NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

INTEGRATION OF RADAR SENSOR DATA WITH SITUATIONAL AWARENESS TOOLS TO RESPOND TO AN UNMANNED AERIAL THREAT

by

Derrick W. Majors and Ryan P. O'Neil

June 2021

Thesis Advisor:	Alex Bordetsky
Co-Advisor:	Eugene Bourakov
Second Reader:	Edward L. Fisher

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

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

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

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2021	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
INTEGRATION OF RADAR SENSOR DATA WITH SITUATIONAL AWARENESS TOOLS TO RESPOND TO AN UNMANNED AERIAL THREAT

5. FUNDING NUMBERS

6. AUTHOR(S) Derrick W. Majors and Ryan P. O'Neil

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

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

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

Detecting unmanned aerial systems (UAS) is complicated. Integrating and sharing radar information across multiple domains (air, land, and sea) is a problem. Current research on UAS detection focuses primarily on detecting UAS over ground forces and national critical infrastructure, but what happens when UAS starts challenging warships in a harbor or open ocean? How can information be collected and shared wirelessly during a multi-agency crisis event? Could detected UAV sensor data be shared in a wireless mesh network (WMN) with other agencies? Our study demonstrated the possibility of integrating simulated data from SAAB's G1X radar system, integrated with the Tactical Assault Kit (TAK) situational awareness application, during a small-scale multi-agency crisis response exercise. The technology worked flawlessly; however, we noticed that counter UAS tactics techniques and procedures (TTP), international UAS laws and regulations, and cueing and automation must be further examined and reworked for today's fight and interagency response. In addition, we discovered that cell phone coverage did not effectively cover San Francisco Bay during the exercise. To mitigate this gap, we successfully extended a WMN using Persistent Systems' MPU-5 radios to create a broader capability of maintaining network functions in a non-networked environment.

14. SUBJECT TERMS RADAR, RiTM, ATAK, WMN, UAS detection, SAAB, G1X, situation awareness, decision-making	**15. NUMBER OF PAGES** 129
	16. PRICE CODE

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

NSN 7540-01-280-5500

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

INTEGRATION OF RADAR SENSOR DATA WITH SITUATIONAL AWARENESS TOOLS TO RESPOND TO AN UNMANNED AERIAL THREAT

Derrick W. Majors
Lieutenant, United States Navy
BSBA, Northern Illinois University, 2008

Ryan P. O'Neil
Lieutenant, United States Navy
BS, Trident University International, 2009
MHAP, Uniformed Services University of Health Sciences, 2014

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN NETWORK OPERATIONS AND TECHNOLOGY

from the

NAVAL POSTGRADUATE SCHOOL
June 2021

Approved by: Alex Bordetsky
Advisor

Eugene Bourakov
Co-Advisor

Edward L. Fisher
Second Reader

Alex Bordetsky
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Detecting unmanned aerial systems (UAS) is complicated. Integrating and sharing radar information across multiple domains (air, land, and sea) is a problem. Current research on UAS detection focuses primarily on detecting UAS over ground forces and national critical infrastructure, but what happens when UAS starts challenging warships in a harbor or open ocean? How can information be collected and shared wirelessly during a multi-agency crisis event? Could detected UAV sensor data be shared in a wireless mesh network (WMN) with other agencies? Our study demonstrated the possibility of integrating simulated data from SAAB's G1X radar system, integrated with the Tactical Assault Kit (TAK) situational awareness application, during a small-scale multi-agency crisis response exercise. The technology worked flawlessly; however, we noticed that counter UAS tactics techniques and procedures (TTP), international UAS laws and regulations, and cueing and automation must be further examined and reworked for today's fight and interagency response. In addition, we discovered that cell phone coverage did not effectively cover San Francisco Bay during the exercise. To mitigate this gap, we successfully extended a WMN using Persistent Systems' MPU-5 radios to create a broader capability of maintaining network functions in a non-networked environment.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

3D	three-dimensional
AESA	active electronically scanned array
AGL	above ground level
AOR	area of responsibility
APAN	All Partners Access Network
API	application programming interface
ATAK	Android Tactical Assault Kit
C2	command and control
CBRN	chemical, biological, radiological, and nuclear
CIV-TAK	civilian tactical awareness kit
COP	common operating picture
COT	cursor-on-target
COTS	commercial off the shelf
COVID-19	Coronavirus 2019
CRADA	cooperative research and development
CST	Civil Support Team
C-UAS	counter-unmanned aerial system
DHS	Department of Homeland Security
DJI	Da-Jiang Innovations (‘Great Frontier Innovations’)
DOD	Department of Defense
EAR	Export Administration Regulations
EDS	electronic defense systems

ELSS	enhanced, low, slow, small
EOIS	electrical, optical, infrared sensors
ESC	electronic systems center
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
G1X	Giraffe 1X
GBAD	ground-based air defense
GINA	global information network architecture
GPS	global positioning system
GUI	graphical user interface
IED	improvised explosive device
IEEE	Institute for Electrical and Electronic Engineers
ITAR	International Traffic of Arms Regulations
JCO	Joint C-sUAS Office
LSS	low, slow, and small
MFK	mobile field kit
MIL-TAK	military tactical awareness kit
MIMO	multiple-input multiple-output
MPU	man-portable unit
NGA	National Geospatial-Intelligence Agency
OODA	observer, orient, decide, act
PRND	preventive radiological, nuclear detection
RADAR	radio detection and ranging
RAM	rocket artillery mortar

RAP	radiation assistance program
RCS	radar cross-section
RF	radio frequency
S.A.	situational awareness
SSL	secure sockets layer
TSA	Transportation Security Administration
TTP	tactics techniques procedures
UAS	unmanned aerial systems
UAV	unmanned aerial vehicle
U.S.	United States
USCG	United States Coast Guard
VHF	very high frequency
W3	what, when, where
WLAN	wireless local area network
WMN	wireless mesh network
XML	extensible markup language

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First and foremost, I, Derrick Majors, would like to thank my wife, Suphawadee (Pooh); without her unconditional love and support, I would not be able to complete this research. As for my immediate family, thank you for supporting me every step of the way. I hope that we continue to make many memories together and go on to more exciting adventures! To the students here at Naval Postgraduate School, thank you for taking your time sharing your experiences and helping me expand my knowledge.

I, Ryan O'Neil, would like to first thank God for all the blessings He has given me throughout my career. Being able to spend this time here in Monterey has allowed so many growth opportunities in my life. I would also like to thank my wife, Phoebe, and four children: Regan, Brianna, Cameron, and Finn, for their support and encouragement for the past two years. Finally, I am grateful for the many friendships that I have gained while being here and the fellowship we were all able to experience together. This community has been one of the most loving and encouraging that I have ever been a part of.

We wish to extend our deepest gratitude to Professor Alex Bordetsky and his intellectual curiosity, positivity, and encouragement that pushed us to see the light at the end of a dark COVID-19 tunnel. Eugene Bourakov, you were instrumental to our success and were ever patient with us. To the first responder community in San Francisco, thank you for allowing us the environment to test our theories and be a part of our experimentation. A special thanks to Phil White, Dave Trombino, Jim Gordon, and Kevin Kem; you guys were a power team that made the impossible possible. Last but certainly not least, we are grateful to have been a part of the SAAB Team. Ludwig Wenklo, Håkan Warston, Anders Petersson, Björn Andersson, Bo Wallander and Vilhelm Bergman: your positive spirit and can-do attitude pushed us through to the finish line. Thank you for spending countless nights after work providing us with feedback and encouragement. Hopefully, we will get to meet up in the future.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

It is 1200 on a beautiful sunny day when a United States Navy vessel pulls into a large metropolitan port for fleet week. As the ship approaches, it turns off its air search radars per Federal Communications Commission (FCC) regulations. The detection and identification of any aerial threat will now depend upon the visual aptitude of watch standers on deck. The metropolitan port's security is directly responsible for the safe transit of that vessel, and so far, all is going like any typical day. However, unbeknownst to either party, a malicious actor launches several unmanned aerial vehicles (UAV) with attached improvised explosive devices (IED) headed to intercept the naval vessel.

This scenario may sound like a pitch to a new bestselling fictional novel, but with the proliferation of small UAVs for private hobby and commercial use comes a very likely real-world threat that could have profound consequences. A UAV can be purchased and equipped with an explosive payload for relatively low cost and be covertly flown over national critical infrastructure, military bases, national borders, and military equipment/ personnel. The miniaturization of technology and navigation and battery life advancements have given rise to comparatively highly advanced commercialized UAV technology, supplying several low, slow, and small UAVs for malicious actors to use.

To highlight three cases of UAVs in the U.S. and national security, on September 29, 2019, five or six UAVs were spotted circling the Palo Verde Nuclear Generating Station inside and outside of protected areas (Rogoway & Trevithick, 2020). Palo Verde dispatched a security team and called the police department, but they could not locate the perpetrators (Rogoway & Trevithick, 2020). This case may have been a UAV hobbyist flying their UAVs over the nuclear facility's security perimeters, or it may have been a malicious actor gathering reconnaissance for a future attack. Due to the remote nature of how UAVs are operated, the perpetrators were able to evade detection and escape undetected.

Reporters Adam Kehoe and Marc Cecotti (2021), writing for *The Drive,* tell a tale of multiple nights that unknown UAVs flew over several USN Destroyers. On the night of

July 14th, 2019, around 2200, the USS Kidd initially spotted two mysterious UAVs (Kehoe & Cecotti, 2021). This sighting prompted the USS Kidd to go through a series of tactics, techniques, and procedures (TTP) for an unknown flying object. The reporters go on to discover that a total of five or six UAVs were reported to have flown around five USN Destroyers and several commercial vessels 100 nautical miles outside of Los Angeles. Additionally, the UAVs flew for over 90 minutes and at a range that is uncharacteristic for any commercially available UAV. The UAVs continued to flash a series of lights prompting reactions from the crew and investigators. Kehoe and Cecotti (2021) dug deep with Freedom of Information Act (FOIA) requests to discover that official investigation launched immediately on July 17th, 2019, and continued through July 25th, 2019, when their FOIA requests were denied due to classification levels. This investigation took several days and included numerous investigators from several agencies coordinating numerous efforts to determine the intent and identify of the UAV operators. Although nothing significant was revealed by the FOIA requests, this case highlights a requirement for UAV detection, tracking, and coordination across military branches.

In another incident in May of 2020, the U.S. Customs and Border Protection agents near Yuma, AZ, seized $300,000 worth of cocaine and methamphetamine flown by one UAV over the U.S. southern border from Mexico (Ingram, 2020). The report goes on to state that Yuma Sector Border Patrol Agents are using night vision googles to monitor the area for UAVs (Ingram, 2020). In these cases, UAVs were used as low-cost solutions for high monetary rewards. UAVs come with an added benefit for malicious perpetrators having an exceedingly small probability of detection.

In an article entitled “Joint Counter-sUAS Strategy to Address Need for Improved Technology,” Devon Suits (2020) paraphrased Maj Gen. Sean A. Gainey: “The increased threat posed by drones, combined with a lack of dependable networked capabilities to counter the unmanned threat, has created a concerning “tactical development” within U.S. Central Command’s area of responsibility” (Suits, 2020, para. 3). The unmanned threat is the most known, unknown threat.

A. PURPOSE

This thesis will examine integrating an electronic phased array radar system into a situational awareness tool to enhance decision-making capabilities for the Department of Homeland Security (DHS) and the Department of Defense (DOD) to defend against unmanned aerial vehicles (UAV)s. We will be utilizing SAAB's Giraffe 1X radar, which allows for a radar capability to identify Enhanced Low Slow Small (ELSS) UAVs while also being small enough to be utilized on a mobile platform. The Giraffe 1X (G1X) can be mounted onto the back of a truck or a small naval vessel, allowing for rapid mobility and minimizing the required setup time. We will be utilizing the Android Tactical Assault Kit (ATAK) for the situational awareness tool platform. Since its development in 2010, ATAK has been deployed in a magnitude of crisis events overseas and at home. For instance, ATAK is regularly deployed as a situational awareness tool during presidential inaugurations, hurricane disaster relief where multi-jurisdictional responders must report to multiple command posts, and most recently has been deployed by the Army National Guard for COVID-19 response (CIVTAK, 2020).

Study in this area is essential because detecting incoming UAV threats at a greater distance allows for an increased decision-making window, as identified in Colonel Boyd's OODA Loop model, and opens the window for UAV threat avoidance. With this added time, on-scene commanders can align forces and counter the incoming UAV threat before it is too late. Additionally, by extending radar data over a wireless mesh network (WMN), units at sea are provided the flexibility of transmitting data in an area that has a degraded network capability or no networking capability at all.

B. RESEARCH OBJECTIVES

Our research evaluates the integration of radar, communications networks, and situational awareness tools in defense against UAS. This study intends to answer this question:

- How does the integration of the Giraffe 1X (G1X) radar and Android Tactical Assault Kit contribute to the DOD and DHS security forces' enhanced decision-making within a naval port?

This study examines the capability gaps and potential utility of using a radar sensor integrated with ATAK for UAV detection in a littoral maritime environment. Our research shows that:

1. The integration of G1X radar sensor data and ATAK utilizing Cursor on Target (COT) messaging is feasible and sustainable.
2. Although there are many situational awareness tools to choose from, the DOD and DHS rely heavily on very-high frequency (VHF) voice circuits for counter UAV coordination.
3. If not trained and proficient in the tools being utilized, new technology can become overwhelming, not used, and may not contribute to the decision-making process.
4. Tactics, techniques, and procedures (TTP) regarding UAV detection and mitigation must be updated and promulgated to all relevant agencies.

C. SCOPE

The general scope of this thesis is to examine the integration of UAV detection capabilities and situational awareness tools that are currently available to assist the Department of Defense and Department of Homeland Security.

We chose to work with the Android Tactical Awareness Kit (ATAK) to demonstrate the capability of situational awareness tools because it was widely available via the Android Play and has already become adapted into many military unit's standard operating procedures (SOPs). ATAK was initially compiled in 2010 by the Airforce Research Laboratory for use by U.S. Special Forces. ATAK provides its users with a display like Google Maps with chat and various custom-built application programming interface (API) plugins. ATAK contains valuable tools when planning missions and sharing valuable mission data. Through the years, it has been used by the U.S. military and has been retrofitted to fit assignments by federal, state, and local agencies.

We chose to work with SAAB AB and their Giraffe 1X 3D multi-mission radar (G1X) because of its ability to detect low, slow, small flyers. SAAB's G1X radar is a small,

lightweight, high-performance electronically scanned array radar that allows for integration with any mobile platform. Our thesis used simulated radar feeds from Sweden and fed them directly into the ATAK system with a custom-built API. We then measured the network for latency and real-time accuracy.

To demonstrate the capability to detect UAVs, we collaborated with the USCG-Sector San Francisco Maritime Preventive Radiological/Nuclear Detection (PRND) enterprise and the Alameda County Sherriff's Office to demonstrate a UAV attack on an ongoing PRND mission. The PRND enterprise was composed of local state and federal maritime first responders under the direction of USCG San Francisco. The demonstration results will be analyzed and reported in Chapter V, discussing situational awareness and diffusion of responsibility issues.

Upon completing the San Francisco Bay demonstration, we evaluated the capability of extending the network using persistent systems multiple-input multiple-output (MIMO) man-portable unit (MPU) generation 5 radios. We used a custom-built network management tool connected to a VHF radio to capture performance data of the G1X data over ATAK on a wireless mesh extended network to assess this capability.

D. LIMITATIONS AND OPPORTUNITIES

We started our thesis in a pre-pandemic environment. This environment may have brought many challenges, but it also provided us with unforeseen opportunities. Additionally, we were able to work around various agreements and international treaties to make our research possible.

1. Coronavirus Disease 2019

Due to Coronavirus Disease 2019 (COVID-19), we had to design new experimentation methods. SAAB was unable to transport their G1X radar into the United States, and due to policy restrictions surrounding flying to a foreign country, we were unable to travel to Sweden. This situation provided us with an unforeseen opportunity to complete our experiments in the "Cyber-Physical." We worked with our foreign partners in Sweden remotely and completed our thesis work here in the United States. This

opportunity presented itself early in our research, and we were able to work with SAAB without being physically present.

2. Cooperative Research and Development Agreement

Cooperative Research and Development Agreement (CRADA) allows students from the Naval Postgraduate School to align their activities with other research and education programs from outside the school. CRADA enables us to work with engineers from defense contractors to bring together our knowledge of operational experience with the technical expertise of skilled engineers. We established a CRADA with SAAB to design a radar in a mesh network. This agreement allows us to experiment with state-of-the-art radar systems and test the technology in the littoral waters off Treasure Island in San Francisco Bay.

3. Exportation of Controlled Technology

Radar technology surrounding the detection of UAVs is technologically advanced and requires due diligence and protection. Advanced technology and intellectual property are protected by the United States Department of State and the Department of Commerce. The Department of State is the approving authority for material controlled by the International Traffic of Arms Regulations (ITAR). The Department of Commerce handles items regulated by the Export Administration Regulations (EAR). To avoid the exportation of controlled technology, we resorted to using simulated radar data created by the G1X radar. This limitation restricted us from using real radar feeds coming from the G1X.

E. SIGNIFICANCE OF RESEARCH

A review of the available literature revealed limited information about the ability of radar systems operating within a wireless mesh network (WMN). Our research explores integrating radar and wireless mesh network technology in defense against unmanned aerial vehicles (UAV). In doing so, we first demonstrated the ability of first responders to observe UAVs during a crisis with and without the assistance of a situational awareness tool. Our results were inconclusive but demonstrated how emerging technologies could disrupt crisis response operations.

In the second part of our research, we extend an ATAK network over a WMN and document network performance while transmitting radar data. In this part of our research, we annotate that ATAK performance is highly dependent on the server's ability to process the information. We believe this information will be helpful in the future when building out a wireless mesh network (WMN) in defense of UAVs within a limited communications environment. WMNs provide a structure of network flexibility where any participant in the network may become the backbone router giving access to the internet. Additionally, these networks work in communications denied environments where data is transferred at high data rates. WMNs are self-organizing, and self-healing which provides the flexibility of nodes and sensors to be able to seamlessly leave and re-join the network when they are within communications range.

For future research, we hypothesize that artificial intelligence/machine learning will be required to process the enormous amounts of information various sensors receive and decipher the data to provide battlefield awareness.

RADM Doug Small, USN, is the Commander of the Navy Warfare Information Systems Command (NAVWAR), leading a global workforce of 11,000 civilian and military members developing and deploying advanced communications systems by Sailors and Marines worldwide (Center for Strategic and International Studies [CSIS], 2021). According to RADM Small, Project Overmatch results from the Great Power competition and United States adversaries challenging freedom of maneuver on the seas in international waters (CSIS, 2021). RADM Small stated that the United States adversaries are gaining numerous technological advantages to challenge the United States and restrict freedom of maneuver in international waters (CSIS, 2021). Our research seeks to create an enhanced distributed maritime operational picture by demonstrating a situational awareness tool, communicating over a wireless mesh network, synchronizing the effects of a distributed Naval force.

F. ORGANIZATION OF THESIS

Our thesis is organized into six main chapters. Chapter I is our introduction. It is based upon a real-life scenario surrounding fleet week. Chapter II focuses on the

background of the models, doctrine, and tools we will be covering. Chapter III is our literature review. Our literature review examined prior research regarding UAV detection technologies and decision-making frameworks. Chapter IV consists of our experiment design. In our experiment design, we cover the four phases required to cover all the objectives we set out to research. Phases III and IV consisted of live experimentation of our models.

Phase III was based upon a PRND mission in San Francisco Bay. During the PRND mission, first-responders faced a demonstrated UAV surveillance and attack by hostile UAVs without situational awareness technology. In the second part of our demonstration, we introduce the ATAK situational awareness tool to help first responders detect UAVs. We proposed that by using ATAK, first responders would be better equipped to handle a UAV threat.

Phase IV was based on ATAK's ability to receive radar feeds through an extended wireless mesh network. This design is used to test using the ATAK network in a littoral maritime setting without using any internet connection. Two or more ATAK devices can be connected via a stretched Wi-Fi network link to maintain connectivity if the cellular network is down or not presented in the area. For example, an extended connection can be established via a mesh network utilizing MPU5 radios by Persistent Systems.

Chapter V discusses our findings and produces recommendations for potential solutions. Chapter VI gives a summary of our results and annotates the limitations of our research. Additionally, we annotated further research that piqued our interest, but the research was outside our thesis's scope and time constraints.

II. BACKGROUND

> The United States is a maritime nation. Our security and prosperity depend on the seas. The Naval Service—forward deployed and capable of both rapid response and sustained operations globally—remains America's most persistent and versatile instrument of military influence. Integrated All-Domain Naval Power, leveraging the complementary authorities and capabilities of the U.S. Navy, Marine Corps, and Coast Guard, advances the prosperity, security, and promise of a free and open, rules-based order.
>
> - USCG, USMC, and USN, *Tri-Service Maritime Strategy*

Advantage at Sea Prevailing with Integrated All-Domain Naval Power is commonly referred to as the *Tri-Service Maritime Strategy*. Published at the end of 2020, the *Tri-Service Maritime Strategy* highlight's that today's maritime security requires the three maritime services to collaborate their technology, roles, investments, and authorities (USCG, USMC, & USN, 2020). The USN must work together in a joint effort with the USMC and USCG and as an international coalition to promote free and open trade of the seas. This strategy alludes to synchronizing multiple efforts to fight budget pressures and greater maritime competition. In doing so, we believe the maritime services must look at their current force structures and create a single collaborative command and control situational awareness picture that can be shared across their branches.

This chapter will provide pertinent background information to include terminology and definitions, C-UAS strategic policy, current sensors, tactical awareness kit, and Ret. Col John Boyd's (2007) observe orientate decide act (OODA) loop decision-making model.

A. TERMINOLOGY/DEFINITIONS

The terms surrounding unmanned aerial systems tend to become obfuscated. For instance, some literature tends to use the terms drone, unmanned aerial vehicle (UAV), and unmanned aerial system (UAS) interchangeably, but there are differences.

When referring to unmanned aerial vehicles, the term drone first appeared sometime after U.S. Admiral William Harrison Standley witnessed a test flight of the

British Royal Navy's DH 82B Queen Bee (Daly, 2020). Daly explains that the Queen Bee was a low-cost radio-controlled aerial vehicle with its sole purpose to be used for target practice (Daly, 2020). Using the Old English definition for drone and its history, the term drone implies that the specified unmanned aircraft has only one repetitious job.

The description of a UAV is an aircraft that can fly either autonomously or with a remote pilot controlling the flight. "Drone" is also a term that could be used to describe this vehicle. This description limits itself to specifying only the vehicle itself and no other components.

UAS includes the UAV and every other component that involves the operation of the flight. UAS consists of the remote, the pilot, the ground control station (GCS), and the communication links. Detection of the presence of UAS can be achieved not only through radar detecting the vehicle itself but also through the means of detecting the radio frequency of the communication links.

This thesis's focus will be on detecting unmanned vehicles using radar capabilities; therefore, the term UAV will be used predominantly. However, much of the literature we will be referring to uses the term UAS or drone, and we will use those terms, respectively.

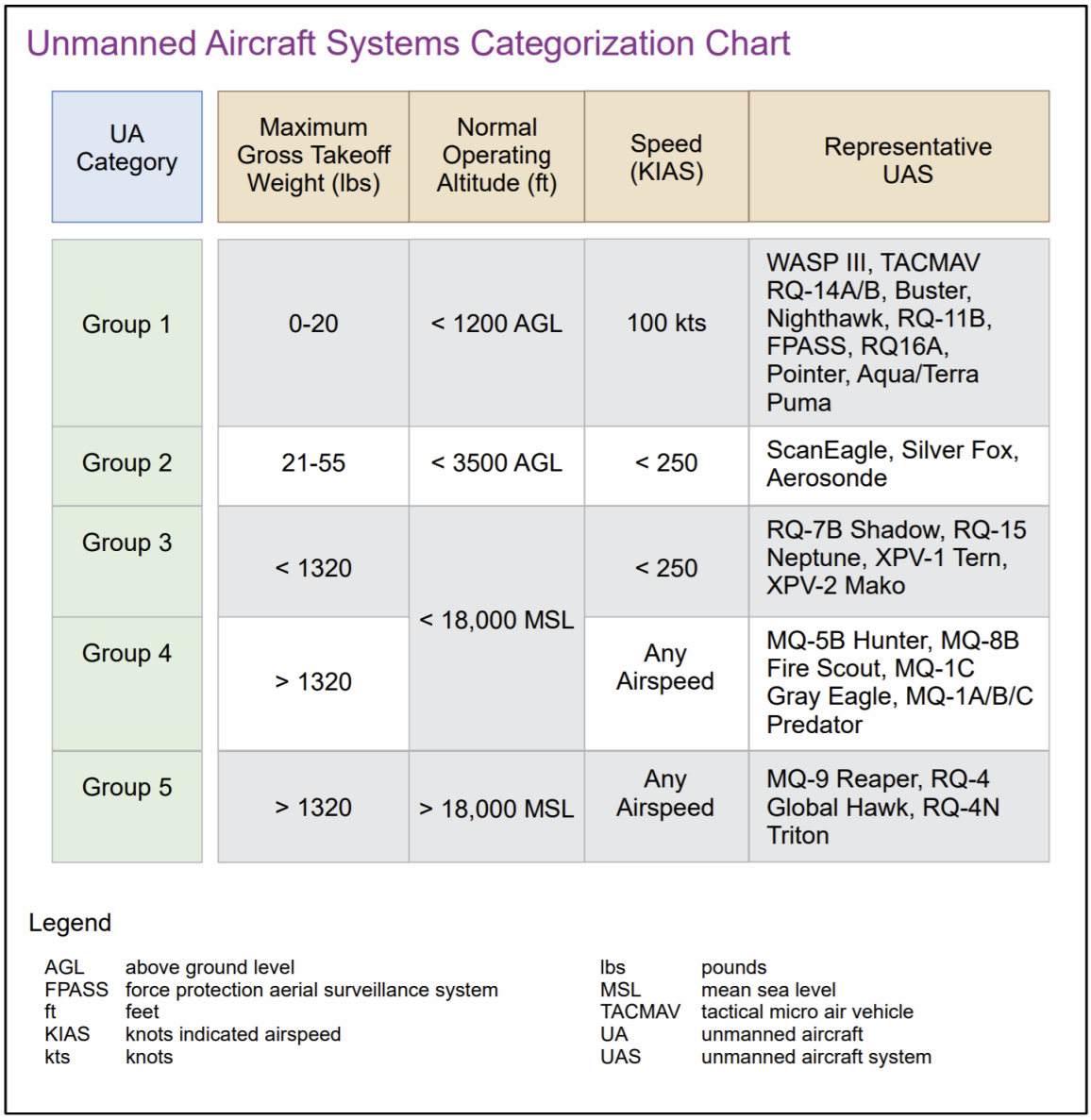
B. COUNTER UNMANNED AERIAL SYSTEMS STRATEGIC POLICY

In 2021, acting Secretary of Defense (SECDEF), Christopher Miller, signed the Department of Defense's (DOD) Counter-Small Unmanned Aircraft Systems (C-sUAS) Strategy. In this strategy, the DOD highlights the increasing threat of UAS applications against DOD operations in the air, land, and sea (Department of Defense [DOD], 2021). The DOD initially embraced the challenge of countering UAS; however, until recently, without clear and concise overarching guidance. This caused the DOD to create numerous and redundant stove-piped solutions to solve tactical issues. The C-UAS strategy breaks down its strategic approach into three lines of effort: readying the force, defending the force, and building the team (DOD, 2021).

The C-sUAS strategy looks at taking a new strategic approach (DOD, 2021). In this approach, the DOD highlights the importance of creating innovative and efficient systems

to minimize budgetary constraints. The DOD's processes must be able to adequately respond to the ever-changing security environment (DOD, 2021). Similar to the *Tri-service Maritime Strategy,* the DOD should "prioritize interoperability and information sharing" with its international partners (DOD, 2021, p. 10). This high-level strategy breaks down how the DOD is coordinating its efforts to push innovation and strengthen its relationships with its international allies and partners. The strategy points out that in 2019 the Secretary of the Army (SECARMY) was designated as the DOD Executive Agent for Counter UAS systems in groups one, two, and three (DOD, 2021); however, what are UAS groups one, two, and three?

For information on UAS groups one, two, and three Joint Publication 3-30 "Joint Air Operations" published by the Department of Defense in 2019 "provides principles and guidance to plan, execute, and assess joint air operations" (Joint Chiefs of Staff [JCS], 2019). The joint publication covers the employment of UAVs to include counter UAV operations. There is a wide range of UAV size and operating characteristics; therefore, the DOD categorizes each UAV based on its weight and flight characteristics (altitude and speed) (JCS, 2019). There are five separate categories, see Figure 1 (JCS, 2019). The first three groups of UAVs represent more miniature and inexpensive UAVs. Groups 4 and 5 represent state-controlled larger UAVs.



Unmanned Aircraft Systems Categorization Chart

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

Legend

AGL	above ground level	lbs	pounds
FPASS	force protection aerial surveillance system	MSL	mean sea level
ft	feet	TACMAV	tactical micro air vehicle
KIAS	knots indicated airspeed	UA	unmanned aircraft
kts	knots	UAS	unmanned aircraft system

Figure 1. UAS Categorization Chart. Source: JCS (2019, pp. 31).

C. NEURAL NETWORKS AND MACHINE LEARNING

Modern-day science has pushed humanity's understanding of biology further than in the past; however, we still do not fully grasp the understanding of nature. Creating a machine with the ability to distinguish a UAV versus a bird or other flying objects is challenging, like a child trying to distinguish an apple from a tomato.

William McDougall, a 20th-century psychologist, first explored comparative judgment in his 1923 book *An Outline of Psychology*. In his book, he describes how a child learns to distinguish an apple from a tomato:

> The function of comparing two things, or making a comparative judgment, in explicit discrimination. It is discrimination proceeded by suspense of judgment, doubt, and explicit inquiry. The young child who has learned to discriminate the tomato from the apple, I.e., has learned to react differently on the sight of apple and tomato, may later have occasion to discriminate between two such objects by explicit comparison. This is not fully achieved, until he learns to name the two objects, and formulate his doubt in the form of a question and the result of his judgment in the form of a proposition. Shortly stated, comparison which discovers difference of discrimination on the plane of explicit judgment; and comparison which discovers likeness is explicit recognition. (McDougall, 2018, pp. 385–386)

Distinguishing an apple from tomato is just a rudimentary task that takes extraordinarily little brain power to the average three-year-old. So how hard could it be for a computer programmer to encode this process for a machine?

In Paul Scharee's (2018) book *Army of None: Autonomous Weapons and the Future of War,* he explains the challenge of explicit programming comparisons with a rules-based approach. Scharee (2018) uses a simple example of how a three-year-old child can immediately distinguish an apple from tomato, and a computer may need millions of pieces of data to achieve the same result. He goes on to explain how a machine uses a neural network as a shortcut by learning from millions of pieces of data to adapt its internal programming structure until the machine optimizes the specified goal (Scharee, 2018). In this case, it was visually distinguishing the difference between an apple and a tomato.

Based on our research and readings, not until recently could a computer accurately distinguish an apple from an orange. Machine learning has enabled programmers to create a model that can use features and data points to generate a prediction if the object is an apple or an orange (Garbade, 2018). How does a machine gain the ability to sense its surroundings?

D. CURRENT UNMANNED AERIAL SYSTEMS DETECTION METHODS

Current UAV detection methods rely on a range of sensors and situational awareness tools. Machines use sensors like radar, radio frequency, heat sensing, electrical optical infrared (EOIR), and sound monitoring. These sensors are for machines, like how senses are for people. Machines perceive the world through various sensors which are programmed by humans to perform specific tasks. Sometimes tasks such as reporting unknown UAVs flying in a designated area come back as false-positive reports. This is especially true when a machine is attempting to distinguish a UAV from a bird.

We will examine how a machine may be able to detect a UAV or UAS using some unusual types of "senses" such as radar, radio frequency (RF), acoustic, and electrical optical infrared (EOIR) sensors. In some settings, it will be easier to detect a UAS versus a UAV and vice-a-versa. For example, a mariner on the fantail of a vessel may hear a UAV long before it is ever seen. This example is like a machine being able to detect a UAV while using a phased array radar versus listening for its RF signature.

1. Radio Detection and Ranging

In the late 1880s, German physicist Heinrich Hertz experimentally proved the theoretical work on electromagnetic waves theorized by James Clark Maxwell (Skolnik, 2020). The encyclopedia explains how Maxwell had theorized how electromagnetic radio waves could be refracted off metallic objects like light waves (Skolnik, 2020). Heinrich Hertz proved this was possible in 1888 utilizing RF at 455MHz (Skolnik, 2020). Later during World War II (WWII), the British Royal Airforce (RAF) used similar technology against German long-range bombers gaining an early advantage (Skolnik, 2020). Skolnik (2020) states that many countries before WWII developed several other methods of aircraft detection, such as infrared (I.R.) sensors and acoustic noise sensors. Still, these technologies were not as valuable as radar (Skolnik, 2020). This information is essential to our study because radar provides over-the-horizon detection capabilities that are not available with I.R. and acoustic sensors.

In J.R. Mentzer's 1955 book, *Scattering and Diffraction of Radio Waves*, the acronym "radar" was first coined in 1940 by the United States Navy. Mentzer gives credit

to Lieutenant Commander S.M. Tucker and Lieutenant Commander F.R. Furth. With the approval of Chief of Naval Operations (CNO) Admiral H. R. Stark, the term for using electromagnetic waves to detect metallic objects and determine their range officially became radio detection and ranging (RADAR) (Mentzer, 1955). Pulse radars operate by sending out modulated electromagnetic (EM) waves from the radiofrequency (RF) part of the EM spectrum. Those waves bounce off objects and are returned to the receiver. The received signal is then amplified, processed, and displayed on a screen for an operator to interpret.

Many improvements have happened since the first pulse radar system was first introduced. These following two radars utilize active electronically scanned arrays (AESA). AESA radars are phased arrays in which the RF beams are electronically steered without moving the antenna. The digital nature allows AESA radars to scan more efficiently than their rotating predecessors (Mishra, 2018). The SAAB Giraffe and FLIR are two examples of AESA radars.

a. SAAB Giraffe Radars

In 2019, SAAB debuted their G1X radar mounted on a Supacat Jackal vehicle at the Digital Economy and Society Index 2019 (DESI-2019) (Defense World.net, 2019). A Supacat Jackal Vehicle is an agile light patrol vehicle able to do rapid assault and fire support; see Figure 2.

Figure 2. Supacat Jackal with Mounted Giraffe1X Radar. Source: SAAB, Personal Communications (2020).

Defense World.net (2019) explains that the mission of the G1X is to provide a compact, lightweight, 3D electronic scanned array radar capable of deploying at airports and myriad types of land and sea vehicles. 3D signifies the ability of a radar to sense three dimensions of an object to include its' distance, range, and altitude. Unlike traditional radars, electronically scanned arrays consist of several antennas, each with its own solid-state transmit-receive module controlled by computers that function as a transmitter and receiver. The Giraffe1X radar can provide simultaneous air surveillance, Rocket, Artillery, and Mortar shells (RAM) detection, and Enhanced Low, Slow, and Small (ELSS) surveillance. It can integrate its targeting data into several situational awareness applications.

The G1X enables flexibility and redundancy in ground-based air defense systems (SAAB, 2020). The G1X's scan rate covers the entire search area once every second. The G1X is an ideal sensor as a C-UAS solution. The total system weighs under 150kg and can be transported on a pickup truck, helicopter, trailer, or boat (SAAB, 2020). Quick to set up and use, the radar can be moved from a pickup truck to a fixed position on a building. Given its mobility and ability to transmit while moving, it can also follow the "frontline" or an ongoing operation in a way a larger sensor could not.

b. FLIR Ranger R6SS

The FLIR Ranger R6SS was first announced in 2016 at a Special Operations Forces Industry Conference in Florida (Tomkins, 2016). Tomkins explains the Ranger R6SS ground surveillance radar can detect and track objects up to a 15-km range using its digital beam-forming and incredible refresh rates. FLIR uses an electronically scanned mid-range radar to detect and track large vehicles up to a 15km range (Tomkins, 2016). The FLIR Ranger R6SS may be mounted on an LTV-X, see Figure 3.

Figure 3. FLIR Systems' LTV-X Vehicle and Ranger R6SS. Source: Tomkins (2016).

2. Radio Frequency

In Marc Raboy's (2018) book *Marconi: The Man Who Networked the World*, Italian inventor Guglielmo Marconi is described as a man who envisioned a world without communication borders. Raboy (2018) explains that in 1896 at the age of twenty-two Marconi first applied for a patent in England entitled "Improvements in Transmitting Electrical Impulses and Signals, and in Apparatus," therefor patenting the first radio wave communications system. Marconi is known as the father of the radio. His inventions and studies furthered wireless technology and have paved the way for radio broadcasts, radars, and wireless communications.

Two popular drone detection systems that use RF include the Aeroscope Detector and Aaronia Drone Detection System. Both systems use an RF detector to detect the controller communicating control signals to the UAV. There are additional RF sensors on the market, but we chose to work with these two as Aeroscope has the ability to detect all DJI manufactured drones, and Aaronia's systems are currently deployed to protect airports and national critical infrastructure.

a. Aeroscope Detector

One way to identify UAVs is to look for RF signals sent between the controller and the UAV. Aeroscope is a comprehensive UAS detection platform that identifies UAS communication links between the controller and the UAV (Da-Jiang Innovations [DJI], 2020). see Figure 4 for a picture of a stationary DJI Aeroscope in use.

Figure 4. DJI Aeroscope from Airworks. Source: Trading (2020).

Aeroscope creates its situational awareness by listening to RF transmitted from the user to the UAV. The RF gathered is then processed against a database of known UAV signals, and an RF fingerprint is built. The fingerprint is built using the aircraft's broadcast GPS, altitude, speed, orientation, model, serial number, and Home Point (DJI, 2020). Aeroscope has a few key features that separate it from many other UAV detection devices, listed in Table 1.

Table 1. Description of Aeroscope Features

Feature	Description
Developed by DJI	DJI drones are the most popular in circulation. 8 out of 10 of the most popular drones were made by DJI (Feist, 2021). Being developed by DJI, Aeroscope is uniquely suited to know the model, signature, serial, and other identifying characteristics of most drones being flown.
Remote ID	Aeroscope is a Remote ID system that has played a significant role in promoting the Remote ID capability. Remote ID is an electronic signature that the UAS gives off that is linked to the pilot's registration. Authorized officials may use this information to monitor and track safe UAV flights. (DJI, 2019)
Geofence	"Aeroscope allows users to implement their own Geofence zones around their property. Geofencing allows the creation of a 'warning zone' and an 'alert zone' based on a specific block or street" (Miller, 2020, para. 6).

As discussed earlier, RF detection is accomplished by tracking and capturing the radio frequency emitting between the pilot or station and the UAV. “Tapping” into an electronic signal without a court order could lead to a criminal lawsuit. Aeroscope faces many challenges surrounding federal regulatory statutes including, the Pen/Trap Statute, 18 U.S.C. Sections 3121–3127, and the Wiretap Act Title III, 18 USC Section 2510. These statutes primarily protect privacy from any entity “recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications” (Federal Aviation Administration [FAA], 2020).

b. Aaronia Drone Detection System

The advanced automatic radio frequency tracking and observation solution (AARTOS) drone detection system was developed by the German-based radio frequency and microwave equipment manufacturing company, Aaronia. It is advertised to provide UAV defense for airports, critical infrastructure, events, military, police, correctional facilities, very important people (VIPs), yachts, and border protection (AARONIA AG, n.d.a). AARTOS uses the RF radiation emitted from the UAV to the operators’ control unit to detect UAVs. The AARTOS scans frequencies between 9 kHz to 20 GHz using 16 or 32 antennas and a spectrum analyzer to provide surveillance (AARONIA AG, n.d.a). The range is highly dependent on the drone operator’s transmitter power. It can detect a larger fixed-wing drone at 5 km, a professional multi-rotor at 3 km, and other typical commercial drones at 700 m (Hindle, 2018). There are three primary components to the AARTOS: a jammer, command center, and tracking antenna, see Figure 5.

Figure 5. AARTOS Drone Detection System. Source: Hindle (2018).

This system is designed to have a C-UAS capability already in place. The jammer module is an omni directional 3D antenna array handling up to 800 watts of output power with a reported range of up to 8 km (AARONIA AG, n.d.b). The jammer works like a counter-radio-controlled electronic warfare (CREW) system. It projects a high-energy signal towards the detected drone to disrupt the communication link between the pilot and the drone.

E. ACOUSTIC SYSTEM FOR UAS DETECTION

Using acoustics to detect UAVs is a fairly new method. Dumitrescu et al., (2020) utilized a spiral microphone array into two concurrent neural networks to determine and classify UAVs within an outlined perimeter, see Figure 6. The purpose of their research was to build a microphone array with cheap, commercial off-the-shelf (COTS) equipment to detect the presence of drones (Dumitresu et al., 2020). Their research found that there are extreme limitations of acoustic detection of UAVs. During their experimentation, large multirotor UAVs of 1.5 meters in diameter may be detected at 500 meters. Smaller multirotor UAVs with a diameter of less than 1 meter can be detected at 380 meters

(Dumitresu et al., 2020). Their research based on competing neural networks in conjunction with spiral microphone arrays to detect and identify UAVs.

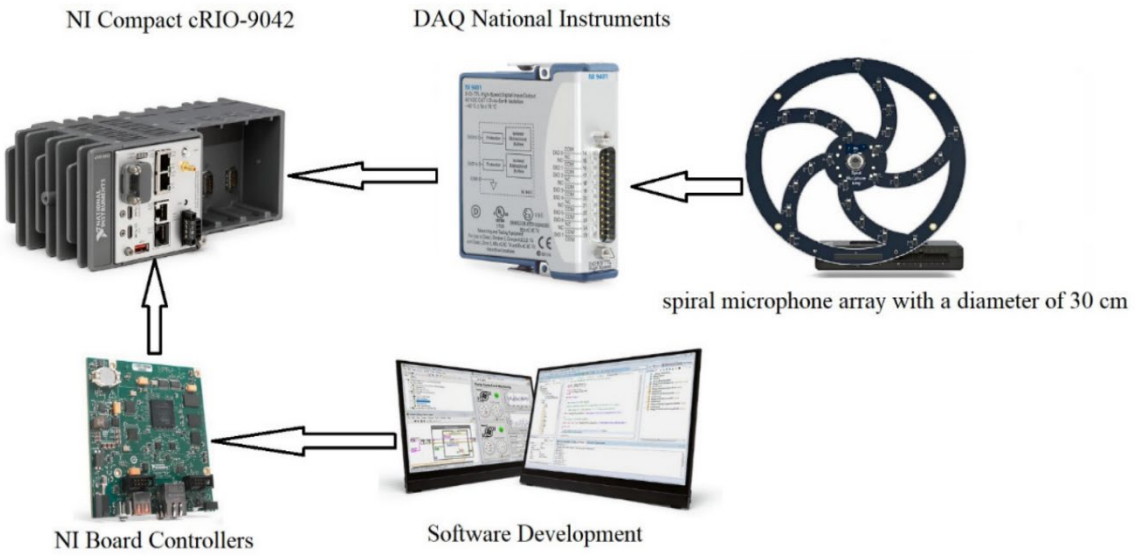


Figure 6. Acoustic System for UAS Detection. Source: Dumitresu et. al. (2020).

F. ELECTRO-OPTICAL INFRARED SENSORS

Electro-Optical Infrared Sensors (EOIS) are being deployed at NASCO shipyards in Japan to provide early warning and target discrimination (NASCO, n.d.). Spynel's I.R. camera paired with the Cylcope intrusion detection software offers a robust solution to detect multiple airborne threats. According to HGH's case study on Spynel integrating multiple sensors is the optimum solution for distinguishing birds from UAVs (HGH Infrared Systems, n.d.). Birds create a unique challenge as UAVs and birds are non-metallic, similar in size, and relatively slow-flying objects. Consequently, birds create numerous false negative alarms.

G. CURSOR ON TARGET

The U.S. Military communicates on hundreds of systems over numerous computer languages. This makes finding a common language a highly complex task. According to Metcalfe's Law, the complexity of interconnecting networks compounds exponentially as

the number of networks increase. Mathematically the number of interconnecting networks can be calculated by using *n* squared. Metcalfe's Law makes finding the intersection of nodes extremely difficult. To combat this problem, in 2009, MITRE developed a message router and named it Cursor-on-Target (COT) Message Router (Kristan et al., 2009). MITRE initially created COT in 2002 to support the U.S. Airforce Electronic Systems Center (ESC) to allow for interconnected systems to communicate, targeting data autonomously without a human in the loop (Paone, 2010).

MITRE took on a new perspective to the problem by looking at the union of datasets and discovered that the Department of Defense tactical systems were highly dependent on transmitting three critical data sets "What, When, and Where" (W3). This minimalistic approach was taken due to tactical forces having limited bandwidth, and it offers a solution for tactical units to transmit tracking data. COT consists of a terse schema with 12 mandatory fields describing the W3 data, see Figure 7 (Kristan et al., 2009).

```
<?xml version='1.0' standalone='yes'?>
<event version="2.0"
    uid="J-01334"
    type="a-h-A-M-F-U-M"
    time="2005-04-05T11:43:38.07Z"
    start="2005-04-05T11:43:38.07Z"
    stale="2005-04-05T11:45:38.07Z" >
  <detail>
  </detail>
  <point lat="30.0090027" lon="-85.9578735" ce="45.3"
             hae="-42.6" le="99.5"  />
</event>
```

Figure 7. Example of COT schema. Source: Kristan et al., (2009).

THIS PAGE INTENTIONALLY LEFT BLANK

III. LITERATURE REVIEW

Previous work that shapes our research includes prior work around UAV detection and integration between sensor detection data and situational awareness tools. We also provided a review of current UAV detection systems available to date. This review can provide a contribution to the body of knowledge for future research relating to UAV detection capabilities. Detection of a UAV is the first stage of situational awareness, which is the start of decision-making. This chapter concludes with a review of three decision-making models and a sense-making framework that can better guide the decision-making process.

A. PRIOR WORK

From 2010 to 2021, nine theses have been produced out of NPS, research seeking how the ATAK device can be better utilized in each author's warfare community. Of the total nine, the research conducted by MAJ Brandon Davis and William Whittaker, USMC, sought to determine how the utilization of ATAK integrated with detection sensors can enhance decision-making and survivability of special operation force (SOF) teams against a UAV threat (Davis & Whittaker, 2019). In their research, Davis and Whittaker explored how the SOF community requires a UAV detection sensor that would be relatively small, lightweight, portable, and allowed for rapid set-up and take down. For this reason, they were able to rule out SAAB's Giraffe 1X from their experimentation. Davis and Whittaker explore their specific research question by focusing their testing on the operator of the ATAK device and less on the sensor itself. Because of this, their experimentation utilized ATAK, a Dowding Server, and a SkyView radio frequency sensor. Their research found successful results of real-time SkyView sensor data over the ATAK device. Our aim is to build from this previous work and utilize a radar capability vice an RF capability and look at how the radar technology integrates into ATAK. We will also focus on how decisions are made and what frameworks and models can be explored to better understand how decision-making is connected to a potentially novel threat yet to be fully explored.

B. UNMANNED AERIAL VEHICLE DETECTION

Detecting a UAV sounds like a straightforward task; unfortunately, this task is daunting for machines. First, machines do not have the natural ability to see. A variety of research has gone into machine recognition techniques and networking various sensors to correlate collected data. UAVs can be detected in numerous ways, such as using radio frequency (RF), radar, sound, and electrical optical infrared (EOIR), to name a few. The main limiting factor between these technologies is cost. For instance, a phased array radar system may cost anywhere between $150,000 and $300,000 (Egozi, 2020), and an RF-only technology such as the DJI portable Aeroscope costs $7400 (Phoenix Future Technologies, n.d.).

C-UAV depends on the ability of technology to detect and track UAVs. The first obstacle for many researchers was to develop technologies that can distinguish a UAV from a bird. To solve this problem, a multitude of researchers leveraged the fact that UAVs and birds have different flight patterns. From there, researchers applied deep learning and convolutional neural networks on UAV photography to determine if a flying object was a UAV or bird. The next hurdle for UAV detection in an expeditionary environment is how to provide enhanced command and control with a radar without an internet connection.

1. Radio Frequency

Recent studies have shown that radio frequency (RF) within communication links can identify the brand and type of UAV flying. For instance, in a 2019 North Carolina State University study entitled “Micro-UAV Detection and Classification from RF Fingerprints Using Machine Learning Techniques,” researchers used a database of 100 RF fingerprints collected from 14 UAV controllers (Ezuma et al., 2019). The researchers were able to identify and classify those 14 UAV controllers 96.3% of the time (Ezuma et al., 2019). This research is necessary because it shows that machine learning depends on the underlying algorithm and finds that a k-nearest neighbor (kNN) classifier achieves a classification accuracy of 97.29% (Ezuma et al., 2019). A NASA (National Aeronautics and Space Administration) grant supported their research. Their citations show that the Federal Aviation Administration (FAA) and National Aeronautics and Space

Administration (NASA) have teamed up to form an Unmanned Aircraft System Traffic Management (UTM) to enable beyond visual line-of-site airspace operations for UAVs.

Their research calls for action to detect and identify "non-compliant" UAVs (Ezuma et al., 2019). The researchers criticized the use of infrared (I.R.) and video-based detection due to line-of-sight limitations. They explained how modern RF fingerprinting examines the waveform signal by its time and domain, which they claimed is not remarkably effective. They proposed that by translating the time-domain of a signal into its energy-time-frequency domain, they can compute its energy trajectory. They classified the signal into discriminating features and ran ten Monte Carlo simulations against the data to produce a result (Ezuma et al., 2019).

Ezuma et al. hypothesize their classification system based upon a naïve Bayes approach provides resiliency against noise and may distinguish between different modulation techniques. The scientists use a pragmatic worldview to figure out if their method performs better than current techniques of classifying RF signals transmitted between the UAV and its controller. They annotate that their study was completed in a laboratory and note that their experiment should be attempted outdoors where a higher signal-to-noise ratio (SNR) will be present (Ezuma et al., 2019). In their experiment, the range was a limiting factor in their investigation, and only line-of-site communication was examined (Ezuma et al., 2019).

2. Radio Detection and Ranging

Since its early discovery in the early 20th century, there have been many advances to radar systems. According to an MIT article written by Fenn et al. (2000) called "The Development of Phased-Array Radar Technology," phased array radars came into existence in the 1950s when researchers discovered that rapidly phasing individual antennas provided more flexibility than mechanical steering. Their article explains the history of phased-array radars and the many advancements since 1950 leading up to active electronically scanned arrays (AESA). Researchers Konstantinos et al. (2020), writing for Aircraft Engineering Aerospace Technology, wrote in their article "AESA Radar and IRST Against Low Observable Threats," discuss how AESA and infrared sensing technology

(IRST) will provide better quality targets when working together (Gaitanakis et al., 2020). In this article, they discuss the capability gap of modern IRST with the retirement of the F-14D Super Tomcat and the commissioning of the F-35 (Gaitanakis et al., 2020). IRST affords a pilot the advantage of detecting an enemy fighter without radar. IRST provides a significant advantage as radar gives away the pilot's position; however, a pilot cannot use IRST alone in gaining a weapons-engageable target. They conclude that data fusion from onboard data sensors and datalinks allows a pilot to create better situational awareness in complex situations (Gaitanakis et al., 2020). Their research used case studies demonstrating how advances in AESA and IRST interoperability will benefit modern-day fighter pilots. Fusion and interoperability of data will be critical in the defense against UAVs. Furthermore, data and interoperability between various systems will be essential in tomorrow's fight.

In 2018 Samiur Rahman and Duncan Robertson (2018) wrote in Scientific Reports the problem of detecting low, slow, and small (LSS) targets. They found that radar uses radio frequency (RF), also known as sound, to detect the radar cross-section (RCS) of an object (Rahman & Robertson, 2018). How does a radar detect a UAV versus a bird when both practically have the same RCS and surface area? By using micro-doppler and distinctive signatures produced by the rotation of rotors versus wingbeats, researchers have been able to distinguish a UAV versus a bird (Rahman & Robinson, 2018). This unique distinction of wingbeats versus rotors makes way for the possibility for computer programmers to code distinct comparisons for machines to analyze.

Another way to detect UAVs is to use multiple input multiple output (MIMO) energy.

3. Multiple Input Multiple Output

In 2013 at an IEEE (Institute for Electrical and Electronics Engineers) conference in Pacific Grove, CA Klare et al. (2013) discussed a radar using MIMO (Multiple Input Multiple Output) technologies to potentially warn search and rescue teams about sliding debris and collapsing ruins. They called this radar the MIRA-CLE (Klare et al., 2013). The presenters go on to explain how the MIRA-CLE Ka band radar uses 16 transmit and receive

antennas arranged in a constellation to form a linear array of 256 elements. Additionally, the radar operates between 36Ghz and 37Ghz at 33dBm (Klare et al., 2013). In their subsequent research in 2018, they have shown the possibility of using wideband frequencies to detect a UAV (Biallawons et al., 2018). Their conclusions have discovered that using range-velocity versus range-Doppler significantly improved the radar's detection performance (Biallawons et al., 2018). Their research is important because radars are significantly looking into micro-doppler radar as a solution to distinguish UAVs from birds.

Although radars are becoming the go-to solution for distinguishing a bird from a UAV, scientists are coming up with new UAV technology to mimic biological life. The biological robotics lab at Purdue University is creating robotic hummingbirds trained by machine learning to mimic the movements of a hummingbird's wings. This future technology will allow UAVs to fly in areas where conventional aerodynamics does not work (Wiles, 2019). This research is important because these sensors will continue to have to discern the differences between biological life and potential UAVs.

C. SITUATIONAL AWARENESS

Situational Awareness (S.A.) at the individual level has been defined as "the perception of the elements in the environment, within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future" (Endsley, 1988, pp. 792). When considering team S.A., a team has been defined as "a set of two or more individuals who must interact cooperatively and adaptively in pursuit of shared, valued objectives" (Salas et al., 1993, pp.82). They also stipulate that teams "have clearly defined, differentiated roles and responsibilities, hold task-relevant knowledge, and are interdependent" (Salas et al., 1993, pp.82). When combining these two definitions, one sees the importance of an integrated common operating picture (COP). The Android Tactical Awareness Kit (ATAK) is a military software platform that brings both individual and team situational awareness capabilities to a single device.

1. Android Tactical Awareness Kit

Developed in 2010 by the Air Force Research Laboratory (O'Brien, 2019), ATAK is a situational awareness application that uses a graphical user interface (GUI) to allow users the ability to communicate, orient one another to their surroundings, share information, and a host of other functions through plugins (such as coordinating medevac, weather information, and various other capabilities that can be captured through separate sensors). The primary view of the application is a map overlay that utilizes National Geospatial-Intelligence Agency (NGA) data (ATAK, n.d.). However, other map overlays may be downloaded and used, such as several styles of google maps (terrain, street, or satellite). It allows for Global Positioning System (GPS) information to be displayed for other user locations, setting bearings and way points, and the ability to orientate oneself using terrain and other markers on the map. ATAK's technological architecture has an overlay manager, allowing for the import and display of keyhole markup language (KML), keyhole markup language zipped (KMZ), and various other extensible markup languages (XML) notations, to include COT discussed earlier. The ATAK product is now being maintained by the TAK Product Center within the Army's Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) Center (Seefers, 2020). ATAK has become a very well-established product line in the DOD, utilized extensively by the Air Force, Army, and Special Operations Forces communities, and has been integrated into 15 DOD programs of record (Seefers, 2020).

2. Civilian–Android Team Awareness Kit

Though initially designed for a military operator, ATAK's platform and capabilities allow for innovation in the private and public sectors. To this end, a non-military version was developed for federal and government agencies. ATAK moved away from a "tactical assault" kit, which is a militarily specific objective; the name changed to a "team awareness" kit. This subtle name change points to the emphasis on situational awareness and collaborative features. This civilian version of ATAK is built upon the same core architecture of the military version but has some differences. Specific plugins such as tools for targeting solutions, firing solutions, and other military-specific utilities are just a few

of these differences. There are now various versions of civilian ATAK available to allow for numerous situations. (See Table 2) for a list of ATAK platforms and a brief description of each.

Table 2. Description of ATAK Clients. Source: Department of Homeland Security Science & Technology Division (DHS S&T) (2019).

Platform	Description
Civilian Android Team Awareness Kit ATAK-CIV	For use by first responders to include police, fire fighters, etc.
Government Android Team Awareness Kit ATAK-GOV	An International Traffic in Arms Regulations (ITAR) restricted version for use by United States Government and Foreign Government agencies.
Windows Team Awareness Kit WinTAK	For use on a Windows operating system. This allows the user not to be restricted to the display of a phone or tablet but to have a full desktop version. They are typically used for operations and command centers.
iOS Team Awareness Kit iTAK	Currently under development. It is reported to be released after successful beta testing and will be able to use the most common functionality as the other versions. There is a version referred to as iTAK on the Apple Store, but it is an entirely different platform after downloading and exploring the interface. It does not have the same interoperability as the android and military versions of ATAK.
Web Team Awareness Kit WebTAK	A web-based version of ATAK allows access to the situational awareness capability without installing the client onto their device.

3. Tactical Awareness Kit Server

The ATAK platform allows for interoperability between all the different versions simultaneously. An ATAK network cluster is initiated once two separate ATAK clients are on the same network (even a local Wi-Fi hotspot), regardless of the version. Access to the internet is unnecessary if the capability required can be utilized between the local area network (LAN). However, if the connection between clients is outside of the LAN, then the internet will need to be accessed. To connect multiple clients, a TAK Server would be used. The TAK server can interface with one or more TAK clients, regardless of client type, see Figure 8. Like a typical server, the TAK Server stores, receives, and sends data.

The TAK Server becomes critical to our research and later experimentation when sending COT data from the G1X to multiple end-user devices.

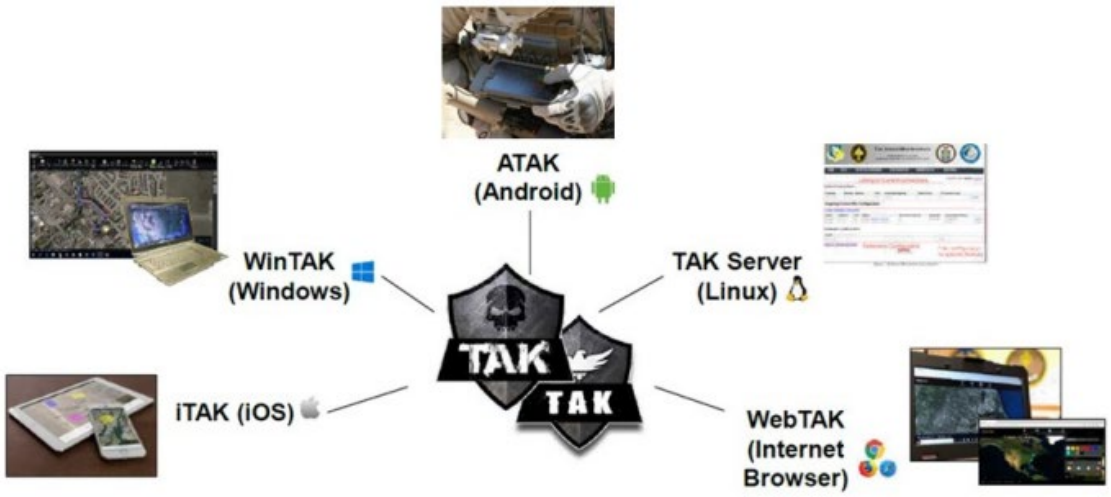


Figure 8. Various TAK Platforms. Source: DHS S&T (2019).

D. DECISION-MAKING

There are three typical ways that a person could categorize the decision-making process: procedural, analytical, and naturalistic. A procedural approach to decision-making is when an individual or organization has predetermined standard operating procedures based on various situations that the user may find themselves in. This is very common in the DOD and is how many of the decisions are made. Having a keen understanding of the procedures will allow rapid decision-making, as long as the user is aware that the situation they are perceiving is aligned to the procedure that needs to be followed. An analytical approach is also a very common decision-making strategy and can be summarized as when one compares a primary option to one or more alternative options. There is usually a comparison of the pros and cons of each option, and the "best decision" is based on the factors that are considered most likely to achieve the desired goal. This type of decision-making is heavily based on evidence that is available. Finally, naturalistic decision-making is when one takes account of the environment they are in and, based on their own

understanding of that environment, make a decision. This type of approach is heavily based on the user's experience, so they may have the cognitive ability to discern the information that they have available. We will look further into three naturalistic decision-making models further and discuss their strengths and weaknesses as it pertains to our research question. We will then discuss how implementing a sense-making framework will greatly assist in the decision-making process.

1. Endsley Model (1995)

Mica Endsley sought to better understand situational awareness by looking at pilots and the aviation industry, claiming that situational awareness has been a crucial commodity for military aircraft since World War I (1995). Endsley's research developed a model that framed situational awareness into three levels: perception, comprehension, and projection. Perception is categorized in how we obtain information. This can be done through sight or sound, or it could be obtained in some other way. Ideally, it is the critical information that we are perceiving and obtaining. After one has obtained the information that they feel is necessary, they need to put it together to try and get meaning or sense out of it. This will answer the "so what" question we are trying to obtain. It can be compared to reading comprehension; not only is it important to understand what all the words on the page say, but it is just as important to understanding the meaning or intent of the story. The final level of situational awareness in the Endsley model is projection or looking into the future and projecting what may happen next or over a period of time. For this projection to take place, however, one must have experience and expertise in the area in order to frame a cognitive or mental model of choices. Endsley likens this to a schema or pattern matching recognition that allows for rapid mental simulation in order to quickly come to the "best" decision available, see Figure 9.

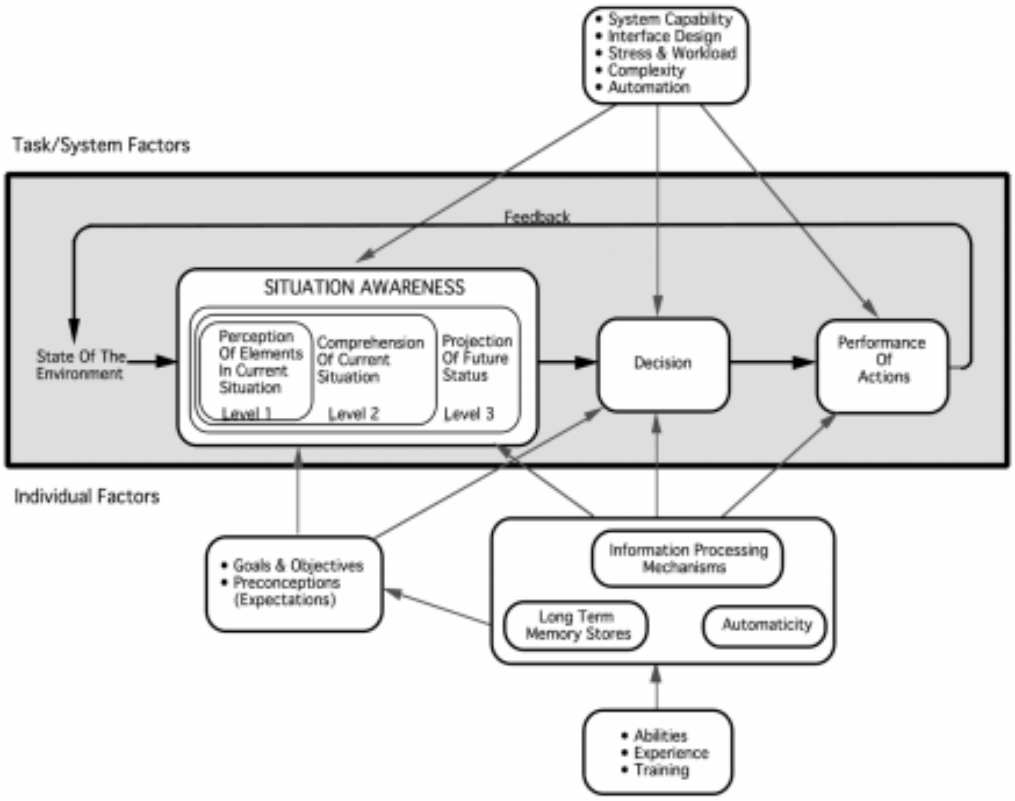


Figure 9. Endsley Situational Awareness Model. Source: Endsley (1995).

Some have argued that Endsley's model required the three levels of situational awareness to be approached in a linear fashion (Sorensen et al., 2010) and (Salmon et al., 2012). However, Endsley herself argues that it should not be considered as linear stages but instead be viewed as "*ascending levels* of SA" (Endsley, 2015). She argues that taking a ridged linear methodology may lead to a focused goal-oriented or data-driven perception that may result in important information being missed or neglected, which may lead to errors or an utterly incorrect conclusion. Instead, there needs to be the ability to allow the situation awareness to switch between the goal(s) and data and take an iterative approach between each level (Endsley, 2015). While in Level Three, projection, it may be determined that some data element is missing, which allows the focus to go back to Level One to find that information needed. This will be important to remember when considering the current uncertainty of the UAV threats that we in the DOD currently face.

2. Recognition-Primed Decision-Making

Recognition-Primed Decision-Making (RPDM) was coined by Gary Klein in his work with firefighters in the early 80s (Klein, 1998). Klein discovered a new way of looking at the decision-making process almost by accident. Up to this point in his career, the two-option hypothesis (Soelberg, 1966) was the definitive work of how decisions were made. Much like the analytical approach to decision-making mentioned earlier, the Recognition-Primed Decision-Making model claims that when faced with making a decision, one would compare option A to option B. Klein was intrigued to find out how individuals were able to make such rapid analytical decisions in crisis situations. He then observed, interviewed, and researched numerous fire stations before, during, and after events that took place during that time of the study, as well as collected stories that the participants were able to recollect based on series of questions that were developed ahead of time. What came from this study was that Klein found that the experienced firefighters, such as commanders and chiefs, did not "decide" anything. There was no comparison that was happening according to their account. Instead, he found that a fusion of two processes occurred: the way a decision-maker sized up the situation and the evaluation of the course of action to take (Klein, 1998), see Figure 10.

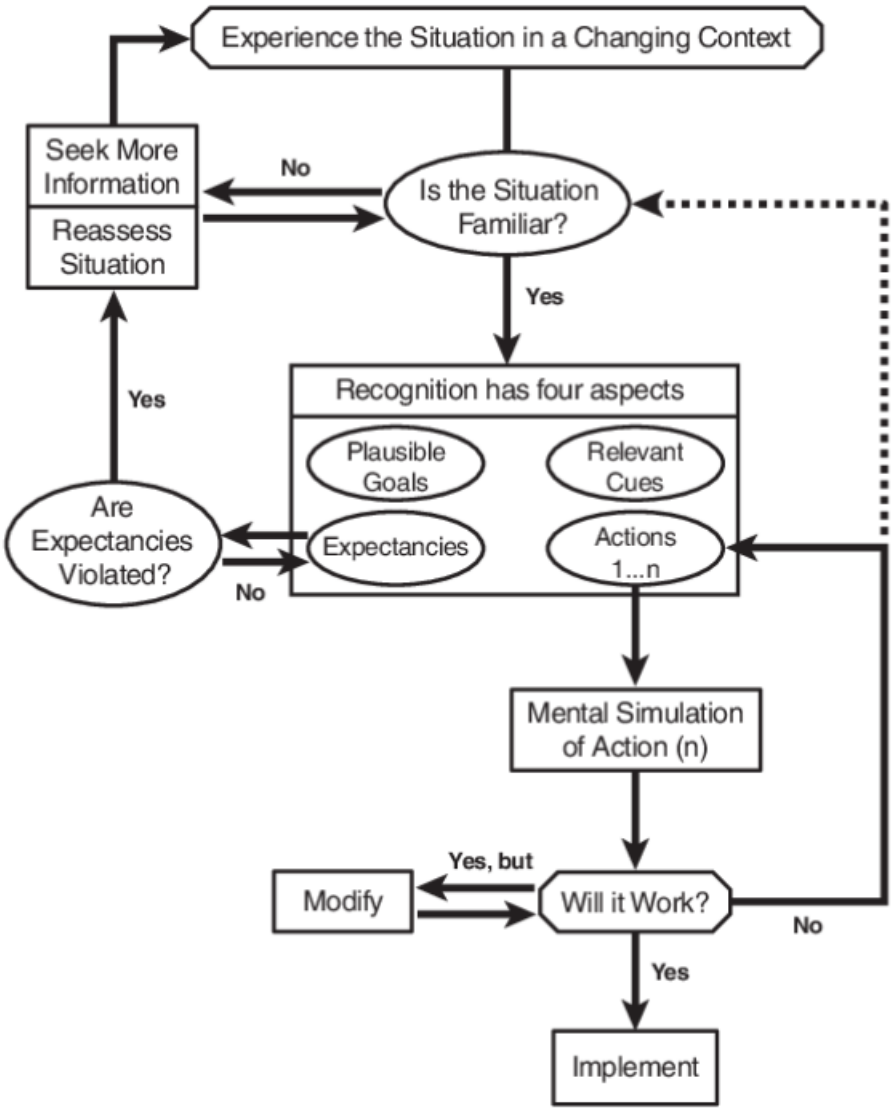


Figure 10. Recognition-Primed Decision Model. Source: Klein (1998).

Klein found that the fire commander would be able to rapidly assess the situation and determine if it were familiar to them or not. If it was, then they would then undergo a recognition process to review their goals, any relevant cues, what they should be expecting to see based on their understanding, and finally develop an action of what to do in this scenario (Klein, 1998). This is where the decision-maker is implementing cognitive sense-making based on their experiences and understanding of the information that they have available to them. Upon selection of the action that they feel is best, the decision maker

would then go through a process of mentally simulating doing that action and continue through that simulation to perceive what the result would be. If the result matched the desired outcome they wanted to achieve, they would implement that action. If it did not, then they would go back to their sense-making and either choose a new action or readdress their expectancies of the event. This could seem like a long process, but according to Klein, it can happen in a matter of seconds to an experienced decision-maker. The greatest weakness in Klein's model is that it requires experience for it to be effective. If the event that the decision-maker is facing is new to them, there will be little data they can pull from during their sense-making. They will not be sure of what to expect, what cues they should be paying attention to, or what actions should be mentally simulated. In the current situation of facing an unknown UAV threat, this model creates potential challenges for any operator in this environment.

3. Observe Orient Decide Act Loop:

The ability to counter a UAV first relies on detecting or observing UAVs. In 1976, U.S. Air Force Colonel John Boyd, known for his dogfighting ability in the Korean War, created a popular decision-making framework still in use today (Boyd, 2007). He based it upon his experience as an F-86 fighter pilot and missions he flew during the Korean War. In his brief "Patterns of Conflict," Boyd discusses how fighter pilots must operate faster than their enemies. To do this, he hypothesized a decision-making framework based on what he saw as an adversary's observation-orientation-decision-action (OODA) Loop (Boyd, 2007).

In the first step of the OODA Loop model, an observer gathers imperfect data and feeds that data into the next step, orientation. When a person is orienting themselves, they take that data and make it into knowledge to feed into a decision. From this decision or hypothesis, the observer may get some feedback to refine their decisions further. They then feed that knowledge into an action that receives a direct response to the interacting environment. Although Colonel Boyd's simple OODA Loop model had profound implications for military strategy, information flows are poorly defined. More specifically, the way people gather, process, and use information differs within every individual

responsible for making decisions. It was not until two years prior to Boyd's death that he developed a graphical representation of his model, see Figure 11. Boyd added feedback loops that were intrinsically there but not explained in his original model (Brown, 2018).

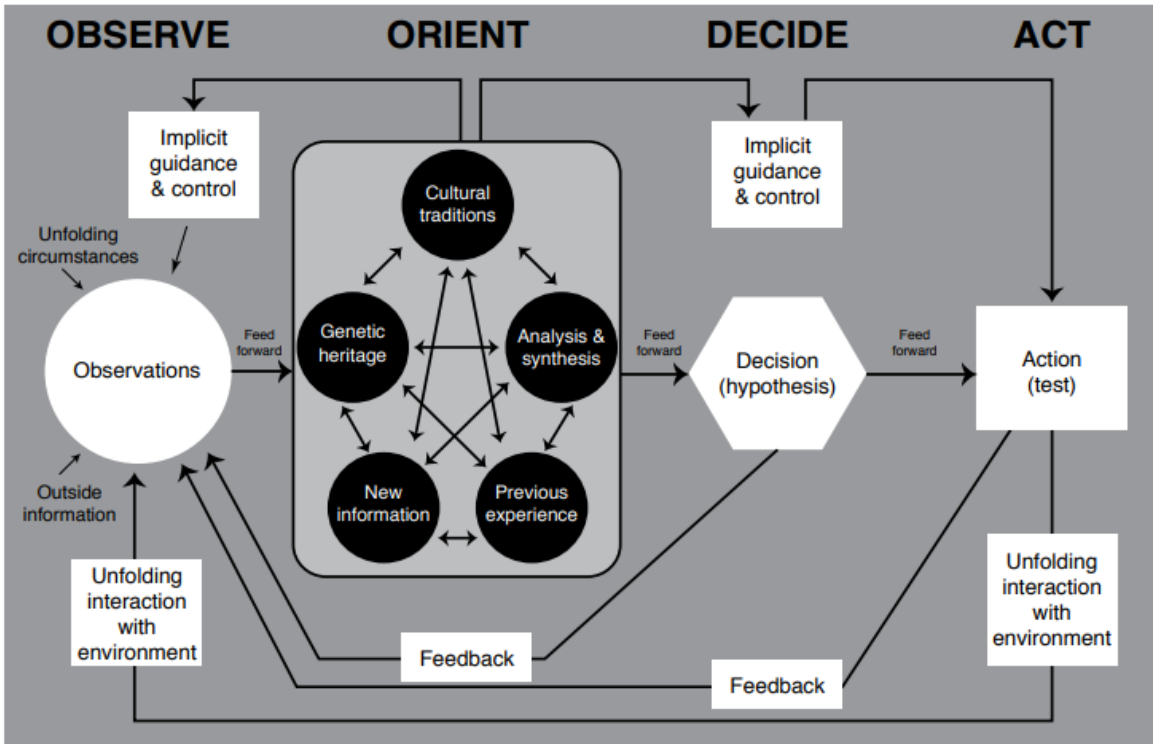


Figure 11. Modified OODA Loop Diagram. Source: Brown (2018).

Boyd's model has many similarities to Endsley's and Klein's models and though there may be different terminology used, using OODA as each stage of the process relates nicely to the other models. See Table 3 for a comparison of Boyd's OODA Loop, Endley's Model, and RPDM as it relates to UAV detection, identification, and execution.

Table 3. Comparison of OODA Loop, Endsley 1995, and RPDM

UAV	Detection	Identification		Execution
OODA Loop	Observe	Orient	Decide	Act
Endsley 1995	Perceive	Comprehend	Project	Perform Action
RPDM	Situation Familiarity	Pattern Recognition	Mental Simulation	Implement

For these reasons, we will be predominantly using Boyd's OODA Loop model's terminology in this thesis, but we will adapt some other terminology that better relates to other models. For instance, though Boyd's model does not explicitly mention sense-making, this step happens during the orientation phase. Sense-making is a critical step that needs further discussion. The Cynefin (pronounced Ken-Evan) Framework, developed by Dave Snowden (2002), can help a decision-maker ensure that they are making sense of the data they are using to formulate a decision action.

4. Cynefin Framework

The Cynefin Framework is a sense-making tool to assist with pattern recognition (Snowden, 2005). The name is Welsh in origin and means habitat or place, but Snowden likens it to mean more specifically a place of multiple belongings. It is important to make a distinction between sensemaking and categorization as it pertains to the Cynefin Framework (Snowden, 2005). Snowden (2005) explains that categorization requires a framework first, and the data then is put into the respective categories that are already predetermined. This methodology is suitable for rapid decisions and is commonly used in research when determining quantitative, cause and effect models. Sense-making, on the other hand, allows the data to drive the narrative. This allows for exploration of the data and enables the decision-maker to possibly see connections or data points that may have been missed in the categorization model. The framework takes the three basic systems (order, complex, and chaotic) and derives five separate domains: From the ordered system: complicated and simple, complex, chaotic, and disorder, see Figure 12 (Snowden, 2005).

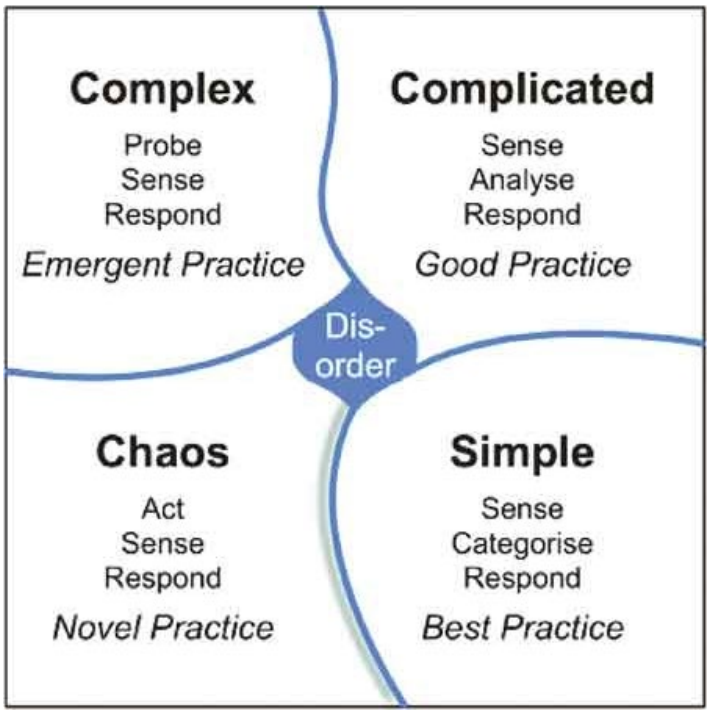


Figure 12. Cynefin Framework. Source: Ang (2020).

Each domain is comprised of its basic system, the relationship between cause and effect, defining characteristic, decision model to use, and the ideal practice to be implemented while in the respective domain, see Table 4. Understanding the domain one is operating in is essential to understanding how best to relate to the data interpreted. Snowden (2005) also emphasizes a point in his model that is sometimes missed or overlooked. According to Snowden (2005), the line between simple and chaotic is different than every other separation in the framework (2005). Instead of a smooth line, what separates the simple and chaotic domain should instead be viewed as a cliff face. If one continued to operate in a simple domain pattern and is handled as a best practice, the situation will eventually drift closer to the chaotic domain until it drops off into a crisis. What was once considered known and repeatable has now become unknown, with little understanding of the variables that are affecting the outcomes. Snowden (2005) suggests that most should operate between the complex and complicated domains (which have areas of transition and better allow for change) and leave only a few very predictable things to operate in the simple domain.

Table 4. Cynefin Domain Characteristics

	Basic System	Relationship with Cause and Effect	Defining Characteristic	Decision Model	Type of Practice	How it relates to disorder
Simple	Ordered	Exists and self-evident	Results are predictable and repeatable	Sense Categorize Respond	Best Practice	Looks for processes to change
Complicated	Ordered	Exists but not self-evident	Requires expertise	Sense Analyze Respond	Good Practice	Looks for more data or time to analyze
Complex	Unordered	Known through hindsight	Unpredictable, emergent outcomes arise	Probe Sense Respond	Emergent Practice	Looks to numerous ideas or points of view
Chaotic	Unordered	None known	Move quickly to see if situation becomes stable	Act Sense Respond	Novel Practice	Looks for any idea to act on

Using the Cynefin Framework in the sensemaking process of naturalistic decision-making will allow the decision-maker to have a better understanding of how they can interpret their data and will guide a more effective decision-making model. For instance, in the case of a Commander being notified of the detection of a potentially hostile UAV, the Commander could quickly assess that there may be no Standard Operating Procedure to guide his/her decision. Using the Cynefin Framework, it then becomes evident that they are not operating in the simple domain. There are some known factors that they can derive from the situation, so they are also not in the chaotic domain. Instead, they could determine if they are operating in the complicated or complex domain, which could be determined by the level of expertise available and if there are any "good practices" known. This then allows the Commander the decision model of Sensing/Analyzing/Responding or Probing/ Sensing/Responding. The commander can run mental simulations through their head quickly and determine if the desired outcome is likely obtainable. They then can make the call to their team to execute their order.

5. Interoperability Framework

When consolidation of capabilities involving multiple technical systems and group entities are considered, it is important to appreciate categories of interoperability types within an enterprise or in multi-organizational endeavors. Isolating technical and non-technical interoperability issues allows leadership and integrators at all levels to allocate specialized assets for each type. Technical interoperability factors in the San Francisco exercise and radar/SA tool integration may include data exchange, internetwork, hardware, infrastructure, applications, and cybersecurity assets (Rohatgi & Friedman, 2010). Non-technical interoperability factors may include integrators, training, and change management entities. The latter example deals with social, operational, programmatic, and cultural aspects of interoperability (Rohatgi & Friedman, 2010). The Interoperability Framework holistically addresses socio-technical systems systematically through logical and consistent means while addressing technical and nontechnical interoperability types through understanding systems from the top-down, ultimately architecting integrated solutions (Rohatgi & Friedman, 2010).

E. SUMMARY

Using a naturalistic decision-making methodology, one must be able to have a clear situational awareness picture. ATAK is a situational awareness tool that allows a unit of any size to develop a more accurate common operating picture. Situational awareness first requires the user to perceive the data that is in front of them and then make sense of that data. Integrating sensor data from technological devices, such as radar and RF, into ATAK brings a fuller picture for sense-making. Once the operator understands their situation, they then would use some form of mental simulation to envision the best action to be taken given the current situation. Accepting the simulated outcome that they were hoping to achieve, they would then act on that course of action.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. EXPERIMENT DESIGN

To obtain meaningful data to assist us in our research question, we collaborated with the San Francisco Preventative Radiation and Nuclear Detection (PRND) community to develop an exercise that would utilize live testing of situational awareness tools being used in a controlled environment under threat. Naval Postgraduate School has been partnering with the SF PRND community, integrating technology to assist in maritime interdiction operations research series of experimentation since 2006. It started locally in Monterey and the San Francisco Bay Area but then extended to the East Coast and overseas to locations such as Greece, Germany, and Sweden. Utilizing the expertise of SAAB, the 95th CST, and the partnerships between NPS and the United States Coast Guard-Sector San Francisco Maritime PRND team, we were able to design, resource, and field several experiments to pursue our research question: **How does the integration of the Giraffe 1X radar and Android Tactical Assault Kit contribute to the DOD and DHS security forces' enhanced decision-making capability within a naval port?**

A. EXPERIMENT FRAMEWORK

The experiment was divided into four phases: equipment familiarization and benchmarking; communications exercise (COMEX); San Francisco Bay demonstration; and network extension (WMN) using persistent systems multiple-input multiple-output (MIMO) man-portable unit (MPU) generation five radios. Phases I and II were required to ensure the integration of technology was feasible, tested, and validated. Phase III would occur in San Francisco Bay during Operation S.F. Bay Guardian 2021. Finally, in Monterey, Phase IV would occur using the NPS Campus and remote site not covered by ATAK network cluster – the Fisherman's Warf in this particular case. Phases II and III were required to be divided into iterative and incremental subphases to ensure all objectives were met. Table five lists the experiment phases and subphases. Further explanation of each phase follows.

The chapter presents each objective of Phases I and II, describing what we did and observed. This chapter also presents our observations of Phase I and II in this chapter and

not in our results because they were only relevant to the further phases. Lastly, our chapter covers what we did for each objective in Phases III and IV, but the observation and results are in Chapter V. See Table 5 for a list of each major phase and subphase.

Table 5. Experiment Phases

Phase 1 – Equipment Familiarization and Benchmarking
Phase 2 – Communications Experiment
Subphase A: NPS SA Server Setup and Configuration
Subphase B: 95th CST ATAK Server Integration
Phase 3 – San Francisco Bay Guardian Exercise
Subphase A: Watch Stander's detection without the use of technology
Subphase B: Watch Stander's detection with the use of technology
Phase 4 – Network Extension Through WMN Using MPU5s Experiment

B. DESIGN CONSIDERATIONS

The San Francisco Bay Guardian 2021 exercise served as our concept of operations for our experimentation. While Bay Guardian 21 brought together multiple federal, state, and local maritime first responders to demonstrate the threat of low, slow, and small UAVs in littoral waters, our experiment drives more into the requirements of placing a live radar system into a wireless mesh network. This will establish a baseline performance that other researchers can build from.

To isolate our variables related to our research question—how does a G1X radar affect a wireless mesh network—we utilized a cyber-physical approach, forwarding simulated radar feeds from Sweden to the United States. After the completion of Phase III, we discovered new challenges in maintaining connectivity in the Bay, which led us to require a Phase IV, extending the wireless mesh network connection via MPU-5s. We measured the network performance by utilizing an MPU-5 radio network management tool.

C. PHASE I – EQUIPMENT FAMILIARIZATION AND BENCHMARKING

The purpose of the first phase was to familiarize ourselves with the software, equipment and establish the benchmark capabilities of capturing G1X data and extending it via ATAK to a remote end-user. Critical to this phase was getting a firm understanding

of each technology before it would be integrated. This phase involved loading different versions of ATAK onto several devices, including various cell phones, tablets, and laptops. Currently, the civilian version of ATAK is only available on Android devices. The military version of ATAK is available from the DI2E Research and Development website or at the NGA App Store (CIVTAK, 2017). Once we understood the functionality of the ATAK software, we then needed to learn more about the G1X radar. We then worked with SAAB to integrate the G1X radar into a wireless mesh network. See Table 6 for Phase I objectives.

Table 6. Phase 1 Objectives

Phase 1 – Equipment Familiarization and Benchmarking
Objective 1: ATAK Familiarization and Benchmarking
Objective 2: Establish Connection Between G1X and CENETIX SA Server
Objective 3: Establish Secure Socket Layer (SSL) Connection to TAK Server

1. ATAK Familiarization and Benchmarking

Familiarization with ATAK was critical as, up to this point, our understanding of the application came through our documentation reading. Through our familiarization, we also were able to get our baseline benchmarking checks completed. The civilian and windows ATAK versions were both available via the Google Play Store; however, the military ATAK is only available for U.S. Military members. After loading and unloading the various ATAK versions on numerous devices, learning how to upload different map interfaces, see Figure 13, navigating the menu, tracking capabilities, setting up a geofence, chatting, and establishing a connection to the NPS TAK server developed by CENETIX Researcher, Eugene Bourakov, we were ready to start testing the capabilities and pre-established integration between ATAK platforms.

Figure 13. ATAK Downloaded Map Overlay Options

At the beginning of this project, we were introduced to the ATAK software. We were informed that it was like a blue force tracker that provides situational awareness and, more importantly, communication functionality. We partnered with the 95th Civil Support Team during a monthly training exercise at Vallecitos Nuclear Center just 30 miles east of San Francisco to allow us an opportunity to see ATAK used in a live environment. The 95th CST has been using ATAK as a situational awareness tool in their operations since 2016, and they have become recognized experts in the National Guard.

Major Alexander Efros, a Nuclear Medical Science Officer and our initial Point of Contact for the 95th CST, invited us to a field experiment with the team in November. While at the Vallecitos Nuclear Center, we gained hands-on experience using ATAK, and they demonstrated its integration with the National Guard's Mobile Field Kit (MFK). We witnessed the team using ATAK primarily for its chat features. However, the team highlighted its capability of communications, photo sharing, and situational awareness through geospatial positioning and tracking other ATAK users. ATAK provided the team

with a common operating picture and flexibility of communications; however, it lacked many PRND functions. The team made up for the lack of APIs by integrating ATAK into a second situational awareness application. This hands-on tacit knowledge was necessary to implement ATAK as a situational awareness tool for S.F. Bay Guardian 2021.

2. Establish a Connection Between G1X and CENETIX SA Server

Data captured by the G1X will be converted to Cursor on Target (COT) message and pushed forward to the CENETIX SA Server for processing. Processing means that by receiving this COT message, the NPS SA Server stores it into a database. A message router was used to read the latest message stored in the database and push the information forward to the TAK server. The TAK server then broadcasts the COT messages out to all end-connected ATAK devices.

3. Establish Secure Sockets Layer Connection to TAK Server

The message wrapper sends a secure session request to the TAK server. The TAK server then replies to the message wrapper with an X.509 certificate containing the TAK server's public key. The message wrapper then confirms the certificate using a certificate authority (CA). The message wrapper then generates a random symmetric key and encrypts it using the TAK server's public key. The message wrapper sends the encrypted keys back to the TAK server. Now both the message wrapper and the TAK server know the symmetric keys and securely transmit information.

D. PHASE II – COMMUNICATIONS EXPERIMENT

The purpose of Phase II was to establish and configure TAK servers that will be used in Phase III. At the end of the communications exercise, the objective is to have SAAB's G1X radar push simulated data onto the NPS SA server and push to the 95th Civil Support Team (CST) TAK servers via SA message router. By the end of this phase, an end-user may view UAV feeds directly on their ATAK devices and chat between all agencies participating in the demonstration. See Table 7 for a list of the objectives by subphase.

Table 7. Phase 2 Objectives

Phase 2 – Communications Experiment
Subphase A: NPS SA Server Setup and Configuration
Objective 1: Configuration of ATAK devices to communicate with the server
Objective 2: Test Compatibility of Simulated Data to both military and civilian ATAK Devices
Subphase B: 95th CST TAK Server Integration
Objective 1: Integration between NPS SA Server and 95th CST TAK Server
Objective 2: Successful Implementation of ATAK Message Router
Objective 3: Successful test of simulated data to 95th CST TAK Server

1. Subphase A: NPS SA Server Setup and Configuration

Messages sent from the G1X in Sweden were captured and stored in a database on the NPS SA server. Another program running on the NPS TAK server captures the traffic and forwards it to the CST TAK server. The NPS SA server is responsible for receiving data and processing it.

a. Configuration of ATAK Devices to Communicate with the Server

To configure the ATAK device to communicate with the TAK server, we first needed to download a file generated from a utility installed on the TAK server and zipped for deployment. We then navigated to the import manager using the menu functions on the ATAK device to load the configuration file. The import manager allows one to get the configuration file and install it on their drive. The file compiles its IP address, SSL port number, and two trust certificates, one for the client and one for the server.

b. Test Capability of Simulated Data to Both Military and Civilian ATAK Devices.

As discussed early in the background, the core functionality between different versions of ATAK (civilian, military, windows, etc.) is the same. For this reason, we expect that each version will fully cooperate with one another based on our research needs. The primary difference in versions is that military ATAK provides extra plugins and

encryption. Other limitations were identified during our experimentation and will be discussed in Chapter V.

2. Subphase B: 95th CST TAK Server Integration

To initiate a connection between our devices and the 95th's TAK server, we received a .zip file generated by their TAK server and followed the steps outlined in Subphase A's Objective One.

a. Integration Between NPS SA Server and 95th CST TAK Server

COT messages are sent directly from the G1X to the SA server. This data must then be wrapped using the SSL protocol to be sent securely to the 95th's TAK server. We accomplished this task by sending COT messages from the G1X and storing the messages in a database on the SA server for asynchronous reading by the message router located on the SA server. Every second, the message router checks for a new COT message captured by the SA server. If one is received, the simulated data would then be encapsulated by an SSL wrapper and forwarded to the IP address and port address number of the 95th CST TAK server. The SSL wrapper is another "in-house" software created using the SOCAT Windows utility specifically for our experimentation. From there, users on the 95th CST ATAK server can see the forwarded activity. We scheduled a planning meeting between all agencies regarding sending live radar data from Sweden into the 95th CST ATAK server to facilitate integrated communications.

b. Successful Implementation of ATAK Message Router

This objective proved more difficult than expected. First, the 95th CST TAK servers are operational and contain other active National Guard Units not participating in this exercise. We federated NPS's TAK server, devices, and AT&T's Fir19stNet devices onto their server, but first, we had to get permission from higher authorities. The current setup of the NPS SA Server was not set up to use SSL certificates, and that level of security is mandatory to access their servers. For the message router to work successfully, it would have to have three components: The IP address and SSL port number of the 95th TAK

Server and a trust and client certificate. That information would then be pushed with the COT data via a secure layer. With the conjunction of an SSL, a wrapper was developed to go along with the XML data to pass along to CST servers. Figure 14 shows how we were able to set up our communications circuit for the demonstration. Simulated G1X data was passed to the NPS SA server. That data was then passed to the ATAK message router and TLS wrapper. The packet was then routed to the 95th CST TAK server and distributed to all the ATAK devices participating in the exercise.

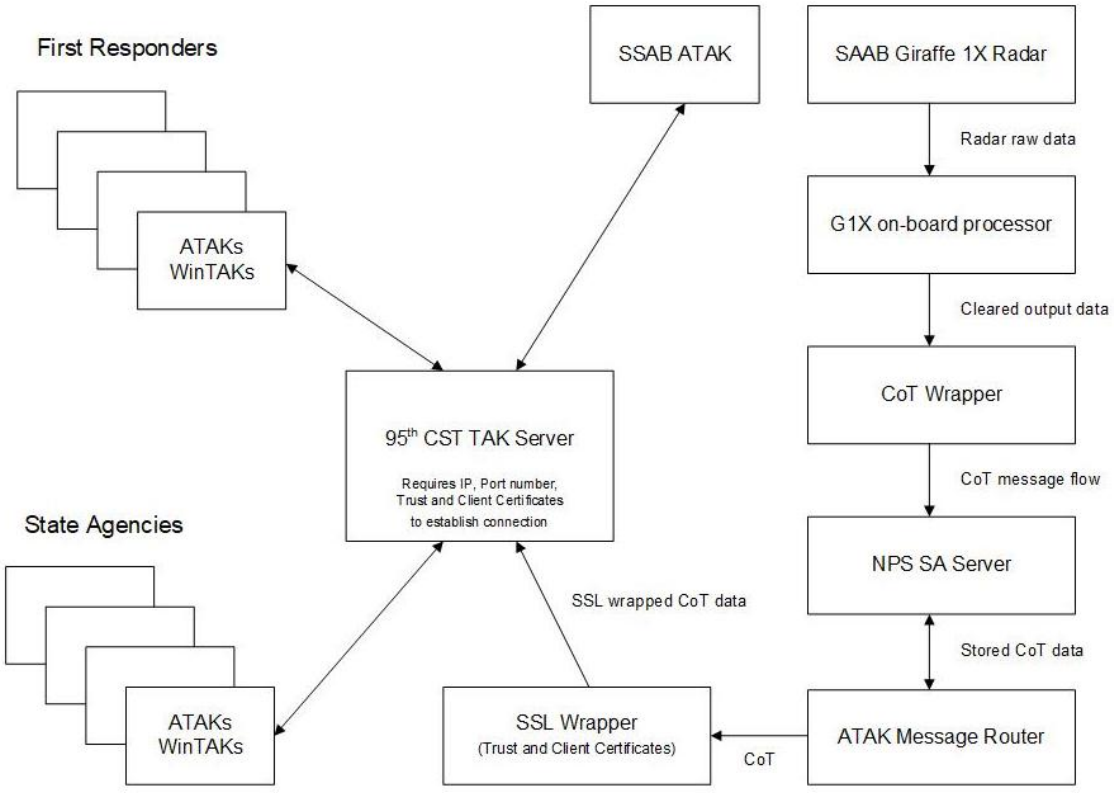


Figure 14. Network Diagram of Subphase B Server Integration

c. Successful Test of Simulated Data to 95th CST TAK Server

This objective would successfully be indicated by having our simulated G1X data appear on other ATAK devices that the exercise participants would be using. In preparation for the San Francisco Bay Guardian exercise, the 95th CST acquired 15 cell phones to be

loaded with the civilian version of ATAK distributed to the participating patrol boats. Figure 15 highlights the successful connection to the 95th CST TAK Server. Each great dot indicates a separate device connected to the server and was able to receive the simulated data that was passed through it.

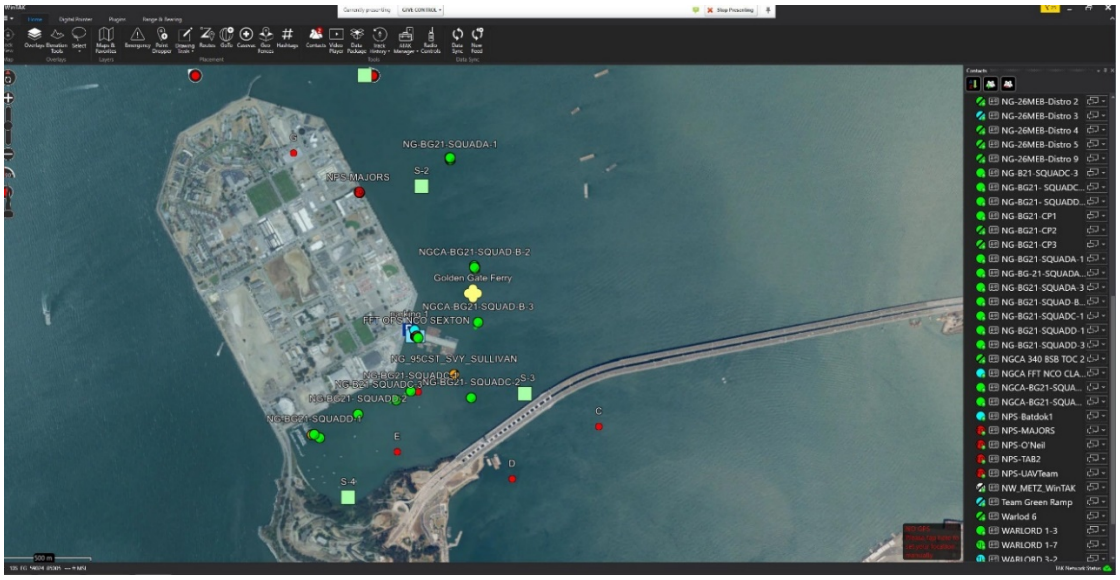


Figure 15. Successful Connection to the 95th CST TAK Server

E. PHASE III – SAN FRANCISCO BAY GUARDIAN EXERCISE

The purpose of Phase III was to examine the graphic user interface (GUI) of the ATAK and Giraffe 1X radar as a situational awareness tool while conducting operations inside of a controlled exercise. Leveraging NPS's long time partnership history with the San Francisco PRND team from prior thesis work in the San Francisco Bay Area, we were able to partner with the lead exercise planner, Fire Chief Philip White (ret), in order to support an exercise, they were in the process of planning. The primary purpose of the Bay Guardian 2021 full-scale exercise was to provide local, state, and federal maritime first responders with Preventive Radiological/Nuclear Detection (PRND) capabilities an opportunity to become familiar with and implement recent updates to the United States Coast Guard-Sector San Francisco Maritime PRND Concept of Operations Plan and PRND Standard Operation Procedures.

This exercise provided an opportunity to evaluate the ability of explosive ordnance personnel to respond to a bomb threat on a commuter ferry, something that had never been done in the past. The exercise allowed us a perfect opportunity to study how the integration of technology allows first responders at the scene of a maritime incident to detect the presence of unauthorized, unmanned aerial vehicles (UAV's) and respond to those threats. The main scenario was a reported threat of a radiological improvised explosive device (IED) on the Golden Gate Ferry. Numerous organizations participated in this scenario, see Table 8.

Table 8. Bay Guardian 2021 Exercise Participants

Participant	Role
Federal Bureau of Investigation (FBI)	The principal agency having jurisdiction for terrorism-related incidents. Also, special response for nuclear incidents with a local Stabilization Team.
United States Coast Guard (USCG), Sector San Francisco	The agency having jurisdiction for maritime security on San Francisco Bay. Two (2) teams from the region, the Sector San Francisco Security boarding team and the regional MSST (Maritime Security and Safety Team) from Coast Guard Island, Alameda.
USCG Auxiliary	Were NOT able to participate due to COVID restrictions.
Department of Energy, Radiological Assistance Program (RAP) Team-7 (Lawrence Livermore National Lab)	Radiological incident response team for California, Nevada, Hawaii, and the Pacific island territories. One of two groups who brought radiological materials (sources) for the exercise, along with radiation detection and safety experts. Additionally, from LLNL, one of the technical reach back experts from DOE Triage participated.
Transportation Security Administration (TSA) VIPR	The agency responsible for intermodal security and response who share a jurisdictional interest with the FBI, USCG-Sector San Francisco, and local law enforcement. This team brought secondary screening experts for the response after the initial (primary screening) detection.
California Office of Emergency Services	The other team who brought radiological materials. Health Physics (radiation safety experts) from California's Radiologic Health Branch.
95th Civil Support Team	The agency that performs as the state's CBRN resource in whose area of responsibility (AOR) the incident takes place. It also serves as the host for the TAK server that the experiment will run over.
Port of San Francisco	Authorized use of Pier 1 on Treasure Island
San Francisco Maritime Exchange	Partners in local maritime transportation security act and the safe ports initiative.

Golden Gate Ferry	Provided a ferry as a platform for two of the scenarios of the Bay Guardian exercise.
San Francisco Police Department	The local first responder in whose jurisdiction the event takes place and shares investigative authority with the FBI, USCG-Sector San Francisco, and the TSA VIPR teams. They brought two boats, one to ferry the FBI Stab Team and the other as a participating search vessel. Probably the most experienced LE team on the Bay.
San Francisco Fire Department	The local first responder in whose jurisdiction the scenario would take place. They provided their newest fireboat, the St. Francis, as a target vessel and their newest Mooseboat as a search vessel.
Oakland Police Department	The local first responder that would respond in response to a request for assistance from the USCG-Sector SF
Alameda County Sheriff's Office	The UAV team was operating their UAVs as a red team against the participants. In the past, they have had rad/nuke search vessels but did not participate in that role for this exercise.
Other members of the Neptune Coalition	Maritime agencies that patrol the AOR of USCG-Sector San Francisco who wished to participate. These included: Central Marin FD; Alameda PD; North Bay FD; Sonoma County Sheriff; Solano County Sheriff; Contra Costa FD; Contra Costa County Sheriff; and Fairfield PD. Also participating in their regional roles for response and coordination were: Northern California Regional Intel Center (NCRIC), FAA, and USCG Sector SF, and for event security, Sacramento County Sheriff.
Naval Postgraduate School	To provide the demonstration of utilizing technology as a situational awareness tool during a potential UAV threat

Our demonstration was split into two subphases. In Subphase A, we wanted to see how long it would take for watch standers to report possible UAV surveillance to the on-scene commander using only their visual/audible capabilities. In Subphase B, we would introduce ATAK as an additional situational awareness tool to equip first responders with the technology to communicate via chat, post photos, and detect threats with the assistance of radar sensor data. See Table 9 for a list of the objectives by subphase.

Table 9. Phase 3 Objectives

Phase 3 – San Francisco Bay Guardian Exercise
Subphase A: Watch Stander's detection without the use of technology
Objective 1: Measure the time from launch until detection.
Objective 2: Measure the distance a UAV was detected without S.A. tools.
Objective 3: Measure the response time before a decision was made.
Subphase B: Watch Stander's detection with the use of technology
Objective 1: Measure the time from when an unknown UAV appears on ATAK to notification of potential threat.
Objective 2: Measure the distance of UAV once detected using SA tools.
Objective 3: Measure the response time before a decision was made.

Subphase A was further broken down into three tests: Reconnaissance, probing, and assault. During the reconnaissance test, we flew UAVs in a clockwise circular pattern around the surface vessels to simulate a malicious actor gathering information about how the units operated during this test and identify gaps in their security that could be later exploited. The UAV team approached closer each pass for about 30 minutes or until a watch stander reported a sighting. For the probing test, we then penetrated the security zone with a UAV and flew directly to the rear of the vessel to see how long it takes for a sighting to be reported. Finally, for the assault test, we flew the UAVs directly at the patrol vessels to simulate a direct attack.

Originally, Subphase B was to be conducted using the same method as Subphase A, only to incorporate the Giraffe 1X radar and ATAK to give the users an enhanced and integrated Common Operating Picture. However, due to the COVID-19 Pandemic, we could not have a Giraffe 1X radar system on-sight and instead needed to use simulated data. However, this limitation proved to be an opportunity to test another factor in using COT feeds over extreme ranges. We re-developed Subphase B to run two separate simulated scenarios over the ATAK network.

In scenario 1, we used a laptop located in Monterey, CA (roughly 120 miles) to simulate the Giraffe 1X radar processor to transmit sensor data, via SSL, to a federated TAK Server hosted by the 95th CST. The TAK Server would then broadcast this signal to

all TAK devices (military and civilian) connected to the server (also utilizing SSL connections), see Figure 16. Scenario two was similar, with the only difference in that the simulated Giraffe 1X feed was sent by the SAAB team located in Gothenburg, Sweden (over 5,000 miles). This scenario allowed us to demonstrate the capability of sensor data feeds to be broadcast to any server connected to the internet. Both scenarios would allow the user to see a "detected" potential threat, identified as a red icon on their screen.

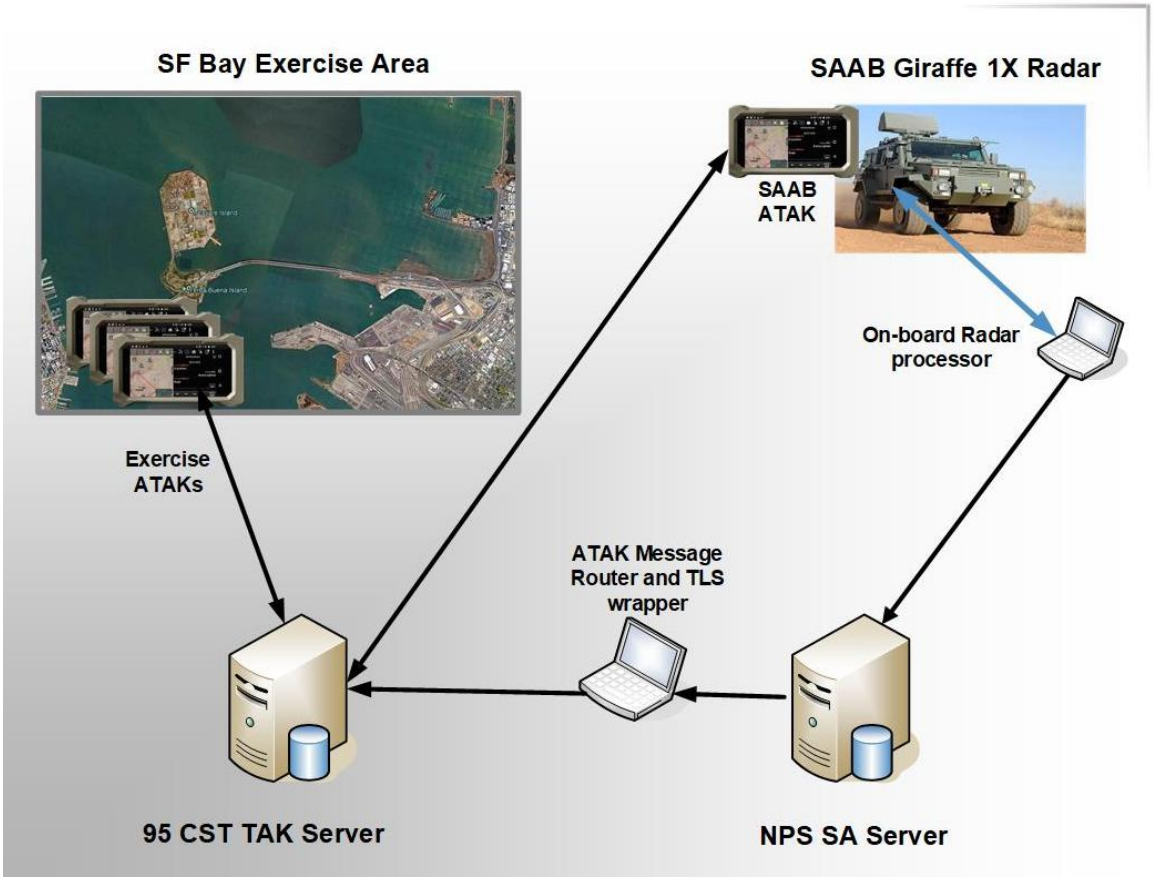


Figure 16. Overview of Phase 3 Network

To record our observations in Subphase A, we created a chart of the time the UAV lifted off when it was on station, the time a watch stander reported it over either the VHF radio or ATAK and the time a decision was made. The UAV was equipped with GPS to record the UAV position when it was spotted. Like Subphase A, we created a chart to record our observations for Subphase B. The chart consists of when each scenario was

started, when the UAV appeared on ATAK, and when the watch stander reported it to the on-scene commander. We monitored both VHF radios and ATAK to record the time a report was made. Results of the test and objectives will be further discussed in Chapter V.

Depending on the device running ATAK, either a mobile Wi-Fi hot spot or the device's cellular connection was used to establish the Wide Local Area Network (WLAN). The Naval Postgraduate team used four devices (two tablets and two phones) for running ATAK during the experiment. One of the two cellular phones had the civilian ATAK loaded, and the other three devices were using the military ATAK version. Another laptop running windows ATAK was also utilized from the NPS campus to also act as a monitor of traffic and run the simulated Scenario 1.

The 95th CST each had an ATAK device that they use as part of their normal operations in the Interagency Operations Center (IOC). They also provided 15 cell phones with civilian ATAK loaded to distribute to each patrol boat team. Being the resident experts in using ATAK, the 95th also integrated 1–2 of its members onto each patrol boat team to help navigate the GUI. All devices were connected to the 95th CST Federated TAK Server through SSL.

F. PHASE IV – NETWORK EXTENSION THROUGH WMN AND MANET

The purpose of Phase IV was to study the potential of taking the current capability of integrating the TAK network and extending it to longer distances, reaching users/devices that may not be connected to an internet source. While evaluating the risks and limitations of any technology, steady connectivity will undoubtedly be one to consider. During our Phase III exercise, it was noted that cell phone coverage was minimal once the vessels were in the middle of the bay.

With this in mind, we considered other possible scenarios where network connectivity may be limited or nonexistent. A few examples of possible instances where there could be little to no network coverage includes in the middle of a bay, out to sea, inside of a cave or mine, in the middle of a large ship or large building, etc. Because of this, we wanted to explore extending an ATAK WMN cluster utilizing an MPU5 wave relay VHF radio signal. Our Phase IV objectives were to test ATAK operability over

WMN, extend the ATAK application over wave relay radios, and apply the simulated GIX radar data. See Table 10 for Phase IV objectives.

Table 10. Phase 4 Objectives

Phase 4 – Network Extension Through WMN Using MPU5
Objective 1: Test and Benchmarking ATAK Operability Over WMN
Objective 2: Extend the ATAK Application over MPU5 Wave Relay Radios
Objective 3: Apply Simulated G1X Radar Data

1. Test and Benchmarking ATAK Operability over WMN

Though we already had the connections established in the previous phases, we needed to start this phase with another connectivity test inside the ATAK network cluster. The key element of Phase IV was to test the ATAK network cluster extension using the MPU5 wave relay. All cellular data was turned off, and previous Wi-Fi connections were forgotten. We then set up a new network cluster using the MPU5 Wave Relay connection. Once we could view each other on our respective ATAK devices, we then opened the browser on the device to search for a website. We received the message that the link could not be found due to no internet connectivity. This message confirmed that we had established an ATAK WMN cluster that was not receiving its information via the internet.

2. Extend the ATAK Application Over MPU5 Wave Relay Radios

To meet this objective, we set up a similar scenario as in Phase III: a G1X radar is monitoring close to the bay area and detects a possible UAV threat in the area. However, in this scenario, the patrol boat in the bay does not have internet connectivity. For instance, the patrol boat would be unaware of the threat because it does not have a situational awareness tool. We used a laptop to simulate the G1X radar sending COT messages to the message router. Like the radar, the laptop would send its data to an NPS TAK server and then push out that data package through an MPU5 radio to the other end-user via the message router, see Figure 17.

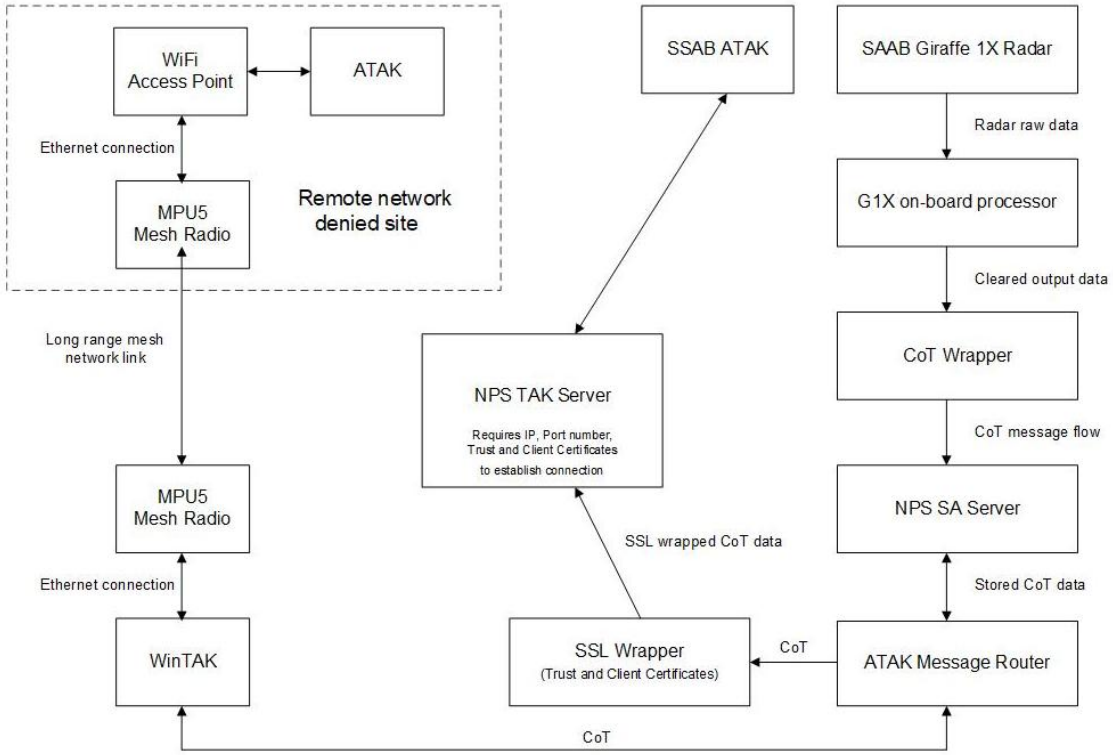


Figure 17. Network Diagram of Phase 4

This connection between the laptop and the "sending" MPU5 radio would be obtained through a direct connection, see Figure 18. It was important to establish a direct line of sight to have a clear signal to the receiving MPU5; therefore, we set up this station on top of the highest building on the NPS campus.

Figure 18. Simulated G1X Radar and “Sending” MPU5 Radio

The second “receiving” MPU5 radio simulated the patrol boat in the middle of the bay. This MPU5 had a Wi-Fi hotspot connected to it to transmit the data to the end-user ATAK device. The patrol boat’s ATAK device would be connected to the MPU5 via Wi-Fi, allowing for the G1X’s data signal to be displayed, see Figure 19.

Figure 19. “Receiving” MPU5 Radio and Wireless Hotspot

To reenact the patrol boat in a dead zone, one of the team members drove to Fisherman’s Warf and ensured that their only Wi-Fi connection was through the hotspot connected to the MPU5, and cellular data was turned off. This scenario ensured that we had a “disconnected” entity that would need to rely on a network extension to have situational awareness. For an overview of the Phase IV network, see Figure 20.

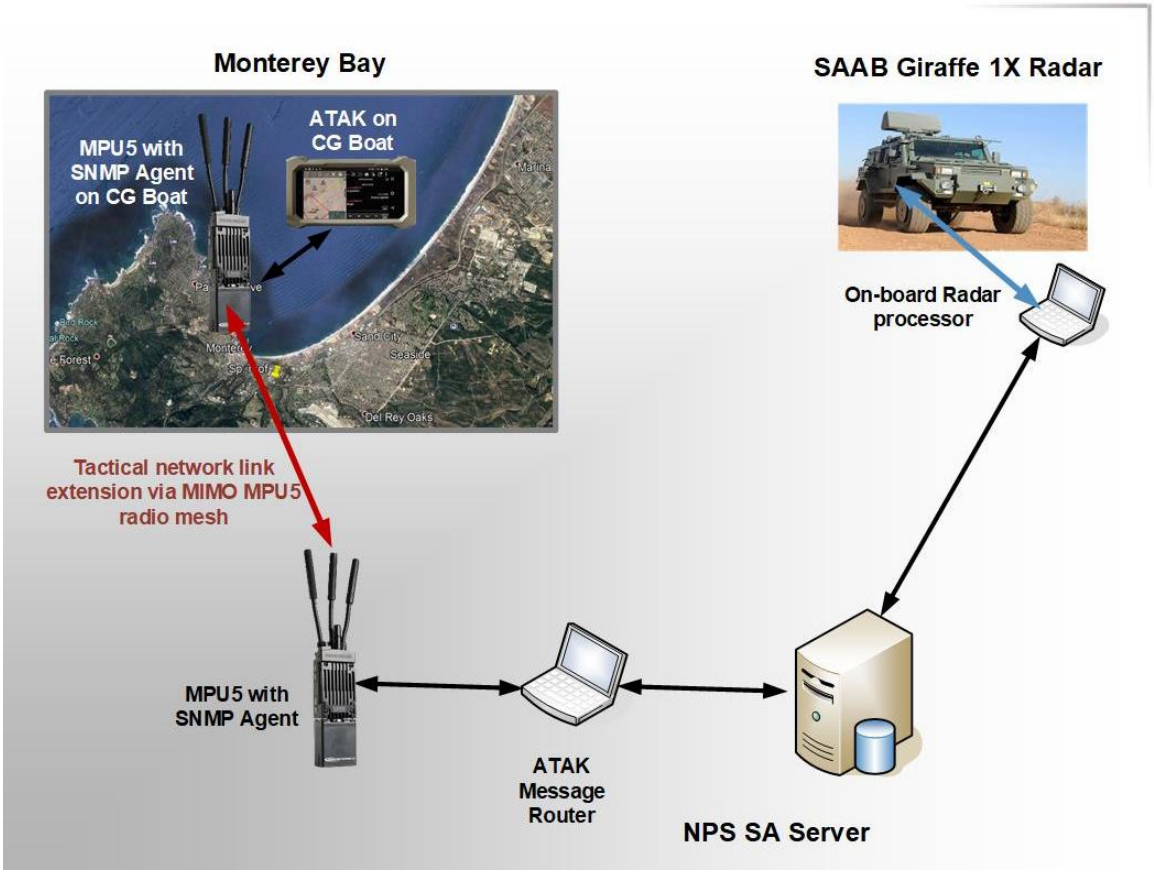


Figure 20. Overview of Phase 4 Network

3. Apply Simulated G1X Radar Data

Once everything was in place, we ran the program simulating the radar transmission and enabled the message router capability. At first, the "patrol boat" was unable to see any transmission, and we had to coordinate the location and the direction of the MPU5 radio antennas. We were able to confirm that the simulated radar data was successfully transmitted to the "patrol boat" ATAK device by viewing the unknown UAV entities shown in red on that ATAK device, see Figure 21.

Figure 21. Confirmation of Successful Transmission of G1X Data to Receiving ATAK Device

V. RESULTS AND ANALYSIS

In this chapter, we discuss the results and conclusions from Phases III and IV presented in Chapter IV. Phase III's results are divided into two parts: the PRND Exercise and the UAV threat detection demonstration. Due to the UAV threat detection demonstration being the focus of our research, we further divide that section into its two subphases; Results of Subphase A - detection without the use of technology and results of Subphase B - detection using technology. After examining all the results, we then discuss how both sections performed together and possible reasons for the results.

Overall, we found that there are variables we were unable to control, and subsequently affected our results. The biggest variable we did not account for is determining who were the watch standers reporting unauthorized UAVs. Additionally, the USCG was not fully aware of our study and thus focused its full effort towards the PRND mission.

A. PHASE III—SF BAY GUARDIAN

As outlined in Chapter IV, we leveraged SF Bay Guardian to conduct a demonstration inside of an exercise. In particular, we worked with local, state, and federal maritime first responders and the United States Coast Guard – Sector San Francisco PRND to create a large-scale exercise simulating a response to a "dirty" bomb threat on a commuter ferry within San Francisco Bay. For a more detailed report on the master exercise scenario, see Appendix A. A list of all the exercise objectives and associated core capabilities can be found in Appendix B.

It should be noted at this point that two separate events had a significant impact on our results. These decisions were out of our control and happened a day or two before the exercise. The first was that a decision was made to no longer have a security zone set up, and the second being that the IOC was only partially set up and manned. The security zone, and personnel to field it, was not implemented due to staffing shortages among the USCG team. Not setting up a security zone made it very difficult to collect any data on the watch stander's ability to see a UAV threat and report it because, practically, there were no watch

standers. The IOC was not fully set up due to COVID-19 requirements. The space that typically is set up to function as the IOC (with monitors, phones, and other command and control (C2) equipment) did not provide adequate space for all the IOC members as set out by the USCG COVID-19 response policy. As a result, the IOC was instead implemented on Pier 1 using some folding tables and the laptops that the participants had brought with them. Without having a formalized IOC center and chain-of-command, it made it impossible to know if the reports of unauthorized UAVs were ever reported.

Although we hit numerous roadblocks, we were able to conduct both the PRND exercise and UAV threat detection demonstration with some limitations. Next, we will discuss the results from the PRND exercise and UAV demonstration.

1. PRND Exercise Results

The exercise was based upon a series of scenarios that ran in the San Francisco Bay just off Treasure Island. See Appendix C for the scenarios. Based on the information discussed during the after-action report of the exercise, all exercise objectives were met (some with comments) for all four scenarios. Even though many of the boat crews had never worked together and some of the scenarios were novel to them, each team followed the SOPs and TTPs and successfully managed each scenario.

2. UAV Threat Detection Demonstration Results

Before the exercise went live, we introduced the Android Tactical Awareness Kit (ATAK) to local, state, and federal maritime first responders to help them see incoming UAVs via live radar tracks fed into ATAK and viewed directly on their cell phones. The morning of the event, we briefed the boat crews on the possibility of UAVs doing surveillance on them and emphasized that any UAV could be a potential threat. The boat crews were instructed in our brief that if any boat crews were to see a possible UAV, they should report it to the on-scene commander for further analysis. Following our introduction, the 95th Civil Support Team (CST) held ATAK user training on the pier with each boat crew. Members from the 95th CST were deployed as SMEs in using ATAK with local, state, and federal maritime first responders to assist them with the technology.

a. Phase III - Subphase A: Detection Without the Use of Technology

Once the scenario was underway, we seamlessly worked with the Alameda County Sheriff's Office (ACSO) as our Red Team asset launching the UAVs. As stated in Chapter IV, we started with our reconnaissance mission and used DJI's Mavic 2 Enterprise, see Figure 22, to fly a circular pattern around the boat crews to see if it would be noticed. We used the Mavic first because it was the smallest and quietest UAV the ACSO had (12.7" x 9.6" x 3.3") and would be the most difficult to detect. We started with the most difficult to detect UAV because we wanted to test how far away from the vessel we could approach without being detected. The UAV had a built-in camera, so we were able to see if the crew members were taking notice of the UAVs. We monitored the UAV cameras to see if participants were looking, waving, or pointing at the UAV; none of these actions were observed. Also, we were monitoring all assigned radio channels for any alerts that UAVs may have been detected. After our flight patterns were conducted with no detection, we then decided to fly closer to try and to get some response from the crews; however, this also did not elicit any response.

Figure 22. DJI's Mavic 2 Enterprise

The Red Team then deployed a DJI Matrice 300 RTK, see Figure 23, a much larger (31.9" x 26.4" x 16.9") and louder UAV. At this point, roughly an hour into the exercise, we received an ATAK chat message that UAVs had been spotted. However, the UAV was detected, and a photo was posted onto ATAK by one of the exercise evaluators, not participants, see Figure 24. This situation was beneficial to us in two ways. First, it showed the capability of posting photos on the application, and second, it highlighted the limitation of using different versions of ATAK. The controller who took the photo and loaded the

image was using a military ATAK device. The civilian ATAK users could not see this photo (to include the IOC representative using a windows version of ATAK). After roughly another 30 minutes of trying to see if the participants would detect the UAV, including using the UAV's speaker capability to talk to the participants, no visual or audible detection from the participants was given. For this reason, we were unable to log or account for any of Subphase A's objectives.

Figure 23. DJI's Matrice 300 RTK

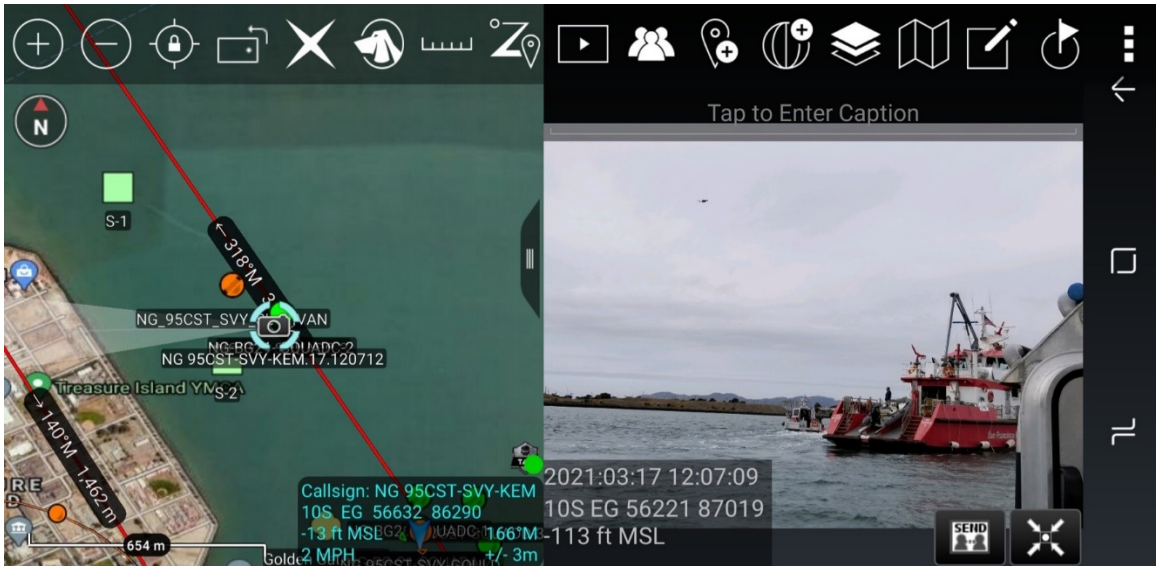


Figure 24. UAV Detected and Uploaded into ATAK

b. Phase III - Subphase B: Detection with the Use of Technology

Due to none of Subphase A's objectives being met, we started Subphase B with an alert to all participants using ATAK's chat feature, warning them of a potential UAV threat. We then activated scenario one, discussed in Chapter IV. The simulated G1X radar data being generated from the NPS message router was sent to the 95th CST TAK server, and immediately multiple icons showed up. The simulated G1X on Yerba Buena Island (south of Treasure Island) and friendly UAVs appeared as both green and blue as icons on the ATAK device. After roughly two minutes, four new red icons appeared, coming from the east. By selecting any of these icons, the boat crews would have been provided further information regarding the make, model, speed, altitude, etc., of the UAV, as well as identified them as an "unknown" status or as a potential threat, see Figure 25.

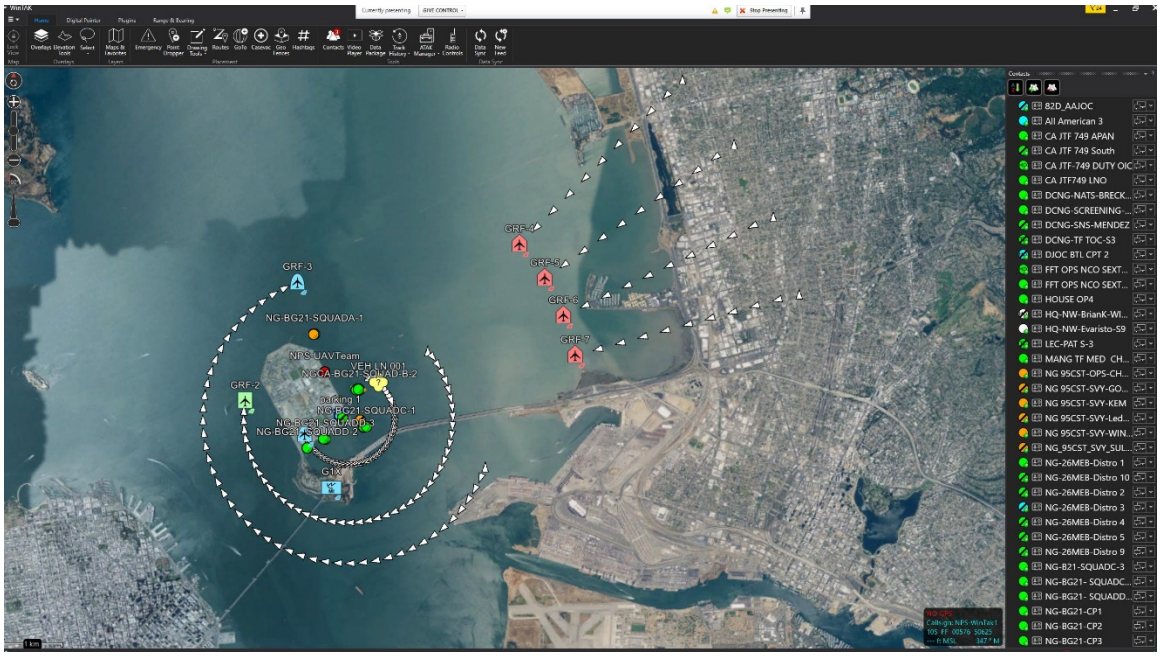


Figure 25. Scenario 1 Identifying Four Potential UAV Threats

After completion of scenario one, which ended with UAVs reaching the boat crews and eventually disappearing, there were no reports or alarms of UAVs. We discussed this with some of the members at the IOC and explained how ATAK would have worked when a radar was deployed. For instance, if a radar was deployed and ATAK was reporting unknown UAVs, watch standers could orientate themselves to observe the UAV. From there, watch standers could report what they see visually to the IOC and possibly determine hostile intent. From there, we moved on to scenario two.

Scenario two was similar to scenario one, except the data was coming from SAAB, located in Sweden. Also, more unknown UAV threats were involved, see Figure 26. After running this scenario and getting the same response from the participants, we ended our part of the exercise. We conclude that none of the objectives in Subphase B were met.

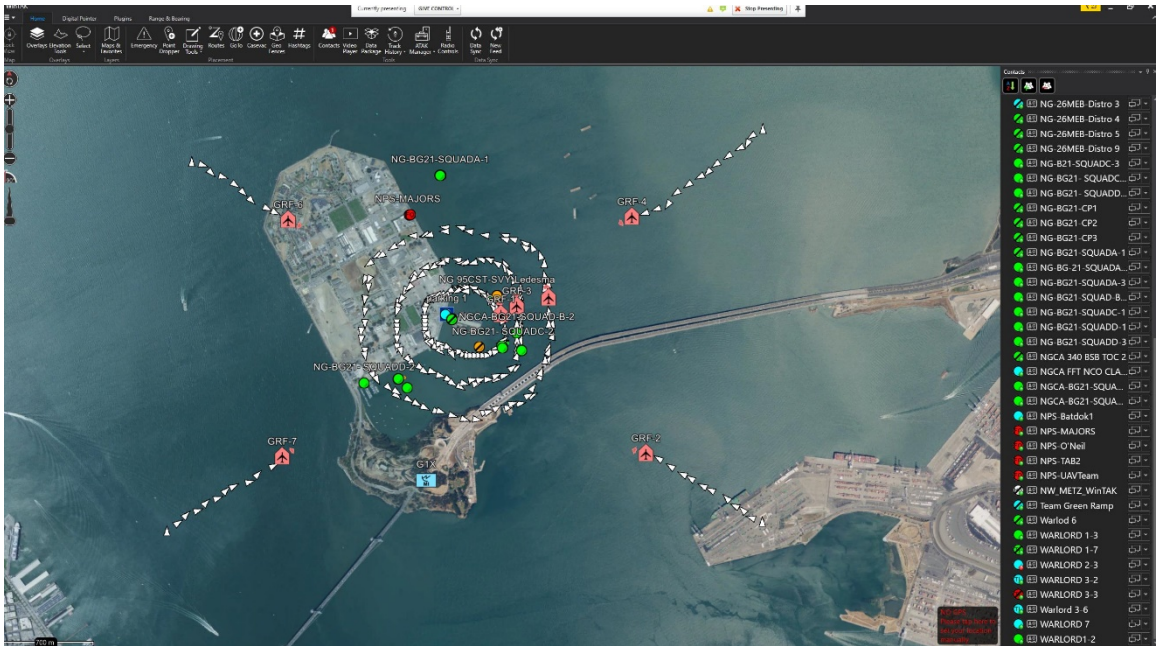


Figure 26. Scenario 2 with Seven Potential UAV Threats

3. Analysis

There are many great outcomes that came from conducting SF Bay Guardian 2021. Through our research and testing, we have discovered that the integration of radar sensor data into a situational awareness tool is entirely plausible. This analysis will go deeper into some of the lessons learned that were discovered from the demonstration and then will discuss the importance of interoperability when going through the decision-making process outlined in Chapter III.

a. Security Zone Function was Not Enforced

As was discussed earlier, due to COVID-19 and the vast number of roleplaying entities that participated in the Bay Guardian exercise, the USCG determined that the security zone function would not be enforced, and the IOC function took place with a lesser capability on Pier 1. No single authority was identified as the lead on the exercise. Without a centralized command, we could not capture any watch stander reports of UAVs.

b. Teams Trained to Focus on the "Immediate Threat."

The immediate threat was clearly the nuclear IED on the San Francisco Bay Ferry. Due to manning requirements and the training opportunity, the security element may have been "turned off" in their minds, leaving them not paying attention to the UAVs flying overhead. Exercise evaluators reported UAVs, but the players did not. The exercise evaluators did not report UAVs because that was not their role.

c. Too Many "New Things" All at Once:

The number of tasks a human can handle at one time is highly debated; however, humans are only able to process so many different things at once. Some studies suggest that true multitasking is not possible and that an individual can only fully think of one thing at once (Gazzaley, 2017), while others say the human mind has the capacity to focus on up to four different things at once (Awh & Vogel, 2008). This San Francisco Bay Ferry Exercise introduced at least seven new characteristics for the role players to focus on, many of which were new technologies, which no prior training had been given. The boat crews did receive a very quick "just in time" training that consisted of showing the crew what the ATAK application looked like and what the primary buttons they were to push. To help alleviate this knowledge gap, the 95th CST (resident experts on using ATAK) integrated one of their team members onto each boat crew to assist in using the ATAK device. However, after talking with many of the 95th members, most of the crews' attention was on the FirstNet phone and how to use RadResponder. This makes sense, as the RadResponder application-related directly to the primary focus of the exercise, the nuclear IED. The following items that involved "new things" were brought up by the agency team leads during the AAR:

- New Relationships

There was a total of 30 separate agencies participating. This included 14 separate boat crews, which is a dramatic increase from the last event that included six agencies total. Many of these teams have never worked together before. This will affect each agency's ability to work together, as described earlier in Chapter III. Novel situations are more

difficult to determine a cause-and-effect relationship. Having no set procedure in place for UAV threats, it is possible that many of the agencies were making assumptions about the other team's awareness and reporting of the UAV threat.

- New Threat

This scenario of radiological IED on a ferry had never been roleplayed before. Our demonstration added to that by also including an element novel aerial threat using UAVs, yet another scenario that has never been role-played. Like the difficulties faced with new relationships, adding novel threats that have yet to have patterns to recognize presents a greater challenge to face for the operator. We compounded this challenge by creating two novel threats.

- New Technology

This exercise was the first time "FirstNet" phones had been used, the first time using RadResponder (loaded on FirstNet phones), the first time using ATAK, and the first time loading simulated radar sensor data into ATAK during a live event. One participant on the boat crews verbalized being "overwhelmed" by all the new technology thrown at them.

d. ***C2 Communication Challenges***

As previously stated regarding the IOC, personal cell phone numbers were distributed, and boat crews were instructed to use those personal cell numbers instead of the IOC. Communication is essential for effective C2, and though we did have identified VHF radio channels for the boat crews to use, either the radios were used to communicate when the role players were to rotate to the next station or, in a few instances, they were used by the participants to call in radiological findings. It appeared that, as stated earlier, the primary method of communication was through personal cell phones (which we were not monitoring). One of the boat crews also described trying to figure out how to use the FirstNet "push to talk" function, and once they figured that out, they seemed to use that function a fair amount as well. Other forms of communication channels were observed during the event to include: VHF radios; ATAK chat function; FirstNet "push to talk"; and

UHF radios. Having multiple forms of communication outside of the predetermined methods of communication presented problems for us to accurately observe participants' ability to detect and report UAV activity.

e. Cell Phone Coverage Lacking:

One of the participants mentioned that there were "dead areas" of coverage on the bay, leading to the ATAK phone having little coverage. This led to a loss of connectivity and drained the batteries much faster than normal. We received a coverage speed report from AT&T that confirmed this complaint, see Figure 27. On the pier, we were getting download speeds of up to 102 Mbps and upload speeds of around 13 Mbps. In the Bay, however, speeds dropped to six and two Mbps, respectively. This led us to further research extending the network past where Wi-Fi or possibly any cellular coverage could reach, which will be discussed in Phase IV.

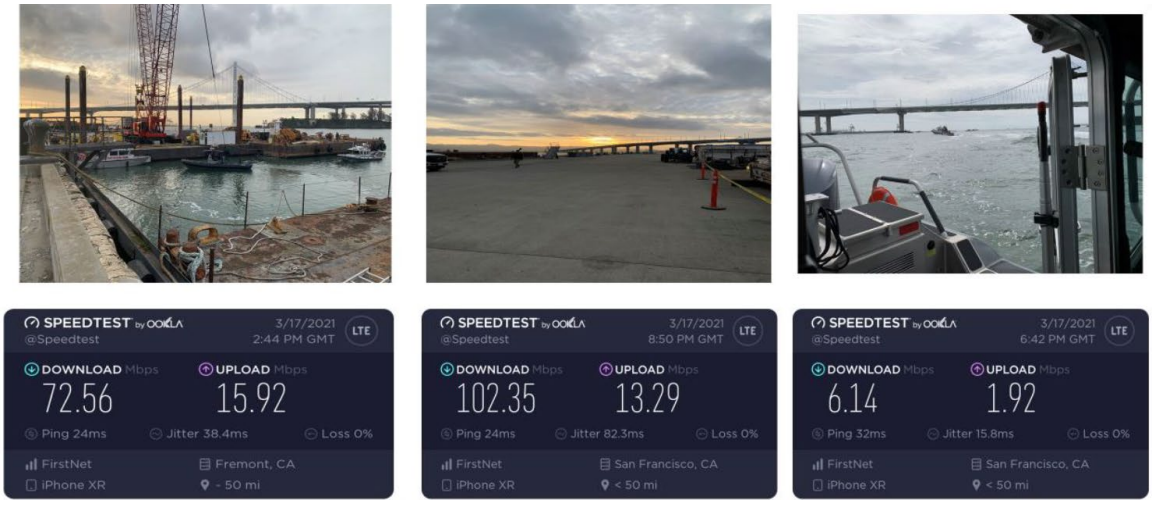


Figure 27. Bay Guardian 2021 Exercise Coverage Speeds

f. Interoperability

To integrate phased-array systems (G1X) into an SA tool (ATAK) to enhance decision-making capabilities, it is important to appreciate both tangible and intangible attributes or concepts that are implicated in this development. Human agents as sensors,

hardware, and software are considered the tangible attributes to integration. Codified frameworks or models applied to foster integration or interoperability are representative of intangible concepts. Both aspects play their respective vital roles in optimal development, deployment, and sustainment of the broader SA enhancement system.

(1) The Duality of Man and Automation (Tangible Attributes of Integration)

Challenges related to situational awareness first stem from the human aspects of critical operations or scenarios. One of the categories of Decision-Making Framework is the naturalistic modality based on individual experiences and depends on the ability of a given subject and their level of acuity or SA. This presents potential challenges due to the lack of standard capabilities from one individual to the next. In stark contrast of automated systems are designed with higher levels of specificity and levels of automated SA that their capabilities render human-dedicated SA close to obsolete when comparing SA sensitivity. This is especially important in highly sensitive or combat environments where UAV detection and measures to secure or neutralize targets are extremely time-sensitive. Humans, like sensors, can detect UAVs. However, organizations such as the DOD integrate specialized automated systems such as ATAK and G1X to enhance overall SA while enhancing other decision-making aspects, such as procedural and analytical. These tangible attributes flourish in their capabilities of a 3D electronic scanned array (G1X) and high-level spatial atmospheric orientation tools (ATAK). These capabilities, along with auxiliary applications designed as conduits for interoperability (COT), coupled with mobile characteristics, allows for detection system integration that serves as force multipliers in command-and-control decision situations (Balcik, 2018). In this interoperable relationship where the human sensor is often attributed to the naturalistic decision-making aspect (Klein, 2008) of operations, the addition of G1X, ATAK, and COT helps to automate procedural and analytical decision-making tasks.

(2) Multi-Framework Application (Intangible Concepts of Integration)

While human assets and technical systems play a vital role in integrating radar data and SA tools, ultimate courses of action will be dependent on observation, orientation, and decisions. The OODA Loop model does this precisely. In San Francisco Bay Guardian

2021, the exercise involved an encounter with a novel situation (potentially malicious UAV) with multiple agencies engaged with varying roles. Ideally, the participants would have detected or observed imperfect data of the potentially malicious UAV and would have fed the data for orientation or a higher level of knowledge specificity. This may include speed, trajectory, distance, range, and altitude. Commanders would have then informed their decision process, feeding the determined decision into action. However, in such a novel situation, it would be assumed that most participants lacked an adequate understanding of the situation or resulting patterns. Therefore, the Cynefin Framework is a vital sense-making tool to incorporate into the OODA Loop model.

For the purpose of this study and the case discussed, the final objective should not be one single framework but how to integrate these models to arrive at optimal levels where capabilities are leveraged to their full capacities. Cynefin Framework's strength is its sense-making capabilities, which can enhance the OODA Loop when new situations are presented to lesser experienced individuals. Similarities consist amongst complicated and complex domains, but the complex domain has the valuable ability to facilitate adaptation (Klien, 201o7). In this case, this would be a complex domain due to an emergent situation and would then call for a Probing/Sensing/Responding decision model. In UAV detection situations, these codified frameworks are applied to foster integration or interoperability and represent intangible concepts that, along with tangible attributes, deliver sound integrated system processes.

4. Summary

During the 2021 San Francisco Bay Guardian exercise, the authors identified a problem due to the lack of detection, reporting, response, and engagement of any UAV threats presented. This was a problem due to the UAV's potential as a critical threat on par with the nuclear IED in the exercise. Assuming the tangible and intangible assets were available to all relevant participants and assuming all hardware and software were fully operational, shortfalls to UAV detection may be attributable to elements outside the infrastructure realms. With a large and diverse cadre, participants may have been challenged with social or non-technical interoperability limitations. Because of these

challenges, it is vital to take a structured approach in assessing, defining, and characterizing technical and non-technical aspects of interoperability within a structured framework to better implement strategies to mitigate these factors. In this case, non-technical interoperability issues should be the point of concentration as a systematic deconstructive approach presented through the Interoperability Framework. Leaders may find solutions to cultural barriers when identified, isolated, and mitigated through enhanced degrees of collaboration, improved training mechanisms, or establishing shared semantics. Semantic Interoperability, as an example, focuses on standardizing language to points where terms and expressions are explicitly defined and recorded to facilitate broad use and understanding across organizational bounds. This is especially applicable within the San Francisco Bay Guardian exercise, G1X/ATAK integration, and joint operations within the DOD.

Human assets remain the foundation of the active DOD component, and resilience in their capabilities is essential for achieving mission objectives. The balance may tip towards technical or artificial intelligence-centric forces, but automated systems are currently tools for humans to operate. Tangible attributes must be reconciled with intangible concepts and social attributes of interoperability to optimize systems design, capability, and sustainment.

B. PHASE IV - WMN EXTENSION EXPERIMENT

As we discussed in Phase III, we discovered that cellular coverage was lacking in the middle of the Bay, which resulted in sporadic network transfer speeds. Loss in cellular data revealed a new gap in the capability of a sustainable ATAK network. Not only could network coverage be lacking in the middle of a bay, but it could also be degraded by going deep underground in a mine, exploring caves, or any other instance where internet connectivity is non-existent or sporadic in bandwidth availability. For this reason, we wanted to explore the extension of an established network using Persistent Systems' MPU-5 radios to explore the possibility of extending the wireless mesh network, ensuring that the devices were "disconnected" from any outside network device.

1. Results

Before starting the experiment, we wanted to ensure that there was a baseline bandwidth connection when all the components were in a central location, using the Wave Relay Management Interface, native to the MPU-5 system, see Figure 28. Our baseline resulted in an upload speed of 11.7 Mbps and download speed of 17.9 Mbps, successfully meeting Objective One, "Test and Benchmarking ATAK Operability over WMN."

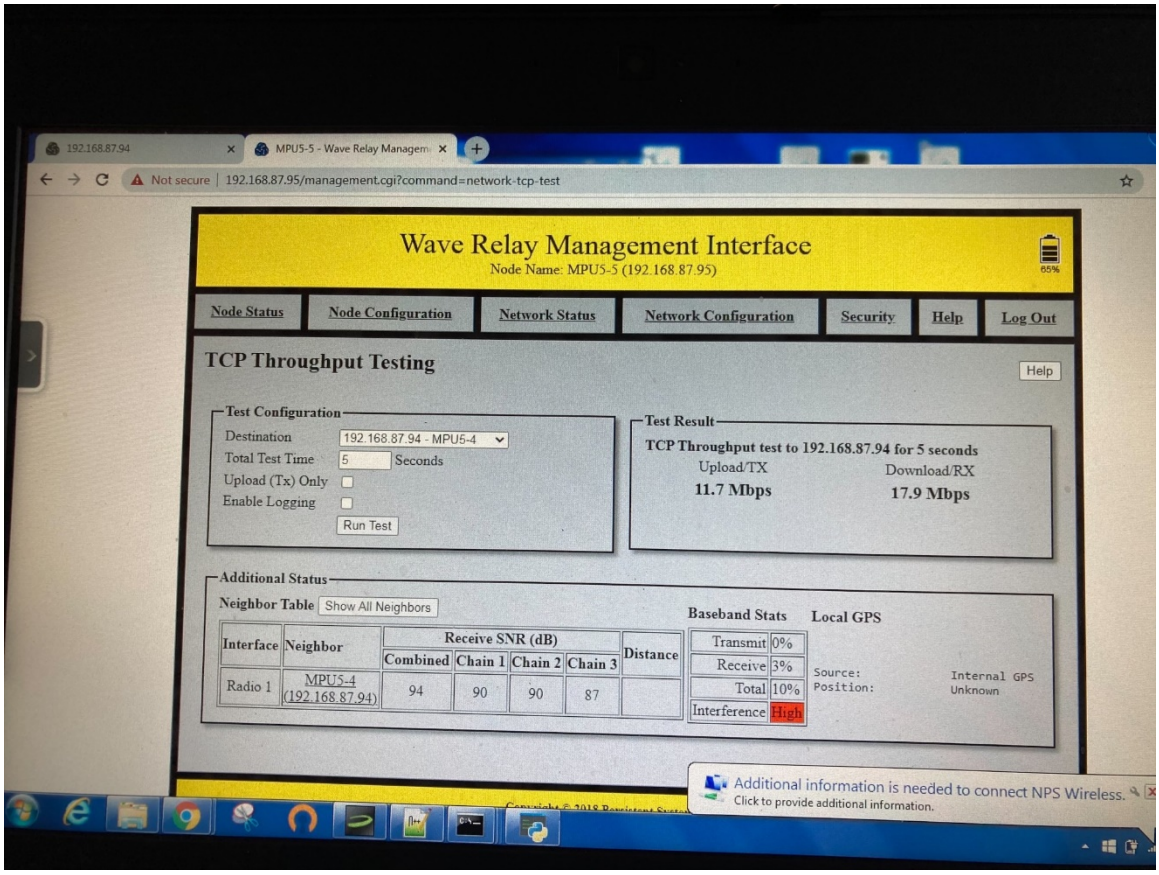


Figure 28. Baseline TCP Throughput for WMN Extension, Before Experimentation

As described in Chapter IV, we had one participant remain with the base MPU-5 that would be directing the signal to the user, who would be operating in a "non-networked environment" using a separate MPU-5. Getting a complete line of sight window between the two MPU-5s was a slight challenge, but through open communications, we were able

to use natural landmarks to get the two MPU-5s connected. We then wanted to test the TCP throughput of this new connection to see how much of a degradation of bandwidth (if any) was affected, see Figure 29. We found that though there was some, 11.9 Mbps upload and 9.3 Mbps download, it was not enough to affect the data package transfer. Verifying an established connection also confirmed successfully completing Objective Two, "Extending the ATAK Application over MPU-5 Wave Relay Radios".

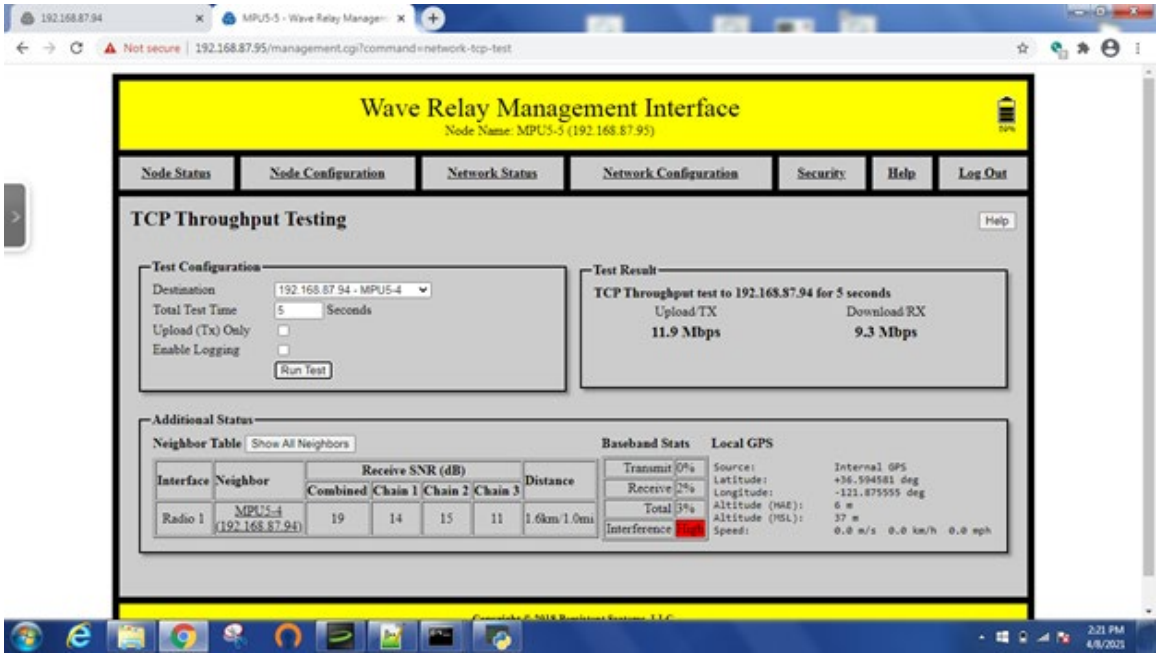


Figure 29. Actual TCP Throughput for WMN Extension, During Experimentation

Using the GPS function native to the MPU-5s, we were able to see that we successfully covered a one-mile range in this experiment, see Figure 30. Once we had line-of-sight, the non-networked device was immediately able to start getting information, and we were able to transmit simulated G1X data to that device, completing Objective Three, "Apply Simulated G1X Radar Data".

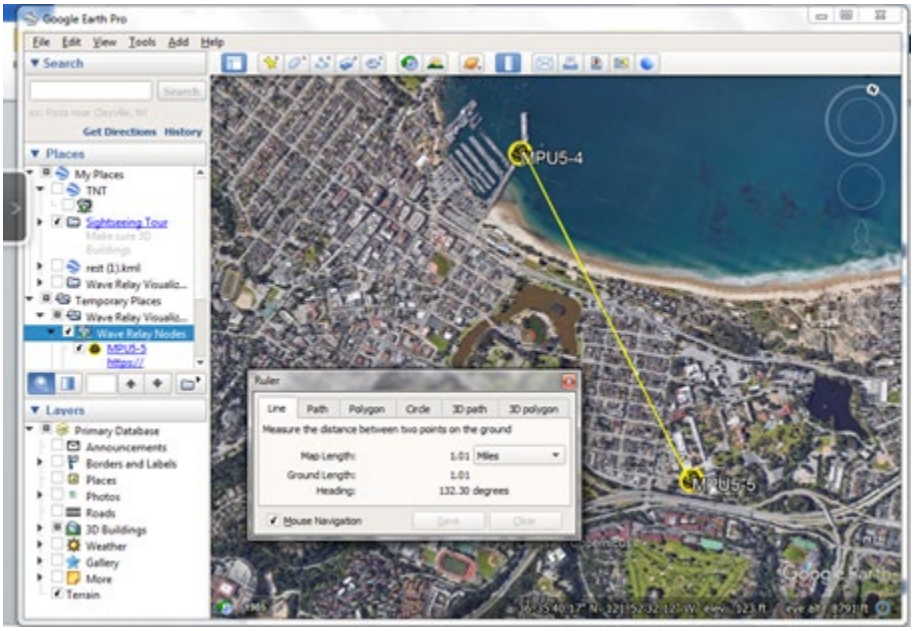


Figure 30. Successful Transmission of Data at 1-Mile Range

2. Analysis

Though all the objectives in Phase III were met with little difficulty, line of sight was still a critical determining factor in this experiment. Ensuring line of sight outside of having established communications via radio link, for instance, could be an incredible challenge for the operators using ATAK. Depending on the environment or limitations of equipment, having UAVs acting as line-of-sight relay points, in any circumstance, would greatly enhance the MPU-5's ability to connect to one another. In our experiment, we were on the highest building on the NPS campus and had a direct view of the wharf where the other participant was, but there was a lot of tree coverage between us. We needed to be right in an opening between tree coverage to get a solid connection, but there will be instances where that will not be a possibility, such as in a heavily forested area, an urban area with numerous large buildings, etc. Utilizing UAVs directly overhead between the two radios would allow a greater line-of-sight capability and could keep a more stable connection if users or radios needed to move after establishing a connection.

Another limitation that was found in this experiment was that, based on how it was structured, the connection that was established was only one way – from the message router

to the end device. If the end device wanted to communicate back, that message would not be received to any other ATAK user on the network. This possible future research will be discussed more in Chapter VI.

VI. CONCLUSION

In this study, we set out to better understand how integrating SAAB's G1X radar system into the TAK environment over a wireless mesh network and provide DHS and DOD commanders with a tool to assist in the detection of UAVs. Our research showed that it is possible to integrate the G1X radar into the TAK situational awareness environment. However, there are numerous limitations when introducing new technology during a crisis event. In this chapter, we will reflect on our research, results, and its significance.

A. SUMMARY

This study has potential limitations that affect the quality of our findings and limited the ability to answer our research question. First, Coronavirus 2019 (COVID-19) brought many challenges to our research. COVID-19 prevented SAAB from bringing their radar technology to San Francisco and prevented us from traveling to Sweden to experience and further test the technology. Additionally, due to COVID-19 protocols, the USCG did not provide a space for a formal command center. This was mitigated by having a formal command center setup on Pier 1; however, the person driving the tents was stuck in traffic. Not having a formalized chain of command created confusion with participants, and formalized reports of UAVs were either not given or lost in confusion. Although COVID-19 created many problems, it also brought us unforeseen opportunities to work with SAAB and simulate radar data while working remotely. The SAAB Team based in Sweden generously worked with us to demonstrate the technology during San Francisco Bay Ferry exercise.

Secondly, due to time constraints and access to classified information, we limited our scope to only unclassified information. Limiting our scope to the unclassified realm only affected the quality of our findings. This prevented us from including current tactics, techniques, and procedures (TTP)s and recent incidents that have taken place over the past year. This would have given sustenance to future studies that could concentrate on laws and regulations enforcing remote identification, security zones, and privacy issues.

We first started out using a strict quantitative methodology to study the technology of using a radar within a wireless mesh network. We proposed to use variables of speed, time, and distance during the San Francisco Bay Exercise but realized during the exercise that there were outside variables we did not account for. We then switched to a more qualitative methodology using empirical research of how first responders and the USCG would react to unknown UAVs. We attempted to describe what happened based on direct observation of the event and the after-action report. Due to the possibility of using human subject research, we excluded all interactions with the participants and concentrated on the technology surrounding radar in a wireless mesh network.

Our demonstration was based inside of a larger exercise whose focus was primarily based upon a different radiological threat. Due to unforeseen logistical issues and training opportunities, the USCG canceled the security zones a week before the demonstration, and watch standers were never assigned to look for a UAS threat; therefore, we were unable to collect pertinent data. Additionally, we do not know if watch stander training is adequate or deficient for UAS detection.

One measurement that we did not consider until the event was attaching an ATAK device to a larger UAV so it could capture its exact GPS coordinates in real-time. This would have provided watch standers the ability to locate and identify a UAV while it was flying in the air. Since we did not attach an ATAK device to the UAVs, it was exceedingly difficult to differentiate a UAV from a bird and the background of San Francisco.

Our research was affected by our bias of deploying this technology without considering that during the exercise, numerous other technologies were also being deployed. For example, there were two situational awareness tools ATAK and RadResponder which required participants to carry two separate Android devices. Additional technologies that were exercised included boat-mounted radiation detectors, AT&T's FirstNet, and Airgain Connect.

A second assumption we made is that we had expected that radar was going to provide accurate and timely data to give commanders more time to respond to a UAV threat. This we believe is true; however, more technology does not solve the problem of

having more than one threat. For example, a participant following the exercise explained to us the exercise felt like facing a loaded gun (an immediate radiological danger), but then you have a secondary UAV threat that you are not fully paying attention to.

B. SIGNIFICANCE

Simulated G1X Radar data was successfully integrated into the ATAK application and transmitted over a wireless mesh network. This provided watch standers with an early warning system to provide on-scene commanders more time to make C-UAS decisions. Users who wish to participate in the network may download ATAK from the Google Play store and view this data with little effort. ATAK provides a platform for multi-governmental agencies to share resources and coordinate efforts. Additional work will have to be done with a live radar relaying information over a wireless mesh radio, and interdepartmental and agency TTPs must be created to coordinate those efforts.

During this thesis, we learned how the FAA, FBI, and FCC were coordinating to protect privacy and wiretapping laws while combating the problem of UAVs flying in unauthorized airspace. As of our publication date, the San Francisco Sherriff's Office lacks the ability to act against unauthorized UAVs because the FAA designates a UAV as an aircraft; therefore, it is considered a hijacking if the Sherriff's Office remotely forces it to land. Additionally, if the Sherriff's Office were to jam the UAV, there may be second, and third-order effects when doing so over a crowded or populated area. UAV regulations keep the "good-guys" honest and create jurisdictional nightmares leaving servicemembers in charge of protecting and serving American citizens, that are defenseless against a UAV threat. Although federal regulators from the FAA, FBI, and FCC have been working in concert to instate federal regulations, those federal regulations have had second and third level effects on state and local first responders and their ability to do their job. Through the firsthand experience of seeing the capability of integrating radar sensor data with situational awareness tools like ATAK, a greater number of personnel have been exposed to the "art of the possible." This deeper awareness of what capabilities are out there may hopefully guide the direction of future policy and regulation development.

The San Francisco Bay Ferry Exercise created an informal communications network among many of the participants. This exercise brought together UAV pilots from Alameda County Sherriff's Office, Contra Costa Fire Department, San Francisco Fire Department, the local UAV school on Treasure Island, and regulators from the FAA. Members from these departments were able to practice flying UAVs over maritime patrol boats and the San Francisco Ferry. Like wargaming, it provoked collaboration and teamwork between various departments and services. More opportunities that allow experience in the detection, identification and mitigation of UAVs should be explored in an interagency setting.

Although the members of the rapid crisis response team had a tough time using the various technological situational awareness tools, it demonstrated how important it is to design technology around the end-user and hold frequent training throughout the year.

C. FUTURE STUDY

We recommend a future study based upon a multi-day demonstration of unmanned technology to include UAVs and unmanned surface vehicles (USVs). To form a baseline, the USCG should set up a tight security perimeter around a high-value unit such as a USN vessel pulling into port. This will gauge if the USN and USCG have proper tactics, techniques, and procedures (TTPs) in place to counter the unmanned threat. The participants should not be briefed on any unmanned threats to exercise their TTPs for countering these unmanned threats. Following the first day event, a debrief of the watch team should take place, and someone should capture their reactions on the bridge and combat information center.

A tabletop exercise then should take place between the USCG, USMC, and USN to discuss how to counter a UAV and UAS threat while pulling into port. Following the tabletop exercise, training should be held for the watch standers and note any differences in the capability to detect and react to an unmanned threat in a subsequent event.

Observers had a tough time spotting small UAS, even noisy ones, during Bay Guardian 2021 exercise. Future work should focus on automated sensors along with cueing

technology to prepare and cue automated defenses. Every time a vessel is out to sea, it is susceptible to unmanned threats, and these threats are growing every year.

Finally, we must consider usability. There are many situational awareness tools currently in use in the military and available on the open market. The end-user must be able to observe and assess the threat environment quickly. In the San Francisco Bay Guardian Exercise, participants were given multiple hand-held devices that caused confusion. Situational tools should be readily available and preconfigured on a device that the user carries all the time, such as their cell phone. First responder's preconfigured devices should have access to emergency communications systems with a myriad of backup links to include cell phone towers and wireless mesh networks.

D. CONCLUSION

The unmanned fleet is around the corner. The problem will only get larger as artificial intelligence and machine learning systems get more advanced at transporting consumer goods worldwide. It is critical for the DOD to fill the current gap in the detection and identification of UAVs and develop SOPs and TTPs that can be quickly implemented to start training the fleet. Without the integration of technology and the training of its fighting force, the unmanned threat will become more advanced and unknown.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. SAN FRANCISCO BAY GUARDIAN SCENARIO

The information in this appendix was obtained from the *San Francisco Bay Guardian 2021 Controller/Evaluator Handbook* (PRND Focus Group, 2021), outlining the overall scenario for the Guardian Bay exercise.

Intelligence sources indicate slightly elevated threat levels for terrorist attacks across the country and warn that state and local jurisdictions should implement all prevention and detection capabilities available at high priority and high-risk sites. In response to reports of attempted theft of radiological/nuclear materials from a high-security research facility in the San Francisco Bay Area as reported by the Northern California Regional Intelligence Center (NCRIC), local government law enforcement, fire hazardous materials, and explosive ordinance teams agree with the FBI to increase their radiological/ nuclear detection and interdiction efforts to an Enhanced Steady State mission state.

To ensure unity of effort, the FBI San Francisco Field Office is providing oversight of land-based PRND "Enhanced Steady State" activities planned to take place at various amusement parks, sports venues, and tourist attractions that could be considered as attractive targets to terrorists. The United States Coast Guard-Sector San Francisco is coordinating all maritime PRND activities.

On Wednesday, 17 March at 0900 hours, a TSA VIPR team member riding on a commuter ferry notices that his/her personal radiation detector is alarming during their patrol of a commuter ferry that is deadheading back to its homeport (Larkspur). Based on his/her interview of a person of interest combined with the totality of circumstances, the alarm cannot be satisfactorily adjudicated. Other members of his team notify their chain of command and the local FBI WMD Coordinator.

Based on the information provided by the TSA VIPR team, the FBI WMD Coordinator alerts his/her chain-of-command of the incident, who in turns requests the USCG to inform the vessel's master of the situation and direct the vessel to a quarantine area under escort until the FBI stabilization team can adjudicate the alarm. While they prepare to be transported to the commuter ferry, the FBI stabilization team requests the

assistance of the USCG-Sector SF to form a safety and security zone around the quarantined vessel. They also reach out to the San Francisco police and fire departments, the Oakland police, and other law enforcement and fire departments with maritime PRND capabilities for assistance.

In response, the USCG Interagency Operations Center (IOC) begins the process of requesting additional CBRN resources that include the Department of Energy Radiation Assistance Team, Cal-OES, the California National Guard 95th Civil Support Team, and other governmental agencies to assist. In response to the potential threat of an act of radiological/nuclear terrorism, a unified command is established with the FBI, USCG-Sector San Francisco, and Cal-OES that will operate out of the USCG Interagency Operations Center on Yerba Buena Island. Because of scene security concerns and/or a hybrid attack (use of UAVs), maritime first responders will also be directed to be on the lookout for unauthorized drones operating in the area and/or attempting to penetrate established safety/security zones around the quarantine area.

This exercise will require Bay Area maritime law enforcement with PRND detection capabilities and other maritime assets to implement the recently updated USCG-Sector San Francisco PRND Concept of Operations Plan and PRND Standard Operating Procedures in a manner consistent with the Department of Homeland Security's Countering Weapons of Mass Destruction Office's National PRND Concept of Operations Plan. This exercise will also, for the first time, require participating personnel to monitor for the presence of unauthorized drones operating in the area of a maritime incident and/or attempting to penetrate established safety/security zones around the quarantine area. Major Events include:

A. USCG MARITIME SRU ASSETS/PERSONNEL

- USCG will oversee the formation of a "safety/security" zone around the quarantined ferry
- USCG personnel under the direction of their chain-of-command will perform chokepoint operations, wide-area search and vessel search operations

- USCG personnel, when circumstances require, will perform radioisotope identification
- USCG personnel will perform "reach-back" according to their "PRND Concept of Operations and Standard Operating Procedures."

B. LOCAL LAW ENFORCEMENT AND FIRE SRU ASSETS/PERSONNEL

- Local enforcement assets and personnel will assist in the formation of a "safety/security" zone around the quarantined ferry
- At the direction of the USCG, local law enforcement/fire SRU's will continue their PRND maritime operations that include the establishment of choke-point operations, wide-area search, and vessel search
- Local enforcement personnel under the direction of the FBI stabilization team will support the transport of personnel and equipment to the ferry to adjudicate the radiation alarm
- Local enforcement and Fire SRU personnel will perform radioisotope identification when circumstances require
- Local enforcement personnel will perform "reach-back" according to their "PRND Concept of Operations and Standard Operating Procedures

C. UAV OPERATIONS

- Assets and personnel who form the security zones will demonstrate their ability to detect unauthorized UAV's operating in the area or attempting to penetrate established safety/security perimeter around the quarantine area
- Will conduct a Law Enforcement Sensitive (LES) debrief of exercise participants to help guide future Unauthorized UAV operations near or within established maritime safety/security zones

D. RED TEAM

- Alameda County Sheriff's Office personnel will attempt to avoid detection and operate their UAV's in the area and attempt to penetrate established safety/security zones undetected
- USCG Auxiliary, Golden Gate Ferry and USS Potomac crew, and others will perform as role players to add realism to the PRND scenarios. (choke-point operations, wide-area search, and vessel search)

E. 95TH CIVIL SUPPORT TEAM (CST)

- 95th Civil Support Team personnel under the direction of the FBI stabilization team will board the ferry and assist in the adjudication of the alarm by searching a portion of the ferry
- 95th Civil Support Team personnel, under the direction of the vessel master, will board the ferry
- 95th Civil Support Team personnel under the direction of the FBI stabilization team will perform radioisotope identification
- 95th Civil Support Team personnel under the direction of the FBI stabilization team perform "reach-back" according to their "PRND Concept of Operations and Standard Operating Procedures."

F. FBI EOD TEAM

- FBI assets and personnel will lead the effort to adjudicate the radiation alarm and potential threat according to the National Response Plan, Terrorism, Law Enforcement Annex

APPENDIX B. EXERCISE OBJECTIVES AND ASSOCIATED CORE CAPABILITIES

The information in this appendix was obtained from the *San Francisco Bay Guardian 2021 Controller/Evaluator Handbook* (PRND Focus Group, 2021), outlining the overall exercise objectives and core capabilities.

Exercise Objective	Core Capability
Exercise and Evaluate Implementation: United States Coast Guard-Sector San Francisco PRND Concept of Operations Plan (rev. 2, 2019) and PRND Standard Operation Procedures: Practice roles, responsibilities, and coordination with commuter ferry provider, the United States Coast Guard, FBI, local and regional maritime PRND first responders.	Planning
Exercise and Evaluate Implementation: Department of Homeland Security's Office of Countering of Weapons of Mass Destruction, National PRND Concept of Operations Plan.	Planning
Maintain a Common Operating Picture and Maritime Situational Awareness: Practice and evaluate the use of an Android smartphone geospatial infrastructure and situational awareness application at a simulated maritime incident on the San Francisco Bay (ATAK-Android Team Awareness Kit). Evaluate information sharing and management processes using assigned maritime VHF radio frequencies, accountability systems to track vessels, personnel, equipment, and mapping technologies.	Situational Assessment
Test alternative communication paths and interoperability across different radio frequencies.	Operational Communications
Directly connect live, closed-circuit video feed from incident to scene to incident command and Interagency Operations Center personnel.	Situational Assessment
Practice implementation of a unified command with the FBI, United States Coast Guard, and other governmental agencies (OGA's) in response to a simulated act of radiological/nuclear terrorism.	Operational Command
Exercise and evaluate the ability of maritime first responders to board a large passenger vessel to search for the presence of illicit radiological/nuclear materials.	Screening, Search, and Detection
Exercise and evaluate the ability of maritime first responders to perform "choke-point" operations to search for the presence of illicit radiological/nuclear materials.	Screening, Search, and Detection
Exercise and evaluate the ability of maritime first responders to perform a wide-area search for the presence of illicit radiological/ nuclear materials (marina).	Screening, Search, and Detection

Exercise and evaluate the ability of maritime first responders to adjudicate radiological alarms in the maritime environment.	Screening, Search, and Detection
Exercise and evaluate the ability of maritime first responders to perform radioisotope identification.	Screening, Search, and Detection
Exercise and evaluate the ability of maritime first responders to send alarm data to a Department of Energy Triage or LSS for further analysis and identification	Screening, Search, and Detection
Exercise and evaluate the ability of first responders to clear an area without radiological materials	Screening, Search and Detection
Exercise and evaluate the ability of first responders to detect the presence of unauthorized UAV's approaching or having penetrated maritime safety and security zones	On-Scene Security and Protection
Exercise and evaluate the ability of explosive ordnance team personnel and equipment to respond to a report of improvised explosive device (IED) on a commuter ferry	On-Scene Security and Protection
Exercise and evaluate operational security (OpSec) in an environment with invasive video capable drones	On-Scene Security and Protection
Exercise and evaluate the ability to establish and maintain maritime safety and security zones to detect and prevent unauthorized entry by watercraft.	On-Scene Security and Protection

APPENDIX C. MARITIME PRND SCENARIOS

The information in this appendix was obtained from the *San Francisco Bay Guardian 2021 Controller/Evaluator Handbook* (PRND Focus Group, 2021), outlining the Maritime PRND scenarios for the Guardian Bay exercise. This will cover the purpose, the expectations of the participants, and a summary of each of the four scenarios.

A. PURPOSE

One of the Bay Guardian 2021 goals is to exercise the recently updated Maritime Preventive Radiological and Nuclear Detection Regional Concept of Operations (CONOPS) and Standard Operation Procedures (SOP). To that end, three squadrons comprised of local, state, and federal maritime first responders will run through four 80-minute PRND scenarios. All scenarios will utilize real radioactive sources. The four scenarios will be based on the following PRND mission areas: Steady State, Enhanced Steady State - Special Event, and Enhanced Steady State – Enhanced Monitoring. Players will exercise their knowledge of the CONOPS and SOP while adjudicating radiation alarms. A PRND Controller/Evaluator and Level II support personnel will be aboard each participating agency's boat. The PRND Controller/Evaluator will assess the participating agency's boat crew's performance based on the objectives and tasks under the Screening, Search, and Detection Core Capability within the Prevention Mission.

B. EXPECTATIONS

Participating agency boat crews will be expected to adjudicate the alarms using radiation detection equipment while following the San Francisco Maritime PRND Regional Concept of Operations and Standard Operating Procedures.

Fire service and law enforcement personnel will be expected to perform primary screening operations and use the totality of the circumstances, including behaviors, interviews, and the nature and location of the radiation, to assess whether the radiation alarm requires further investigation.

If the alarm cannot be adjudicated at the primary screening level using PRDs and other investigatory techniques, secondary screening assets will be required. If the team has a radioisotope identification device (RIID) and the proper training to utilize the equipment, then the team should further adjudicate the alarm, as outlined in the Maritime PRND Regional Concept of Operations.

If the alarm cannot be adjudicated at the secondary screening level using a RIID, then fire and law enforcement personnel, with the assistance of Level II personnel, embedded on each boat, perform technical reachback. Technical reachback is required for the Vessel Search scenario and optional for the Safety Boarding, Chokepoint, and Area Search (Marina) scenarios, time permitting.

If, at any time, the gamma dose rate and/or neutron count on the PRD or RIID exceeds established thresholds, then law enforcement personnel should follow the USCG SMAC concept (Stop, Move- Away, Alert, and Close-OFF).

If at any time the incident becomes suspicious, law enforcement personnel should contact the Sector San Francisco IOC immediately.

C. SCENARIO SUMMARIES

Each of the four scenarios will follow the same general timeline of 80 minutes per scenario. At the end of each scenario, players will be allowed 20 minutes to transit to the next scene. The Scenario Controller/Evaluator will direct the timing of the scenario start and will communicate with the MCC after they are finished to ensure players are not released until their next scenario is ready to receive them.

1. Scenario 1: Enhanced Steady State - Enhanced Monitoring: Vessel Search and Reachback Scenario

The squadron will work together in this scenario to form one integrated search team that will divide up the responsibilities necessary to the efficient search of a vessel to find the source of radiological alarms and the performance of technical reach back.

The National Terrorism Advisory System has issued a warning to the nation's public transportation systems due to a non-specific terrorist threat. In response to the

warning, the teams will board an occupied vessel transiting unauthorized through an established security zone to perform primary

PRND screening operations. Fire and law enforcement personnel will be expected to adjudicate multiple radiation alarms using radiation detection equipment while following the San Francisco Maritime PRND Regional Concept of Operations and Standard Operating Procedures.

The vessel operator will be non-compliant, causing the level of suspicion to escalate. As a result, the fire and law enforcement personnel will perform secondary screening with the assistance of Level II, if necessary.

The nature of the spectrum collected from the source will require technical reachback. In turn, Level II personnel will perform technical reachback utilizing Laboratory Scientific Services (LSS) or DOE Triage.

2. Scenario 2: Steady-State: Safety Boarding Scenario

The squadron will work together in this scenario to form one integrated search team that will divide up responsibilities in their assigned Area of Responsibility (AOR).

While performing maritime law enforcement operations, a patrol vessel stops a recreational boater to perform a routine boating safety check (one at a time). A passenger on the recreational boat is carrying naturally occurring radioactive material (NORM) in his/her backpack. The source is strong enough to cause a boarding officer's PRD to alarm.

The passenger will be non-compliant, causing the level of suspicion to escalate. As a result, the officers will perform secondary screening with the assistance of Level II, if necessary. The nature of the spectrum collected from the NORM will not require the officers to request technical reachback, and the recreational boater is allowed to continue their transit.

3. Scenario 3: Enhanced Steady State-Enhanced Monitoring: Chokepoint Operation

The squadron will work together in this scenario to form one integrated search team that will divide up the responsibilities necessary in the efficient operation of a PRND chokepoint

The National Terrorism Advisory System has issued a warning to the nation's public transportation systems due to a non-specific terrorist threat. In response to the warning, the teams will form a PRND chokepoint near a possible target of interest.

The target vessel will be directed to pass between two fire/law-enforcement boats. White the target vessel passes by, it will be screened for the presence of radiological/ nuclear materials. Upon receiving a radiation alarm, the target vessel will be boarded and searched for the source of radiation. A passenger on the recreational boat is carrying naturally occurring radioactive material (NORM) in his/her backpack. The source is strong enough to cause a boarding officer's PRD to alarm.

The passenger will be non-compliant, causing the level of suspicion to escalate. As a result, the officers will perform secondary screening with the assistance of Level II, if necessary. The nature of the spectrum collected from the NORM will not require the officers to request technical reachback, and the recreational boater will be allowed to continue their transit.

4. Scenario 4: Enhanced Steady State - Special Event: Area Search (Marina) Scenario

The squadron will work together in this scenario to form one integrated search team that will divide up the responsibilities necessary to perform an efficient PRND area search (Marina)

In preparation for a visit by a foreign dignitary, fire and law enforcement boats will perform PRND primary screening operations at a marina on the San Francisco Bay. Boat crews must plan and execute a search of the marina (one at a time). Each team, while performing primary screening at the marina, receives a PRD alarm that is localized to a dock box at the marina.

Fire and law enforcement personnel will be expected to adjudicate the radiation alarm using radiation detection equipment while following the San Francisco Maritime PRND Regional Concept of Operations and Standard Operating Procedures.

The cause of the alarm in the dock box appears to be from an industrial source (soil density gauge). However, the owner of the dock box is not listed as the licensee in the CDPH-RHB documents found with the source. This will cause the level of suspicion to escalate. As a result, fire and law enforcement personnel will perform secondary screening with the assistance of Level II, if necessary. The nature of the spectrum collected from the industrial source will not require technical reachback, but the source will be seized, and CDPH-RHB called for further instructions.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

AARONIA AG. (n.d.-a). *AARTOS drone detection system.* AARTOS AARONIA Drone Detection. Retrieved June 4, 2020, from https://drone-detection-system.com/

AARONIA AG (n.d.-b). *Anti-drone jammer. A*ARTOS AARONIA Drone Detection. Retrieved February 22, 2021, from https://drone-detection-system.com/sensor-types-overview/anti-drone-jammer/#highlights.

Ang, Z. V. (2020, April 29). *Decision-*

during this COVID-19 pandemic through the lens of the Cynefin Framework. BusinessWorld. https://www.bworldonline.com/decision-making-during-this-covid-19-pandemic-through-the-lens-of-the-cynefin-framework/.

ATAK. (n.d.). *About*. ATAK. Retrieved January 14, 2021, from https://atakmap.com/p_about.aspx

Awh, E., & Vogel, E. (2008). The bouncer in the brain. *Nature Neuroscience*, *11*(1), 5–6. https://doi.org/10.1038/nn0108-5

Balcik, C. (2018, December 13). How mobility solutions are transforming military tactical operations & driving better mission outcomes. *Samsung Business Insights*. https://insights.samsung.com/2018/12/13/how-mobility-solutions-are-transforming-military-tactical-operations-driving-better-mission-outcomes/

Biallawons, O., Klare, J., & Fuhrmann, L. (2018). Improved UAV detection with the MIMO radar MIRA-CLE Ka using range-velocity processing and TDMA correction algorithms. *2018 19th International Radar Symposium (IRS)*, 1–10. https://doi.org/10.23919/IRS.2018.8447914

Boyd, J. (2007, January). *Patterns of conflict.* Project White Horse. http://www.projectwhitehorse.com/pdfs/boyd/patterns%20of%20conflict.pdf

Brown I. T. (2018). *A new concept of war, John Boyd, the U.S. Marines, and maneuver warfare*. Marine Corps University Press.

Center for Strategic & International Studies (2021, May 07*). Project Overmatch: a conversation with RADM Douglas Small, USN* [Video]. YouTube. https://www.youtube.com/watch?v=1bfH5qW2gXw

CivTAK. (2020, April 29). *National Guard rolls TAK for COVID-19*. https://www.civtak.org/2020/04/29/national-guard-rolls-tak-for-covid-19/

CivTAK. (2017, July 24). *ATAK available at NGA app store*. https://www.civtak.org/2017/07/24/atak-available-at-nga-app-store/

Daly, D. (2020, December 8). *A not-so-short history of unmanned aerial vehicles (UAV)*. Consortiq. https://consortiq.com/short-history-unmanned-aerial-vehicles-uavs/

Davis, B. R, & Whittaker, W. G. (2019, December 19). *Integration of situational awareness tools in the fight against unmanned aerial systems* [Master's thesis, Naval Postgraduate School]. NPS Archive: Calhoun. https://calhoun.nps.edu/handle/10945/64130

Defense World.net. (2019, September 10). *Saab's Giraffe 1X Radar installed on Supacat Jackal vehicle debuts at DSEI-2019*. https://www.defenseworld.net/news/25436/Saab_s_Giraffe_1X_Radar_Installed_on_Supacat_Jackal_Vehicle_Debuts_at_DSEI_2019#.YJRhe8CSlPY

Department of Homeland Security Science Technology Division (2019). *Team Awareness Kit (TAK) - enhancing homeland security enterprise collaboration on the mobile edge*. dhs.gov. https://www.dhs.gov/sites/default/files/publications/tactical_awareness_kit_508.pdf

DJI. (2019, August 23). *DJI AeroScope enables remote ID in an unmanned traffic management system*. DJI. https://enterprise.dji.com/news/detail/aeroscope-enables-remote-id-in-utm-system

Da-Jiang Innovations. (2020). *Aeroscope user manual*. https://dl.djicdn.com/downloads/AEROSCOPE/20201014/Aeroscope_AS-F1800_User_Manual_EN_v2.0.pdf

Department of Defense. (2021, January 7). *U.S. Department of Defense counter-small unmanned aircraft systems strategy*. https://media.defense.gov/2021/Jan/07/2002561080/-1/-1/1/DEPARTMENT-OF-DEFENSE-COUNTER-SMALL-UNMANNED-AIRCRAFT-SYSTEMS-STRATEGY.PDF

Dumitrescu, C., Minea, M., Costea, I. M., Cosmin Chiva, I., & Semenescu, A. (2020). Development of an Acoustic System for UAV Detection. *Sensors (Basel, Switzerland)*, 20(17), 4870. https://doi.org/10.3390/s20174870

Egozi, A. (2020, November 25). *ARTsys360 low-weight, affordable C-UAS radar "can also provide urban drone traffic surveillance*." Unmanned Airspace. https://www.unmannedairspace.info/counter-uas-systems-and-policies/artsys360-low-weight-affordable-c-uas-radar-can-also-provide-urban-drone-traffic-surveillance

Endsley, M. (1988). Situation awareness global assessment technique (SAGAT). *Proceedings of the IEEE 1988 National Aerospace and Electronics Conference*, 789–795 vol.3. https://doi.org/10.1109/NAECON.1988.195097

Endsley, M. R. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *37*(1), 32–64. https://doi.org/10.1518/001872095779049543

Endsley, M. (2015). Situation Awareness Misconceptions and Misunderstandings. *Journal of Cognitive Engineering and Decision Making*, *9*(1), 4–32.

Ezuma, M., Erden, F., Anjinappa, C. K., Ozdemir, O., & Guvenc, I. (2019, April 10). *Micro-UAV Detection and Classification from RF Fingerprints Using Machine Learning Techniques*. North Carolina State University. https://arxiv.org/abs/1901.07703.

Federal Aviation Administration. (2020, August). *Advisory on the application of federal laws to the acquisition and use of technology to detect and mitigate unmanned aircraft systems*. (9.95.300-UAS). https://www.faa.gov/uas/resources/C_uas/media/Interagency_Legal_Advisory_on_UAS_Detection_and_Mitigation_Technologies.pdf

Feist, J. (2021, April 27). *Most popular drones, according to you!*. Drone Rush. https://dronerush.com/popular-drone-18182/

Fenn, A. J., Temme, D. H., Delaney, W. P., & Courtney, W. E. (2000). The Development of Phased-Array Radar Technology. *Lincoln Laboratory Journal,* 12(2), 321–340.

Gaitanakis, G., Limnaios, G., & Zikidis, K. (2020). AESA radar and IRST against low observable threats. *Aircraft Engineering and Aerospace Technology*, 92(9), 1421–1428. https://doi.org/10.1108/AEAT-01-2020-0011

Garbade, M. (2018, July 9). A simple machine learning algorithm to differentiate between an apple and an orange. *Education Ecosystem Blog.* https://blog.education-ecosystem.com/a-simple-machine-learning-algorithm-to-differentiate-between-an-apple-and-an-orange.

Gazzaley, A. (2017). *Distracted Mind: ancient brains in a high-tech world*. MIT Press.

HGH-Infrared Systems. (n.d.). *SPYNEL IR camera: a proven solution for drone swarms / small UAVs detection & tracking*. HGH-Infared. Retrieved June 3, 2021, from https://hgh-infrared.com/wp-content/uploads/2020/11/HGH_CaseStudy_Spynel_DroneUAVDetection.pdf

Hindle, P. (2018). Drone detection and counter measures take the world stage. *Microwave Journal* (International Ed.), 61(9), S6–18.

Ingram, P. (2020). Drones buzz $300k in coke, meth over border near Yuma. *Tucson Sentinel.com.* https://www.tucsonsentinel.com/local/report/050420_yuma_drones/drones-buzz-300k-coke-meth-over-border-near-yuma/

Joint Chiefs of Staff. (2019) *Joint air operations* (JP 3-30). https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_30.pdf

Kehoe, A., & Cecotti, M. (2021). Multiple destroyers were swarmed by mysterious 'drones' off California over numerous nights. *The Drive*. https://www.thedrive.com/the-war-zone/39913/multiple-destroyers-were-swarmed-by-mysterious-drones-off-california-over-numerous-nights.

Klare, J., Saalmann, O., & Biallawons, O. (2013). The MIMO radar MIRA-CLE Ka. *2013 Asilomar Conference on Signals, Systems and Computers,* 1418–1422. https://doi.org/10.1109/ACSSC.2013.6810529

Klein, G. (1998). *Sources of power: how people make decisions*. MIT.

Klein, G. (2008). Naturalistic decision making. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *50*, 456–460.

Kristan, M. J., Hamalainen, J. T., Robbins, D. P., & Newell, P. J. (2009, November). *Cursor-on-target message router user's guide*. MITRE. https://www.mitre.org/sites/default/files/pdf/09_4937.pdf

O'Brien, J. (2019, May 7). AFRL technology employed by U.S. Coast Guard to rescue stranded ice fishermen. *Air Force Research Laboratory*. https://afresearchlab.com/news/afrl-technology-employed-by-u-s-coast-guard-to-rescue-stranded-ice-fishermen/

McDougall, W. (2018). *An outline of psychology.* Routledge.

Mentzer, J. R. (1955). Scattering and diffraction of radio waves. Pergamon Press.

Miller, C. (2020, August 05). *DJI Aeroscope review: features, specs, and how it's used in layered drone detection*. 911 Security. https://www.911security.com/blog/dji-aeroscope-review-features-specs-and-how-its-used-in-layered-drone-detection.

Mishra, A. (2018). AESA radar and its application. *2018 International Conference on Communication, Computing and Internet of Things* (IC3IoT), 205–209. https://doi.org/10.1109/IC3IoT.2018.8668101

NASCO (n.d.). *Spynel-U wide area surveillance system*. NASCO.co.jp. Retrieved June 3, 2021, from www.nasco.co.jp/cms/mark/pdf/HGH/Spynel-U.pdf

Paone, C. (2010, September 15). *Cursor on target conference to feature hands-on challenge*. https://www.af.mil/News/Article-Display/Article/115608/cursor-on-target-conference-to-feature-hands-on-challenge/

Phoenix Future Technologies. (n.d.). *DJI portable Aeroscope*. Phoenix Future Technology. Retrieved June 3, 2021, from https://phoenixfuturetech.com/product/dji-portable-aeroscope/

PRND Focus Group. (2021). San Francisco Bay Guardian 2021 controller evaluator handbook. [Handbook].

Raboy, M. (2018). *Marconi: the man who networked the world*. Oxford University Press.

Rahman, S., & Robertson, D. (2018). Radar micro-Doppler signatures of drones and birds at K-band and W-band. *Scientific Reports*, 8(1), 17396–11. https://doi.org/10.1038/s41598-018-35880-9

Rogoway, T., & Trevithick, J. (2020, July 29). The night a mysterious drone swarm descended on Palo Verde Nuclear Power Plant. *The Drive*. https://www.thedrive.com/the-war-zone/34800/the-night-a-drone-swarm-descended-on-palo-verde-nuclear-power-plant.

Rohatgi, M., & Friedman, G. (2010). A Structured approach for assessing & analyzing technical & nontechnical interoperability in socio-technical systems. *2010 IEEE International Systems Conference*, 581–586. https://doi.org/10.1109/SYSTEMS.2010.5482337

SAAB. (2020). *Giraffe 1X: SAAB*. https://www.saab.com/products/giraffe-1x.

Salas, E., Cannon-Bowers, J., & Blickensderfer, E. (1993). Team performance and training research: emerging principles. *Journal of the Washington Academy of Sciences*, 83(2), 81–106. http://www.jstor.org/stable/24531239.

Salmon, P. M., Stanton, N. A., & Young, K. L. (2012). Situation awareness on the road: review, theoretical and methodological issues, and future directions. *Theoretical Issues in Ergonomics Science*, *13*(4), 472–492.

Scharre, P. (2018). *Army of none: autonomous weapons and the future of war* (First edition.). W. W. Norton & Company.

Seffers, G. I. (2020, October 28). Army tactical assault kit always adapting for new era. *SIGNAL Magazine*. https://www.afcea.org/content/army-tactical-assault-kit-always-adapting-new-era.

Skolnik, M. I. (2020, November 18). Radar. In *Encyclopedia Britannica*. https://www.britannica.com/technology/radar/History-of-radar

Snowden, D. (2002). Complex acts of knowing: paradox and descriptive self-awareness. *Journal of Knowledge Management*, *6*(2), 100–111.

Snowden, D. (2005). Strategy in the context of uncertainty. *Handbook of Business Strategy*, *6*(1), 47–54. https://doi.org/10.1108/08944310510556955

Soelberg, P. (1966). Unprogrammed Decision Making. *Academy of Management Proceedings*, *1966*(1), 3–16. https://doi.org/10.5465/ambpp.1966.4980853

Sorensen, L. J., Stanton, N. A., & Banks, A. P. (2011). Back to SA school: contrasting three approaches to situation awareness in the cockpit. *Theoretical Issues in Ergonomics Science*, *12*(6), 510–513.

Suits, D. (2020, October 8). Joint counter-sUAS strategy to address need for improved technology. *Army News Service*. https://www.army.mil/article/239593/joint_counter_suas_strategy_to_address_need_for_improved_technology

Tomkins, R. (2016, May 25). *FLIR Systems launches ground surveillance products*. UPI. https://www.upi.com/Defense-News/2016/05/25/FLIR-Systems-launches-ground-surveillance-products/7871464199487/.

Trading, A. W. (2020, January 30). AirWorks explains how to protect airports from drones with DJI Aeroscope. *CISION PR Newswire*. https://www.prnewswire.com/ae/news-releases/airworks-explains-how-to-protect-airports-from-drones-with-dji-aeroscope-300995435.html

Wiles, K. (2019, May 9). *Hummingbird robot using ai to go soon where drones can't*. Purdue University. https://www.purdue.edu/newsroom/releases/2019/Q2/hummingbird-robot-uses-ai-to-soon-go-where-drones-cant.html

U.S. Army. (n.d.). *C5ISR Center U.S.ARMY CCDC*. Retrieved full date, from https://c5isr.ccdc.army.mil/

USCG, USMC, & USN. (2020). *Advantage at sea: prevailing with integrated all-domain naval power.* https://media.defense.gov/2020/Dec/16/2002553074/-1/-1/0/TRISERVICESTRATEGY.pdf

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California