV and C-UAV technologies.

Standard M4 rifles provide no significant ability to reduce the risk of collateral damage when attempting to mitigate a threat drone inbound. The lack of proficiency for topside watch standers against incoming drones means more shots required to mitigate, as well as more risk for collateral damage due to random or errand shots. The SMASH M4 does not allow the operator to even pull the trigger without an accurate shooting solution. Even in the low likelihood that there is a miss, the missed round would still travel downrange towards the target, not wildly off-range towards civilians or other assets.

There is no silver bullet to eliminate the threat from weaponized drones. The SMASH system is a quick action opportunity that can be easily given to topside watchstanders in an effort to improve the successful mitigation likelihood against weaponized threats now.

REFERENCES

[1] A. Sherbinin and R. Kuzma, *How Drones Could Mission Kill a U.S. Destroyer | RealClearDefense*, 2020. [Online]. Available: https://www.realcleardefense.com/2020/05/05/how_drones_could_mission_kill_a_us_destroyer_313338.html.

[2] O. Radu, G. Slămnoiu, and L. Zărnescu, "Harbor Protection Against Terrorist Threats: Difficulties and Possible Solutions," Naval Research Center Constanta, Constanta, Romania, Tech. Rep., 2006, pp. 3–4.

[3] B. Germond, "The geopolitical dimension of maritime security," *Marine Policy*, vol. 54, pp. 137–142, Apr. 2015. DOI: 10.1016/j.marpol.2014.12.013.

[4] S. Savitz, I. Blickstein, P. Buryk, R. W. Button, P. DeLuca, J. Dryden, J. Mastbaum, J. Osburg, P. Padilla, A. Potter, C. C. Price, L. Thrall, S. K. Woodward, R. J. Yardley, and J. M. Yurchak, "U.S. Navy Employment Options for Unmanned Surface Vehicles (USVs):" RAND Corporation, Santa Monica, CA, Tech. Rep., 2013, p. 156.

[5] C. Strode, D. Cecchi, and H. Yip, "The effectiveness of a system-of-systems for countering asymmetric maritime threats in ports and harbours," in *1st International Conference and Exhibition on Waterside Security (WSS 2008), Technical University of Denmark, Copenhagen, Denmark, 25-28 August 2008.*, Denmark: NURC, 2008.

[6] United States Navy, "THE NAVY UNMANNED SURFACE VEHICLE (USV) MASTER PLAN," Program Executive Office Littoral and Mine Warfare (PEO-LMW), Washington DC, Tech. Rep., Jul. 2007.

[7] C. Brownstein, J. Baker, P. Hull, N. Minogue, G. Murphy, and P. Winston, "Report of the DHS National Small Vessel Security Summit," US Department of Homeland Security, Washington, DC, Tech. Rep., 2007, p. 122.

[8] P. R. Trischitta, H. Salloum, B. Bunin, and P. Orton, "Mitigating threats of small vessels to maritime security," in *2012 IEEE International Conference on Technologies for Homeland Security, HST 2012*, 2012, pp. 654–659, ISBN: 9781467327084. DOI: 10.1109/THS.2012.6459926.

[9] H. Kang, J. Joung, J. Kim, J. Kang, and Y. S. Cho, "Protect Your Sky: A Survey of Counter Unmanned Aerial Vehicle Systems," *IEEE Access*, vol. 8, pp. 168 671–168 710, Sep. 2020, ISSN: 2169-3536. DOI: 10.1109/access.2020.3023473.

[10] A. H. Michel, *Report: Counter-Drone Systems*, Feb. 2018. [Online]. Available: https://dronecenter.bard.edu/counter-drone-systems/.

[11] A. H. Michel, "COUNTER-DRONE SYSTEMS," Tech. Rep., 2019. [Online]. Available: https://store.frost.com/.

[12] R. Müller and C. Brook, "Vessel protection in expeditionary operations: At anchor and in foreign harbours," in *2010 International Waterside Security Conference, WSS 2010*, 2010, ISBN: 9781424488940. DOI: 10.1109/WSSC.2010.5730265.

[13] "Counter-Small Unmanned Aircraft Systems Strategy," Tech. Rep., 2021.

[14] T. L. Cline and J. E. Dietz, "Agent based modeling for low-cost counter UAS protocol in prisons," *International Journal of Aviation, Aeronautics, and Aerospace*, vol. 7, no. 2, p. 2, Jan. 2020, ISSN: 23746793. DOI: 10.15394/IJAAA.2020.1462. [Online]. Available: https://commons.erau.edu/ijaaa/vol7/iss2/2/.

[15] F. Giovanneschi, M. Laurenzis, S. Hengy, M. Hammer, A. Hommes, W. Johannes, O. Rassy, E. Bacher, S. Schertzer, and J.-M. Poyet, "An adaptive sensing approach for the detection of small UAV: first investigation of static sensor network and moving sensor platform," in *Signal Processing, Sensor/Information Fusion, and Target Recognition XXVII*, I. Kadar, Ed., vol. 10646, SPIE, Apr. 2018, p. 27, ISBN: 9781510618039. DOI: 10.1117/12.2304758. [Online]. Available: https://www.spiedigitallibrary.org/conference-proceedings-of-spie/10646/2304758/An-adaptive-sensing-approach-for-the-detection-of-small-UAV/10.1117/12.2304758.full.

[16] W. Barr, "Department Activities to Protect Certain Facilities or Assets from Unmanned Aircraft and Unmanned Aircraft Systems," Tech. Rep., 2020. [Online]. Available: https://www.justice.gov/ag/page/file/1268401/download.

[17] J. Knight, “Calhoun: The NPS Institutional Archive DSpace Repository COUNTERING UNMANNED AIRCRAFT SYSTEMS,” Tech. Rep., 2019. [Online]. Available: http://hdl.handle.net/10945/63997.

[18] A. Solodov, A. Williams, S. Al Hanaei, and B. Goddard, “Analyzing the threat of unmanned aerial vehicles (UAV) to nuclear facilities,” *Security Journal*, vol. 31, no. 1, pp. 305–324, Feb. 2018, ISSN: 17434645. DOI: 10.1057/s41284-017-0102-5.

[19] R. J. Wallace and J. M. Loffi, “Examining unmanned aerial system threats & defenses: A conceptual analysis,” *International Journal of Aviation, Aeronautics, and Aerospace*, vol. 2, no. 4, pp. 10–11, Oct. 2015, ISSN: 23746793. DOI: 10.15394/ijaaa.2015.1084. [Online]. Available: http://commons.erau.edu/ijaaa/vol2/iss4/1/.

[20] T. Humphreys, “STATEMENT ON THE SECURITY THREAT POSED BY UNMANNED AERIAL SYSTEMS AND POSSIBLE COUNTERMEASURES,” 2015.

[21] M. J. Hopmeier, *A Proposed Taxonomy and Structure for Discussing Drone Threats and Countermeasures*, Washington DC, 2016.

[22] J.-P. Yaacoub, H. Noura, O. Salman, and A. Chehab, “Security analysis of drones systems: Attacks, limitations, and recommendations,” *Internet of Things*, vol. 11, p. 100 218, Sep. 2020, ISSN: 25426605. DOI: 10.1016/j.iot.2020.100218. [Online]. Available: /pmc/articles/PMC7206421/?report=abstract%20https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7206421/.

[23] E. National Academies of Sciences and Medicine, *Counter-Unmanned Aircraft System (CUAS) capability for battalion-and-below operations: Abbreviated version of a restricted report*. National Academies Press, Mar. 2018, pp. 1–35, ISBN: 9780309458139. DOI: 10.17226/24747.

[24] M. Demirhan and C. Premachandra, “Development of an Automated Camera-Based Drone Landing System,” *IEEE Access*, vol. 8, pp. 202 111–202 121, 2020, ISSN: 21693536. DOI: 10.1109/ACCESS.2020.3034948.

[25] M. Caccia, M. Bibuli, G. Bruzzone, V. Djapic, S. Fioravanti, and A. Grati, "Modular USV and payload design for advanced capabilities in marine security applications," in *2011 19th Mediterranean Conference on Control and Automation, MED 2011*, 2011, pp. 430–435, ISBN: 9781457701252. DOI: 10.1109/MED.2011.5983158.

[26] M. R. Patterson and S. J. Patterson, "Unmanned systems: An emerging threat to waterside security: Bad robots are coming," in *2010 International Waterside Security Conference, WSS 2010*, 2010, ISBN: 9781424488940. DOI: 10.1109/WSSC.2010.5730271.

[27] I. Guvenc, F. Koohifar, S. Singh, M. L. Sichitiu, and D. Matolak, "Detection, Tracking, and Interdiction for Amateur Drones," *IEEE Communications Magazine*, vol. 56, no. 4, pp. 75–81, Apr. 2018, ISSN: 01636804. DOI: 10.1109/MCOM.2018.1700455.

[28] J. Rowley, "Autonomous Unmanned Surface Vehicles (USV): A Paradigm Shift for Harbor Security and Underwater Bathymetric Imaging," in *OCEANS 2018 MTS/IEEE Charleston, OCEAN 2018*, Institute of Electrical and Electronics Engineers Inc., Jan. 2019, ISBN: 9781538648148. DOI: 10.1109/OCEANS.2018.8604611.

[29] L. L. Faulkner, B. P. Kritzstein, and J. J. Zimmerman, "Security infrastructure for commercial and military ports," in *OCEANS'11 - MTS/IEEE Kona, Program Book*, 2011, ISBN: 9781457714276. DOI: 10.23919/oceans.2011.6107174.

[30] G. F. GRESH, "A Vital Maritime Pinch Point: China, the Bab al-Mandeb, and the Middle East," *Asian Journal of Middle Eastern and Islamic Studies*, vol. 11, no. 1, pp. 37–46, Mar. 2017, ISSN: 2576-5949. DOI: 10.1080/25765949.2017.12023324.

[31] J. Stevenson, "Strategic rivalries around the Bab el-Mandeb Strait," *Strategic Comments*, vol. 24, no. 4, pp. viii–x, Apr. 2018. DOI: 10.1080/13567888.2018.1485341. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/13567888.2018.1485341.

[32] A. Banerjee, "SANDIA REPORT Redefining Maritime Security Threats in the Eastern Indian Ocean Region," Sandia National Laboratories, Albuquerque, NM, Tech. Rep., 2017, p. 45. [Online]. Available: http://www.ntis.gov/search.

[33] S. Park, S. Shin, Y. Kim, E. T. Matson, K. Lee, P. J. Kolodzy, J. C. Slater, M. Scherreik, M. Sam, J. C. Gallagher, B. R. Fox, and M. Hopmeier, "Combination of radar and audio sensors for identification of rotor-type Unmanned Aerial Vehicles (UAVs)," in *2015 IEEE SENSORS - Proceedings*, Institute of Electrical and Electronics Engineers Inc., Dec. 2015, ISBN: 9781479982028. DOI: 10.1109/ICSENS.2015.7370533.

[34] S. Siewert, M. Andalibi, S. Bruder, I. Gentilini, and J. Buchholz, "Drone net architecture for UAS traffic management multi-modal sensor networking experiments," in *IEEE Aerospace Conference Proceedings*, vol. 2018-March, IEEE Computer Society, Jun. 2018, pp. 1–18, ISBN: 9781538620144. DOI: 10.1109/AERO.2018.8396716.

[35] M. Benyamin and G. H. Goldman, "Acoustic Detection and Tracking of a Class I UAS with a Small Tetrahedral Microphone Array," Tech. Rep., 2014.

[36] F. Christnacher, S. Hengy, M. Laurenzis, A. Matwyschuk, P. Naz, S. Schertzer, and G. Schmitt, "Optical and acoustical UAV detection," in *Electro-Optical Remote Sensing X*, G. Kamerman and O. Steinvall, Eds., vol. 9988, SPIE, Oct. 2016, 99880B. DOI: 10.1117/12.2240752. [Online]. Available: http://proceedings.spiedigitallibrary.org/proceeding.aspx?doi=10.1117/12.2240752.

[37] J. M. Goppert, A. R. Wagoner, D. K. Schrader, S. Ghose, Y. Kim, S. Park, M. Gomez, E. T. Matson, and M. J. Hopmeier, "Realization of an autonomous, air-to-air Counter Unmanned Aerial System (CUAS)," in *Proceedings - 2017 1st IEEE International Conference on Robotic Computing, IRC 2017*, Institute of Electrical and Electronics Engineers Inc., May 2017, pp. 235–240, ISBN: 9781509067237. DOI: 10.1109/IRC.2017.10.

[38] R. O'Rourke, "Navy Lasers, Railgun, and Gun-Launched Guided Projectile: Background and Issues for Congress," Congressional Research Service, Washington DC, Tech. Rep., 2021, p. 49. [Online]. Available: https://crsreports.congress.gov.

[39] D. Balbuena, M. Casserly, B. Dickerson, S. Graves, V. Maldonado, B. Pandya, L. Pham, and J. Sanders, "NAVAL POSTGRADUATE SCHOOL MONTEREY, CALIFORNIA CAPSTONE PROJECT REPORT Approve for public release; distribution

is unlimited UAV SWARM ATTACK: PROTECTION SYSTEM AL-TERNATIVES FOR DESTROYERS," Tech. Rep., 2012.

[40] Department of the Army, "Rifle and Carbine Headquarters, Department of the Army," Tech. Rep., 2016. [Online]. Available: https://atiam.train.army.mil/catalog/dashboard.

[41] SMASH, "SMASH AD Counter Drone Fire Control System for Small Arms," Tech. Rep., 2021.

[42] DSJ Staff, *SMASH 2000 being evaluated by the U.S. Army under Foreign Comparative Test (FCT) | Defense Systems Journal*, Oct. 2020. [Online]. Available: https://dsjournal.com/2020/10/15/smash-2000-being-evaluated-by-the-u-s-army-under-foreign-comparative-test-fct/.

[43] Army Public Affairs, *Army announces selection of interim C-sUAS systems | Article | The United States Army*, Jun. 2020. [Online]. Available: https://www.army.mil/article/236713/army_announces_selection_of_interim_c_suas_systems.

[44] D. ; Arteche, K. ; Chivers, B. ; Howard, T. ; Long, W. ; Merriman, A. ; Padilla, A. ; Pinto, S. ; Smith, and V. Thoma, "Calhoun: The NPS Institutional Archive DSpace Repository Drone defense system architecture for U.S. Navy strategic facilities," Tech. Rep., 2017. [Online]. Available: http://hdl.handle.net/10945/56172.

[45] G. Lykou, D. Moustakas, and D. Gritzalis, "Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies," *Sensors*, vol. 20, no. 12, p. 3537, Jun. 2020, ISSN: 1424-8220. DOI: 10.3390/s20123537. [Online]. Available: https://www.mdpi.com/1424-8220/20/12/3537.

[46] I. Grigoryev, "AnyLogic in Three Days," Tech. Rep., 2018.

[47] A. Riegsecker, "SCANS FRAMEWORK: SIMULATION OF CUAS NETWORKS AND SENSORS A Dissertation," Tech. Rep., Jan. 2021. DOI: 10.25394/PGS.13338626.V1. [Online]. Available: /articles/thesis/SCANS_Framework_Simulation_of_CUAS_Networks_and_Sensors/13338626/1.

[48] Google Maps, *Google Maps*, 2021. [Online]. Available: https://www.google.com/maps/@40.4368814,-86.892637,851m/data=!3m1!1e3.

[49] C. Kouhestani, B. Woo, and G. Birch, "Counter unmanned aerial system testing and evaluation methodology," in *Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security, Defense, and Law Enforcement Applications XVI*, E. M. Carapezza, Ed., vol. 10184, SPIE, May 2017, p. 1 018 408. DOI: 10.1117/12.2262538. [Online]. Available: http://proceedings.spiedigitallibrary.org/proceeding.aspx?doi=10.1117/12.2262538.

[50] *Naval Station Mayport | Base Overview & Info | MilitaryINSTALLATIONS*. [Online]. Available: https://installations.militaryonesource.mil/in-depth-overview/naval-station-mayport.

[51] J. Spires, *Mexican cartel turns to C4 equipped suicide drones - DroneDJ*, Aug. 2020. [Online]. Available: https://dronedj.com/2020/08/25/mexican-cartel-turns-to-c4-equipped-suicide-drones/.

[52] Department of the Army, "FM 5-250 ii," Tech. Rep., 1992.

[53] A. Bernardini, F. Mangiatordi, E. Pallotti, and L. Capodiferro, "Drone detection by acoustic signature identification," in *IS and T International Symposium on Electronic Imaging Science and Technology*, Society for Imaging Science and Technology, 2017, pp. 60–64. DOI: 10.2352/ISSN.2470-1173.2017.10.IMAWM-168.

[54] G. C. Birch, J. C. Griffin, and M. K. Erdman, "SANDIA REPORT UAS Detection, Classification, and Neutralization: Market Survey 2015," Tech. Rep., 2015. [Online]. Available: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online.