

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

COUNTER-UNMANNED AERIAL SYSTEMS (C-UAS) INTEROPERABILITY IN THE GLOBAL GEOPOLITICAL ENVIRONMENT

by

Allen N. Golphin III and Boswyck D. Offord II

September 2021

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

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** September 2021	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE COUNTER-UNMANNED AERIAL SYSTEMS (C-UAS) INTEROPERABILITY IN THE GLOBAL GEOPOLITICAL ENVIRONMENT	**5. FUNDING NUMBERS**
6. AUTHOR(S) Allen N. Golphin III and Boswyck D. Offord II	
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)

The U.S. Navy (USN) and U.S. Marine Corps (USMC) are tasked with providing counter-unmanned aerial system (C-UAS) defense for a multitude of mission facets. Using the plethora of C-UAS capabilities available for market purchase, both services have invested in non-complementary C-UAS capabilities. Furthermore, C-UAS coordination and integration is not well-defined in USN or USMC warfare doctrines. This work addresses the current and future C-UAS hardware interoperability and effectiveness needs by distinguishing where and when interoperability is appropriate, identifying operational interferences, and recognizing any duplication of efforts. Areas of responsibility and host nations' operational authority, legal restrictions, and variances in unmanned aerial system (UAS) threats serve as constraints and impose restraints on which C-UAS technologies are optimal for universal employment. We focus on threats from smaller, handheld, commercially available UASs. To meet the demand of joint C-UAS requirements, the USN and USMC must divest from the previous mentality of interim solutions to solve a permanent problem. Long-term, interoperable C-UAS solutions capable of performing at high rates of effectiveness against current and future UAS threats are needed.

14. SUBJECT TERMS C-UAS, UAS, interoperability, unmanned aerial system, counter-unmanned aerial system	**15. NUMBER OF PAGES** 251
	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.

COUNTER-UNMANNED AERIAL SYSTEMS (C-UAS) INTEROPERABILITY IN THE GLOBAL GEOPOLITICAL ENVIRONMENT

Allen N. Golphin
Lieutenant, United States Navy
BS, Georgia State University, 2013
MS, Johns Hopkins University, 2018

Boswyck D. Offord
Lieutenant Commander, United States Navy
BS, Norfolk State University, 2009

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
September 2021

Approved by: Britta Hale
Advisor

Douglas L. Van Bossuyt
Co-Advisor

Gurminder Singh
Chair, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The U.S. Navy (USN) and U.S. Marine Corps (USMC) are tasked with providing counter-unmanned aerial system (C-UAS) defense for a multitude of mission facets. Using the plethora of C-UAS capabilities available for market purchase, both services have invested in non-complementary C-UAS capabilities. Furthermore, C-UAS coordination and integration is not well-defined in USN or USMC warfare doctrines. This work addresses the current and future C-UAS hardware interoperability and effectiveness needs by distinguishing where and when interoperability is appropriate, identifying operational interferences, and recognizing any duplication of efforts. Areas of responsibility and host nations' operational authority, legal restrictions, and variances in unmanned aerial system (UAS) threats serve as constraints and impose restraints on which C-UAS technologies are optimal for universal employment. We focus on threats from smaller, handheld, commercially available UASs. To meet the demand of joint C-UAS requirements, the USN and USMC must divest from the previous mentality of interim solutions to solve a permanent problem. Long-term, interoperable C-UAS solutions capable of performing at high rates of effectiveness against current and future UAS threats are needed.

THIS PAGE INTENTIONALLY LEFT BLANK

Contents

1 Introduction **1**
1.1 Problem Statement 1
1.2 Methodology 3

2 Background **7**
2.1 Unmanned Aerial System Groups 7
2.2 UAS Employment in History 8
2.3 UAS Employment by Non-state Actors 10
2.4 Modern UAS Threat Scenarios 14
2.5 UAS Modes of Operation 17
2.6 UAS Tactics Overview 19
2.7 U.S. CUAS Technology 25
2.8 CUAS Market 28
2.9 CUAS Targeting Cycle 31
2.10 Current CUAS Technological and Legal Limitations 35
2.11 Applications of CUAS Products 40
2.12 Summary 41

3 Adversarial UAS Operators **43**
3.1 Unmanned Aerial System Employment Overview 43
3.2 Hobbyist 44
3.3 Non-state Actors 45
3.4 State Actors 49
3.5 Adversarial UAS Employment Association 52
3.6 Summary 53

4 UAS Technologies **55**
4.1 Unmanned Aerial Systems Architecture Overview 55
4.2 UAS Flight Controller 56

4.3 UAS Ground Control Station 58
4.4 UAS Command and Control 58
4.5 DJI UAS Case Study 71
4.6 Summary 82

5 UAS Threats In Each Area of Responsibility 85
5.1 Adversarial Tactics by Area of Responsibility 85
5.2 Summary 113

6 Current USN and USMC CUAS Technologies 115
6.1 The Counter Unmanned Aerial Systems Kill Chain 115
6.2 Detection and Tracking Techniques 120
6.3 Mitigation Techniques 124
6.4 USN and USMC CUAS Interoperability 126
6.5 Summary 126

7 Modeling and Simulation of the Effectiveness of CUAS Technologies 129
7.1 Counter Unmanned Systems Effectiveness Factors 129
7.2 Model Description, Limitations, Assumptions, and Constraints 129
7.3 Effectiveness Against Current UAS Threats 137
7.4 Effectiveness Against Emerging UAS Threats 147
7.5 Summary 159

8 CUAS Legal Limitations in Each Area of Responsibility 161
8.1 Counter Unmanned Aerial Systems Employment Framework 161
8.2 Overview Of CUAS Legal Implications In The Continent Of The United States 162
8.3 Overview Of CUAS Legal Implications Outside The Continent of the United States 165
8.4 CUAS Legal Implications in each Geographic Area of Responsibility. . . . 169
8.5 CUAS Employment – Legal Framework Way Ahead 183
8.6 Summary 191

9 Conclusion and Future Work 193

9.1 Recommendations 195
9.2 Future Work 196

Bibliography **197**

Initial Distribution List **217**

THIS PAGE INTENTIONALLY LEFT BLANK

List of Figures

Figure 2.1 UAS Autonomy Capability Levels 22

Figure 2.2 Decision Chain of an Autonomous System 22

Figure 2.3 CUAS Targeting Cycle 30

Figure 2.4 DOD Targeting Cycles 30

Figure 2.5 Previous CUAS Employment 41

Figure 3.1 Countries with Group 1-3 UASs 48

Figure 3.2 Non-state Actor UAS Capabilities 49

Figure 3.3 Countries with Armed UAS Programs 51

Figure 4.1 UAS Components 56

Figure 4.2 Example UAS-to-UAS C2 Architecture 68

Figure 4.3 Example UAS Cellular C2 Architecture 69

Figure 4.4 Example UAS SATCOM C2 Architecture 71

Figure 4.5 DJI Phantom 3 NMAP Results 72

Figure 4.6 Serial Bus Data Frame 74

Figure 4.7 DJI Drone Python Setup 79

Figure 4.8 DJI Drone Connection API 80

Figure 4.9 DJI Drone Receive and Transmit Functions 81

Figure 4.10 DJI Drone Waypoint Programming 82

Figure 5.1 Asia's Internet Speeds 106

Figure 7.1 CUAS Reliability Block Diagram 131

Figure 7.2 CUAS Subsystems Reliability 131
Figure 7.3 Detection Subsystem Reliability Histogram (Current) 138
Figure 7.4 Mitigation Subsystem Reliability Histogram (Current) 140
Figure 7.5 CUAS Reliability Histogram (Current) 141
Figure 7.6 CUAS Probability of Detection Histogram (Current) 143
Figure 7.7 CUAS Probability of Mitigation Histogram (Current) 145
Figure 7.8 CUAS Effectiveness Histogram (Current) 146
Figure 7.9 Detection Subsystem Reliability Histogram (Emerging) 148
Figure 7.10 Mitigation Subsystem Reliability Histogram (Emerging) 150
Figure 7.11 CUAS Reliability Histogram (Emerging) 152
Figure 7.12 CUAS Probability of Detection Histogram (Emerging) 154
Figure 7.13 CUAS Probability of Mitigation Histogram (Emerging) 156
Figure 7.14 CUAS Effectiveness Histogram (Emerging) 157

Figure 8.1 U.S. Naval Facilities in CENTCOM AOR 171
Figure 8.2 U.S. Naval Facilities in EUCOM AOR 174
Figure 8.3 U.S. Naval Facilities in PACOM AOR 176
Figure 8.4 U.S. Naval Facilities in NORTHCOM AOR 178
Figure 8.5 U.S. Military Facilities in SOUTHCOM AOR 180
Figure 8.6 Panama Canal 182
Figure 8.7 Multi-national CSG Communication, Radar, NAVAID, EW Military Equipment Commercial Spectrum Use 185
Figure 8.8 Real-time Spectrum Operations 186

List of Tables

Table 2.1 UAS Groups 8

Table 2.2 Non-state Actor Use of Unmanned Aerial Systems 11

Table 2.3 Common Commercial UASs 14

Table 2.4 Modern UAS Employment Options 16

Table 2.5 Comprehensive Roadmap for UAS Autonomy 21

Table 2.6 Group 1-3 Historic UAS Tactics Used 24

Table 2.7 Detection, Tracking, and Classification Sensors 32

Table 2.8 CUAS Interdiction Systems and Means 35

Table 2.9 counter unmanned aerial system (CUAS) Detection, Location, and Classification Limitations 38

Table 3.1 Israeli Heron Group 3 Capabilities 50

Table 6.1 Detection and Tracking Techniques 116

Table 6.2 Mitigation Techniques 117

Table 6.3 Comparison of CUAS Detection Techniques against UAV/GCS . 124

Table 6.4 UAS Automation Level 125

Table 6.5 UAS Collaboration Types 125

Table 7.1 CUASs Assumptions against Current UAS Threats 135

Table 7.2 CUASs Assumptions against Emerging UAS Threats 136

Table 7.3 Detection Subsystem Reliability Summary Stats (Current) 138

Table 7.4 Mitigation Subsystem Reliability Summary Stats (Current) 140

Table 7.5 CUAS Reliability Summary Stats (Current) 142

Table 7.6 CUAS Probability of Detection Summary Stats (Current) 143
Table 7.7 CUAS Probability of Mitigation Summary Stats (Current) 145
Table 7.8 CUAS Effectiveness Summary Stats (Current) 147
Table 7.9 Detection Subsystem Reliability Summary Stats (Emerging) . . . 149
Table 7.10 Mitigation Subsystem Reliability Stats (Emerging) 151
Table 7.11 CUAS Reliability Summary Stats (Emerging) 152
Table 7.12 CUAS Probability of Detection Stats (Emerging) 154
Table 7.13 CUAS Probability of Mitigation Summary Stats (Emerging) . . . 156
Table 7.14 CUAS Effectiveness Summary Stats (Emerging) 158
Table 7.15 Comparison of Model Results 158

List of Acronyms and Abbreviations

2D	two dimensional
3D	three dimensional
AESOP	Afloat Electromagnetic Spectrum Operations
AES	advanced encryption standard
AFCENT	Air Forces Central
AFRICOM	Africa Command
AGL	above ground level
AOA	angle of arrival
AORs	areas of responsibility
AOR	area of responsibility
API	application programming interface
AQAA	al-Qaida and their adherents and affiliates
ARCENT	Army Forces Central
AREPS	Advanced Refractive Effects Predication System
ARG	amphibious readiness group
BLOS	beyond line of site
BPSK	binary phase shift keying
BTS	base transceiver station
BVLOS	beyond visual line of site

C2	command and control
CDL	communication data link
CDMA	code division multiple access
CENTCOM	Central Command
COCOM	combatant command
CONOPS	concept of operations
CONOP	concept of operation
CONUS	continent of the united states
COP	carry-on program
COP	common operational picture
CORIAN	Counter-Remote Control Model Aircraft Integrated Air Defense Network
COTS	commercial off-the-shelf
CROE	combined ROE
CRUDES	cruiser-destroyer
CSG	carrier strike group
CTF	Command Task Force
CTKD	cross-transport key derivation
C-sUAS	counter-small unmanned aerial system
CUAS	counter unmanned aerial system
DEA	Drug Enforcement Agency
DES	digital encryption standard

DEWRAP	Directed Energy Weapon Review and Approval Process
DF	direction finding
DHS	Department of Homeland Security
DJI	Da-Jiang Innovations
DOTMLPF	Doctrine, Organization, Training, Material, Leadership, Personnel, and Facilities
DRIP	Drone Remote Identification Protocol
DSSS	direct sequence spread spectrum
DOD	Department of Defense
DoN	Department of the Navy
DoS	denial of service
EA	electronic attack
EBRISS	Enhanced Battlespace Reconnaissance, Intelligence and Surveillance Software
ECPA	Electronic Communication Privacy Act
EM	electromagnetic
EMI	electromagnetic interference
EMS	electromagnetic spectrum
EMSO	electromagnetic (EM) spectrum operations
EO	electro-optical
EP	electronic protect
ES	electronic support

ESC	electric speed controllers
ESM	electronic support measures
EUCOM	Europe Command
EW	electronic warfare
EXORD	executive order
FAA	Federal Aviation Administration
FAAD C2	Forward Area Air Defense Command and Control
FARC	Fuerzas Armadas Revolucionarias de Colombia
FCC	Federal Communications Commission
FDMA	frequency division multiple access
FDNF	forward deployed naval force
FDOA	frequency difference of arrival
FHSS	frequency hopping spread spectrum
FISA	Foreign Intelligence Surveillance Act
FLAG	Fiber-optic Link Around Globe
FMS	foreign military sales
FOI	frequency of interest
FS-LIDS	Fixed Site-Low, Slow, Small Unmanned Aircraft Integrated Defeat System
FTP	file transfer protocol
FY	fiscal year
G8	Group of Eight

GBAD	Ground Based Air Defense
GCC	Gulf Cooperation Council
GCS	ground control station
GEO	geostationary orbit
GFM	Global Force Management
GNSS	Global Navigation Satellite System
GPS	Great Power Competition
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HADR	humanitarian assistance and disaster relief
HELIOS	High-Energy Laser with Integrated Optical Dazzler and Surveillance
IED	improvised explosive device
IETF	Internet Engineering Task Force
INDOPACOM	Indo-Pacific Command
IQR	interquartile range
IREPS	Integrated Refractive Effects Predictions System
IR	infrared
ISIS	Islamic State in Iraq and Syria
ISR	intelligence, surveillance, and reconnaissance
IoT	internet of things
JA	Judge Advocate
JCO	Joint Counter-small unmanned aerial system Office

kW	kilowatt
L-MADIS	Light-MADIS
LAN	local area network
LEO	low earth orbit
LNA	Libyan National Army
LOB	line of bearing
LOS	line of site
LTE	Long Term Evolution
LWIR	long wavelength infrared
LaWS	laser weapon system
MARCENT	Marine Forces Central
MADIS	Marine Air Defense Integrated System
MARFORCOM	Marine Corps Forces Command
MEB	Marine Expeditionary Brigade
MEF	Marine Expeditionary Force
MEO	medium earth orbit
MEU	Marine Expeditionary Unit
MGRS	military grid reference system
MIMO	multiple input multiple output
MITM	man-in-the-middle
MNF	multinational force
MTBF	mean time between failures

MWIR	medium wavelength infrared
NAVCENT	Naval Forces Central
NATO	North Atlantic Treaty Organization
NDAA	National Defense Authorization Act
NECC	Navy Expeditionary Combat Command
NEO	noncombatant evacuation operations
NIC	National Intelligence Council
NINJA	Negation of Improvised Non-State Joint Aerial-Threats
NMAP	network mapper
NORTHCOM	Northern Command
NPS	Naval Postgraduate School
NSA	National Security Agency
OCONUS	outside the continent of the united states
ODIN	Optical Dazzling Interdictor, Navy
OFDM	orthogonal frequency division multiplexing
OFM	Own Force Monitoring
OFRP	optimized fleet readiness plan
OIR	Operation INHERENT RESOLVE
OPNAV	Office of the Chief of Naval Operations
OPTASK	operational tasking
OUSD	Office Under the Secretary of Defense
PACOM	Pacific Command

PDB	power distribution board
PLAN	People's Liberation Army Navy
QPSK	quadrature phase shift keying
QRC	quick reaction capabilities
QRF	quick reaction force
RBD	reliability block diagram
RC4	Rivest Cipher 4
RF	radio frequency
RFID	radio frequency identification
RID	remote identification
ROE	rules of engagement
RSSI	received signal strength indicator
RTSO	Real-Time Spectrum Operations
SATCOM	satellite communications
SecDef	Secretary of Defense
SDN	software defined network
SEA	simultaneous authentication of equals
SHAPE	Supreme Headquarters Allied Powers Europe
SHF	super high frequency
SMG	Shia Militia Groups
SOP	standard operating procedure
SOUTHCOM	Southern Command

SPMAGTF	Special Purpose Marine Air Ground Task Force
SROE	supplemental rules of engagement
SRUF	supplemental rules for the use of force
SWIR	short wavelength infrared
THAAD	Terminal High Altitude Area Defense
TDMA	time division multiple access
TDOA	time difference of arrival
TKIP	temporal key integrity protocol
TLS	transport layer security
TTPs	tactics, techniques, and procedures
UAS	unmanned aerial system
UAV	unmanned aerial vehicle
UHF	ultra-high frequency
UMTS	Universal Mobile Telecommunications System
USFF	U.S. Fleet Forces Command
USMC	United States Marine Corps
USN	United States Navy
VEO	violent extremist organization
VLOS	visual line of site
VPN	virtual private network
WEP	wired equivalent privacy
WMD	weapon of mass destruction

WPA	WiFi protected access
WPA2	WiFi protected access 2
WPA3	WiFi protected access 3

Executive Summary

The threat imposed by commercially available, modifiable unmanned aerial systems (UASs) can no longer be viewed as a temporary problem set. To adequately address current and emergent UAS threats, the United States Navy (USN) and United States Marine Corps (USMC) must graduate from a mentality of quick fixes, workarounds, and on-the-job training and matriculate to a level of sustained, interoperable, and mature counter unmanned aerial system (CUAS) capabilities to identify, detect, classify, track, and neutralize the UAS problem set. Currently, the Department of Defense (DOD) and its subsidiaries leverage and operate from a plethora of over 235 CUAS capabilities that serve as quick reaction capabilities (QRC) and common operational pictures (COPs) as delineated in this research and the current CUAS market [1]. As denoted by the Joint Counter-small unmanned aerial system Office (JCO), these capabilities are not capable of generating, maintaining, and populating a shared COP for the tactical and operational warfighter, or senior decision maker to adequately address the growing UAS problem set [2].

Our area of research is in support of Marine Corps Forces Command (MARFORCOM) and Navy Expeditionary Combat Command (NECC). It was founded to evaluate current CUASs employed by the USN and USMC for their effectiveness and ability to interoperate amongst themselves in light of the joint CUAS requirements created by the JCO in 2020. In 2019, the DOD issued DOD Directive 3800.01E, placing the U.S. Army as the executive agent for countering Groups 1 through 3 UAS threats domestically and abroad [3]. To meet the growing presence and concerns imposed by Groups 1 through 3 UASs operating over or in the vicinity of friendly forces and installations, both domestically and abroad, the JCO, under direction of the Army, selected Forward Area Air Defense Command and Control (FAAD C2) as the proprietary means of providing a shared COP for managing, disseminating, and collaborating on information regarding UAS threats. Furthermore, the JCO identified eight counter-small unmanned aerial system (C-sUAS) solutions categorized into three systems-of-systems approaches and one command and control (C2) system:

1. Fixed/Semi-Fixed Systems
    - Fixed Site-Low, Slow, Small Unmanned Aircraft Integrated Defeat System (FS-LIDS): sponsored by [U.S.] Army.

    - Negation of Improvised Non-State Joint Aerial-Threats (NINJA): sponsored by [U.S.] Air Force.
    - Counter-Remote Control Model Aircraft Integrated Air Defense Network (CORIAN): sponsored by [U.S.] Navy.
2. Mounted/Mobile System
    - Light-MADIS (L-MADIS): sponsored by [U.S.] Marine Corps.
3. Dismounted/Handheld Systems
    - Bal Chatri: sponsored by Special Operations Command.
    - Dronebuster: no sponsor [but] commercial off-the-shelf capability.
    - Smart Shooter: no sponsor [but] commercial off-the-shelf capability.
4. Command and Control
    - FAAD C2: sponsored by [U.S.] Army.
        - FAAD C2 [includes] interoperable systems like the Air Force's Air Defense System Integrator (ADSI) and the Marine Corps' Multi-Environmental Domain Unmanned Systems Application Command and Control (MEDUSA C2) [3].

To understand how to evaluate the effectiveness of the current CUAS capabilities against current and emergent threats imposed by Groups 1 through 3 UASs, our research takes the unique approach by evaluating the UAS threat from a maritime and ground perspective. Understanding the adversary and their associated offensive capabilities and limitations allows for the best assertion of what defensive capabilities and level of force is required to protect, defend, and conduct counter offensive where applicable.

Our research uniquely defines and categorizes the threat actors and their associated means of UAS application through the lens of a military tactician. We define the threat actors who operate Groups 1 through 3 UASs with the National Intelligence Council (NIC) definition of hobbyist, state, and non-state actors. This definition is applied to the historical context of adversarial UAS applications in every area of responsibility (AOR) and the extent of damage yielded to human life and infrastructure. This context of understanding who operates Groups 1 through 3 UASs and how they have wielded UASs as a tool to thwart DOD strategy and policy is then translated into what means of C2 are leveraged in every AOR to support adversarial UAS flight and payload operations. Knowledge of the means of C2 accessible in an AOR is leveraged to support the assessment of what adversaries are able to conduct

currently with commercial off-the-shelf (COTS) UASs, as well as what adversaries will be able to execute with emergent technology, infrastructure, and innovation.

After evaluating how adversaries are able to employ Groups 1 through 3 UASs in the varying AORs, our research investigates the current CUAS capabilities recommended by the JCO and employed by the USN and USMC to support countering UASs. Thereafter, further research is conducted to evaluate the degree of effectiveness associated with specific CUAS capabilities leveraged to support identifying and neutralizing varying numbers of UAS threats. We implement and leverage unbiased simulations to demonstrate the rate of effectiveness and the level of interoperability with other subsidiary CUAS subsystems needed to support the CUAS kill chain. This unique, unbiased approach is intended to inform senior decision makers of the actual effectiveness of current CUAS capabilities employed in the Fleet, versus the commercially advertised effectiveness.

Our research concludes on the discernment of legal limitations imposed upon existing and emergent CUAS capabilities needed to support the CUAS kill chain against UAS threats. Our unique application of radio frequency (RF) deconfliction methods, procedures, and capabilities further delivers the potential for understanding the extent of CUAS capabilities' active emission applications in an AOR. Further, we delineate Advanced Refractive Effects Predication System (AREPS), Real-Time Spectrum Operations (RTSO), Own Force Monitoring (OFM), and Builder as predictive analysis tools capable of supporting RF deconfliction and approval to operate existing and emergent CUAS capabilities, as well as determine how effective CUAS capabilities will be if applied to a specific area, weather, or terrain.

Conclusion

The operational environment is saturated with both UAS and CUAS products with increased use by adversarial operators. There remains an emergent need to establish requirements for the USN and USMC to conduct joint, interoperable CUAS operations against Groups 1 through 3 UAS threat. We observe the effectiveness of current USN and USMC CUAS capabilities could worsen as more UASs are operated in AORs with advance technology. To meet the demand of joint CUAS requirements, the USN and USMC must divest from the previous mentality of interim solutions to a permanent problem. Long-term, interoperable CUAS solutions that are capable of performing the high rates of effectiveness against today's and future UAS threats are needed.

Recommendations

The following list encapsulates suggested recommendations to improve CUAS interoperability and effectiveness in the geopolitical environment:

- Establish a common baseline architecture to be used as the foundation for the Department of the Navy (DoN) CUAS *supported by*:
  - Configuration management for evolving software
  - Change management for requirements or mission shifts
- Integrate spectrum analysis tools such as AREPS, RTSO, or Builder into existing and future CUASs capabilities and CUAS planning to improve radar and RF detection, tracking, and neutralization techniques.
  - Leverage spectrum analysis tools to compute and display passive RF probability of detection in varying weather and terrain environments.
  - Leverage spectrum analysis tools to support the prediction of fratricide, minimization of electromagnetic interference (EMI), and legal deconfliction for host nation employment.
- Acquire and implement CUAS capabilities to provide:
  - high probability of detection at extended ranges
  - interoperability with the JCO mandated FAAD C2 architecture
  - high probability of detection for increased numbers of simultaneous UAS targets, such as clusters and swarms
- Conduct site surveys and blue force laydown to support accurate sensor placement to account for multi-domain threat axis, geometry for the terrain, and friendly force emissions.

The threat UASs pose today are here to stay and will likely get worse in the near future. If the suggested recommendations are implemented, they should help to protect DOD interests against current and emerging UAS threats.

Bibliography

[1] A. Michel. *Counter-Drone Systems*. Center for the Study of Drone at Bard College, Annadale-on-Hudson, NY, USA, 2018 [Online]. Available:

https://dronecenter.bard.edu/files/2018/02/CSD-Counter-Drone-Systems-Report.pdf

[2] M. Jamison, "C-suas industry open house," presented at DOD C-sUAS Industry Open House, Arlington, VA, USA, Oct. 30 2020 [Online]. Available: https://govtribe.com/file/government-file/c-suas-industry-open-house-presentation-dot-pdf

[3] N. Strout, "Army selects eight counter-drone systems for the joint force," Defense News, June 26, 2020 [Online]. Available: https://www.defensenews.com/unmanned/2020/06/26/army-selects-eight-counter-drone-systems-for-the-joint-force/

THIS PAGE INTENTIONALLY LEFT BLANK

Acknowledgments

Allen N. Golphin III: First, and foremost I would like to sincerely thank my wife, Brandy. Without her tireless love, support, and patience, the completion of this process would have not been possible. I would also like to thank my children (Nylah, Tre, AJ, and Rylee) because when the hardship of this journey was upon me, they provided a breath of fresh air, the laughter, and love that was needed to pick me up! To my advisors, Dr. Hale and Dr. Van Bossuyt, thank you for the guidance, insight, and maintaining the right standard throughout this journey. To Bos, thank you for providing balance, a calm perspective, and optimistic outlook along with sound critical thinking. This process has been a journey that I will always remember for learning experience and contributions the Navy!

Boswyck Offord II: To my family, I extend a heartfelt thank you for your time, understanding, flexibility, and support during my matriculation through graduate school. The journey was wrought with hardships as attributed to my learning curve for the computer science curriculum and the COVID-19 pandemic. However, your unwavering aid during my periods of isolation associated with school and the pandemic was intangible to my growth and maturation professionally, personally, and morally. To my professors, thank you for maintaining a high bar for our quality of work. To my thesis partner, thank you and your family for your time and sound reasoning, judgement, and immense characters. This process and product is more rewarding because we completed it together—One Team, One Fight.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 1:
Introduction

1.1 Problem Statement

counter unmanned aerial system (CUAS) technology is the reference of an ability to detect, classify, and intercept unmanned aerial systems (UASs) of a suspicious nature. The emergence in this area of research and development was founded to meet the growing presence and concerns of malicious UASs operating in or in the vicinity of United States Navy (USN) and United States Marine Corps (USMC) friendly forces and installations. This research evaluates the currently used CUAS capabilities leveraged by the USN and USMC for their effectiveness in supporting the CUAS kill chain, as well as their ability to interoperate with other means of CUAS deployed within and between the services and the Department of Defense (DOD). Furthermore, this research investigates the level of interoperability and support the current CUAS capabilities provide to meet the requirements established by the Joint Counter-small unmanned aerial system Office (JCO) in 2020.

The JCO was created in 2019 to support the CUAS interoperability needs by the joint force against Groups 1 through 3 UASs in the DOD [1]. The JCO identified the DOD lacked the requisite command and control (C2) architecture, doctrine, and commonality to adequately address combating UAS threats domestically and abroad. To support identifying a common C2 architecture for the DOD to adhere to, the JCO placed the U.S. Army as the executive agent for all DOD Group 1 through 3 CUAS matters in DOD Directive 3800.01E [2].

UASs are considered threats if they present the imminent potential to conduct hazardous, malevolent, or undesirable acts against equities deemed essential or protected. These threats must be handled with systems containing the appropriate de-escalatory techniques suitable for the operational environment they are employed in. CUAS research has been an area of interest for the U.S. and its allies for over a decade, commencing with a North Atlantic Treaty Organization (NATO) led study in 2003 during the Global War on Terrorism in the Middle East. Prior to the proliferation of small, portable, radio frequency (RF) enabled UAS products, CUAS research focused on low, slow, and small aerial targets known as Low Slow

Flyers in an area of armed conflict. The area of research has matriculated at a reactive rate, proportional to the proliferation of UAS technology and affordability in the commercial markets.

In 2008, the RAND Corporation published their first report on threats instigated by UAS to the United States' strategic equities, thus defining the operational need for CUAS [3]. In the following years, CUAS products have flourish throughout the commercial sector led by several laboratories, organizations, private firms, and contractors. In 2018, there were over 235 CUAS products produced by 155 manufacturers in 33 countries [4]. With the plethora of CUAS capabilities available for use, the U.S. Department of the Navy (DoN) must consider which type of CUAS product is best for wide acquisition and application against emergent threats across our designated areas of responsibility (AORs) during active and non-active conflicts. The USN and USMC are tasked with providing global CUAS defense for a multitude of mission facets to include fixed installations, forward operating bases, maritime assets, and mobile ground elements. Using the plethora of CUAS capabilities available for market purchase, both branches of the DoN have invested in non-complementary CUAS capabilities to provide protection and reassurance. Further, CUAS coordination and integration is not well defined in USN or USMC amphibious and expeditionary warfare doctrine. This work addresses the future hardware and interoperability development needs for USN and USMC CUAS kill chains by distinguishing where and when interoperability is appropriate, identifying operational interferences, and any duplication of efforts. This includes consideration of which CUAS capabilities serve best for wide acquisition and application against emergent threats across our designated AORs during active and non-active conflicts.

AORs and associated host nations' operational authority, legal restrictions, and variances of UAS threats serve as a constraint and restrain to which CUAS technology is optimal for universal employment. We focus on threats imposed by smaller, handheld, commercial UASs to the civilian and military environments. This work informs and supports future requirements and concepts of operations for DoN CUAS kill chains to improve interoperability for USN and USMC CUAS operations. The DoN must ascertain which CUAS capabilities meet the desired threshold for detection, classification, and neutralization. Furthermore, host nations' authority, legal restrictions, and variances of UAS threats serve as a constraint to which CUAS technology is optimal for universal employment. Here, we shall

focus on the threats imposed by smaller, handheld, commercial UASs to the civilian and military environments. This research is intended to provide a comprehensive analysis of current UAS threats and legal restrictions to CUAS applications in all AORs to determine the most ideal CUAS technology for procurement and operationalization.

1.2 Methodology

There exists an overabundance of CUAS products containing a variety of technologies to identify, locate, track, and neutralize nefarious UASs in the civilian and military operational environments. Further, CUAS is befall with limitations just as any emerging technology. The ambiguity of deciding upon a best means of CUAS capability to address a UAS problem set is compounded by the lack of DoN policy for acquiring interoperable technologies. As product availability proliferates throughout the commercial and contracted business sectors, product performance will be varied. Thus, the level of variance between expected CUAS performance against a threat may be skewed. This challenge is exacerbated as the growth in the UAS industry continues to yield improved technology and cheaper hardware. The forward momentum of the UAS market inevitably plagues the CUAS market as a reactive means of addressing the problem. As the market continues to expand, CUAS technology will require more flexibility in capabilities.

Critical and efficient interactions between CUASs depends on an interoperable technological foundation defined by common architecture, modularity and parts interchangeability, data transport integration, and standardized C2. To accurately assess the operational advantages and disadvantages for CUAS employment, an analysis of the predominant UAS threats in each area of responsibility (AOR) and the disparity of inherent legal and operational restrictions in each AOR must be understood. Additionally, an analysis of currently fielded CUASs and their intended locations of employment is required to assess where interoperability is appropriate. To adequately defeat emergent UAS threats with the appropriate CUAS technology, we must understand how the adversary employs UASs in each AOR. The following methodology is implemented in the following chapters of this research:

1. Review and analyze historical and current UAS and CUAS tactics, techniques, and procedures (TTPs), technology, and systems in use or development by the USN and USMC to establish the levels of interoperability, interference, duplication, and

limitations that exist.

- We assess the implication of historic UAS TTPs against current CUAS TTPs.
- We leverage U.S. Marine Corps Forces Command (MARFORCOM), Navy Expeditionary Combat Command (NECC), Office of the Chief of Naval Operations (OPNAV) N2/N6, and DOD and civilian agencies for information on current CUAS technologies and systems in use or development.

2. Review and analyze USN and USMC mission sizes, geographic location conditions, and communication environments for differences and similarities with respect to AOR.
    - The study of UAS C2 links, nodes and architecture support arguments for proposals to leverage complementary CUAS technology against current and emergent UAS threats.
    - We leverage factual information from USN and USMC service command elements in each geographic combatant command (COCOM) on CUAS standard operating procedures, authorities, force employment, and best practices.
3. Review and analyze hobbyists', non-state actors', and state-actors' UAS TTPs em-ployed with respect to the operational and informational environment in each AOR.
    - UAS operations are inherently connected to the technological constraints of the geographic area and actors that employ them. Therefore, trend analysis ensued to determine what UAS technological aspirations are and will become operationalized to enable future UAS engagements.
    - To achieve the desired tactics, research is conducted to determine the technological means employed by UASs in combative and non-combative environments to support current and future CUAS TTPs.
    - Information obtained from USN and USMC service command elements in each geographic COCOM obtained to support our analysis on adversaries' UAS employment history, trends, and capabilities.
4. Identify host nation and geographic operational and legal restraints to CUAS technological application.
    - Research ensued to identify operational and legal restraints CUAS technological application, as it pertains to each AOR and associated host nations.
        - Our forward deployed forces operate on a leased capacity of U.S. soil in foreign countries. Therefore, host nations hold jurisdiction over operational

planning and subsequent endeavors that impact rules of engagement.

- Supporting information for host nation and each AOR's operational and legal restriction to the employment of CUAS capabilities gathered and evaluated.

5. Develop future-looking concept of operations (CONOPS) for different sizes and locations of CUAS missions.
6. Identify employment gaps in existing and projected CUAS kill chains from an operational perspective and an interoperability perspective.
7. Develop models and simulations of expected CUAS hardware behavior to identify shortfalls and successes within the CUAS kill chain, as related to deficiencies with hardware or interoperability.

The aforementioned methodology is used in the subsequent chapters of this thesis to assess the optimization of CUAS capacities within the legal bounds of an AOR by conducting comparative analysis of the UAS threat and the decided upon CUAS countermeasure. After identifying the most suitable means of CUAS capabilities for an AOR, we contrast the capabilities' operational means against the legal bounds of the host nation and AOR. The CUAS capability must possess the inherent flexibility and pedigree to meet the required legal restrictions of an AOR during combative and non-combative rules of engagement. The study of the aforementioned UAS and CUAS tactics, technological applications, and employment restraints underpin the necessity of identifying a CUAS capability capable of adaptation to meet the interoperability needs of the USN and USMC.

This thesis concludes with recommendations proposed to the USN and USMC to support the acquirement and operationalization of effective and interoperable CUAS capabilities to support the current and emergent threats posed by adversaries and their employment of UASs.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 2:
Background

This chapter provides the requisite background information and context of the UAS problem set, which is later elaborated upon in the following chapters in greater detail. Here, we inform the reader of the historical application of small, commercially available UASs in the global geopolitical environment and their relevance to this area of research. It further associates the historical application of UASs to their present day use. We define and identify the legacy UAS TTPs and varying modes of C2 used to support UAS flight and payload operations leveraged by various hobbyist, non-state, and state actors. We define the CUAS targeting cycle and its relevance in detecting, tracking, and mitigating current and emergent UAS threats in the operational environment. We lastly discuss the legal constraints associated with potential emergent CUAS capabilities in the global operational environment.

2.1 Unmanned Aerial System Groups

The development and perceived growth of CUAS technology is related and attributed to the growth and militaristic use of UASs in the civilian and military environments. The inception and use of UASs for militaristic means have been present throughout modern warfare for centuries. The DOD defined UAS groups in 2009 based upon their weight, above ground level (AGL), and speed as shown in Figure 2.1.

Table 2.1. UAS Groups. Source: [5].

Joint UAS Groups

UAS Category	Weight	Altitude	Speed
Group 1	Less than 20 pounds	Less than 1,200 feet AGL	Less than 100 knots
Group 2	21-55 pounds	Less than 3,500 feet AGL	Less than 250 knots
Group 3	Less than 1320 pounds	Less than 18,000 feet AGL	Less than 250 knots
Group 4	Over 1320 pounds	Less than 18,000 feet AGL	Any speed
Group 5	Over 1320 pounds	Over 18,000 feet AGL	Any speed

FY2009–2034 Unmanned Systems Integrated Roadmap, Department of Defense, 2009.

UASs and their employment have become ubiquitous in military, civilian, and recreational environments. This ubiquity is attributed to technological advancements in micro electrical-mechanical systems-based precision sensors used to control the pattern of movement, speed, and stability for UASs. The depreciation in cost and mass manufacturing of these attributes have aided in the inclusion of UASs into modern life.

2.2 UAS Employment in History

The first recorded military employment of a UAS was during the Italian War of Independence in 1849, with the use of unmanned balloons loaded with explosives [6]. The evolution of technology and employment of UASs in warfare would continue to improve and serve as a low cost, low risk, high reward means of conducting tactical operations to achieve strategic advantages.

2.2.1 U.S. Military Investment In UASs

The U.S. commenced research and development of UASs in 1916, during the First World War. C2 failures of RF remote controlled UASs ensued, resulting in a digression of UAS aspirations to rudimentary anti-aircraft targeting practice. During World War II, approximately 15000 UASs were manufactured in southern California for this sole purpose [7].

However, the ultimate intent remained as a means to deliver pilotless aircraft capable of conducting intelligence, surveillance, and reconnaissance (ISR), and launching kinetic combat operations. In 1918, the result yielded the U.S. Army's Kettering Bug, which was capable of diving deep into well-defended adversarial territory to deliver kinetic payloads [8]. Subsequently, Germany leveraged this ideology and capability during World War II to develop their own UAS as a variant of their V-1 flying bombs. These unmanned vehicles were leveraged in the first-ever use of a terrorist related UAS campaign, flying haphazardly and indiscriminately targeting civilian and military targets alike [9].

Following the employment of the Kettering Bug, in 1932 the USN commenced development of radio-controlled aircraft under its Curtiss N2C-2 UAS program [10]. Thereafter, mass production of UASs commenced in support of World War II. This mass production is widely attributed to Reginald Denny and his Radioplane OQ-2, which served as the first remote-controlled aircraft produced for the U.S. military [10]. The U.S. DOD would continue to invest, acquire, and field UASs for decades to come until the maturation of the National Defense Authorization Act (NDAA) necessitated an official requirement and budgetary expenditures for the employment of UASs. Section 220 of the NDAA, FY2001 established the following long-term goals of UAS employment:

- Goal – It shall be a goal of the Armed Forces to achieve the fielding of unmanned, remotely controlled technology such that:
  - by 2010, one-third of aircraft in the operational deep strike force aircraft fleet are unmanned; and,
  - by 2015, one-third of the operational ground combat vehicles are unmanned. [9]

2.2.2 U.S. Military UAS Influence On Adversaries

This research delineated the U.S. military becoming more vested and reliant on UAS technology to support, enable, and lead several warfighter capabilities and efforts to achieve desired tactical advantages. However, the display of U.S. UAS technology and superiority has also provided a pedigree of test beds to enable and train state and non-state actors, allied and adversarial alike. The broad procurement and operationalization of commercially available UASs has provided a means for converting the most rudimentary of air forces

and air defense systems to rival that of recognized superpowers such as the United States, China, and Russia. Subsequent maturation and increased sophistication in RF, cellular, Wi-Fi, satellite, and Bluetooth communications has provided for improvements in the UAS employment model [11]. As such, UASs are now more reliable, protected, and can travel farther as discussed in Chapter 4. What once was perceived as benign and germane to the technological era which incepted it, has become a more menacing problem to defeat.

2.3 UAS Employment by Non-state Actors

UASs have played a relevant role throughout modern history, leading to present day threats represented by state and non-state adversarial actors. The use of UASs by non-state recognized actors can be dated back to 1994 by Japanese cult-like followers known as Aum Shinrikyo [12]. This group successfully employed remote controlled helicopters with aerial dispensatory systems to release Sarin nerve agents on the Matsumoto courthouse and Tokyo Subway systems. Subsequent terrorists plots ensued, including:

1. July 2001, al-Qaida attempted attack using Group 1 UASs equipped with improvised explosive device (IED) against Group of Eight (G8) Summit leaders [13].
2. February 2002, al-Qaida attempted attack using Group 1 UASs equipped with anthrax payloads against the English House of Commons [14].
3. June 2002, al-Qaida conceptual plot to use Group1 UASs equipped with IEDs against civilian airliners [13].
4. August 2002, Fuerzas Armadas Revolucionarias de Colombia (FARC) plot to use Group 1 UASs to carry out IED strikes against Colombian Army and civilian equities [15].
5. December 2003, Hizbollah, Al-Aqsa Martyrs' Brigades, and Fatah form a joint plot to use UASs equipped with IEDs to attack perceived Jewish trespassers in the Gaza Strip [16].

The aforementioned cases were all plots that were either foiled due to law enforcement or military intervention. However, there are several instances of initial and grand scale successes with UASs that garnered international attention and necessitated the need for products to counter the use of UASs. Examples of these instances are captured in Table 2.2.

Table 2.2. Non-state Actor Use of UASs. Adapted: [17]

Date	Location	Entity	UAS Type(s)	Purpose	Result(s)
7 November 2004	Nahariya, Northern Israel	Hezbollah	Iranian Mirsad-1 Drone	20-Minute Reconnaissance Mission	Either a) Crashed in the Sea Near Lebanese Shore or b) Returned back to Hezbollah Base
11 April 2005	Acre, Northern Israel	Hezbollah	Iranian Mirsad-1 Drone	Overflight of Israeli Communities (Started as a Protest of Lebanese Airspace Violations)	Successful Operation; Returned Back to Hezbollah Base
13 September 2005	North Waziristan, Pakistan	al-Qaida	Chinese Made Remote Control Model Airplane	To Recon Pakistani Security Forces prior to attack; also weaponized (IED)	Seized in major raid of al-Qaida hideout by the Pakistani Army
14 September 2005	Fair Fax County, Virginia	Ala Asad Chandia (Abu Qatada); Lashkar-e-Taiba Trained	Obtained MP 1000SYS-Electronic Automatic Pilot System for Model Aircraft in April 2002	For Lashkar-e-Taiba terrorist group drone use in Pakistan	Indicted and subsequently convicted
13 August 2006	Near Tyre, Lebanon; Near Haifa, Israel; Western Galilee, Israel	Hezbollah	3 Ababil drones, each with 40-50 kilogram warhead	Against "Strategic Targets"	All 3 shot down by Israeli F-16s
2006-2007	Columbus, Ohio	Christopher Paul (al-Qaida trained)	5-foot-long model helicopter	Conducted drone research from terrorism purposes	Arrested by FBI and convicted (Plea in 2008)
28 September 2011	Ashland, Massachusetts	Rezwan Ferdaus (al-Qaida Affinity)	Scale models F-86 Sabre and F-14 Phantom jets (GPS capability)	IED (C-4 explosive) attack on Pentagon and Capitol buildings	Arrested by FBI and convicted (Plea in 2012); Sting operation

Continued on next page

– Table 2.2 – continued from previous page

Date	Location	Entity	UAS Type(s)	Purpose	Result(s)
19 May 2012	Helmand Province, Afghanistan	Taliban	Might be recovered NATO UAS (Desert Hawk drone)	Unknown use - possible recon. Found with IED materials and small arms	Captured in raid
6 October 2012	Dimona, Israel	Hezbollah	Iranian Ayoub drone	Recon of Israeli nuclear weapons complex & military exercise preparation	Shot down by Israeli F-16 jet
22 April 2013	Over the sea, 10 kilometers West of Haifa, Israel	Hezbollah	Unmanned drone; type not specified	Mission unknown	Shot down by Israeli F-16 jet at an altitude of 6,000 feet.
Oct 2013	West Bank, Palestine	Hamas	Plot centered at Hebron University to place explosives on UAV	Fly into Israel to engage unknown target(s)	Palestinian Authority arrested plotters prior to launch
14 July 2014	Ashdod, Israel	Hamas	5-foot-long homemade drone aircraft with small rockets (Unconfirmed Hamas video image)	Fly into Israel to engage unknown target(s)	Shot down by Israeli Patriot missile
23 August 2014	Near Raqqa Province, Northern Syria	Islamic State (IS)	DJI Phantom FC40 Quadcopter	Recon of Syrian Army Military Base 93 prior to ground assault	Successful operation [Imagery provided via IS propaganda video on YouTube]
30 August 2014	Falluja, Iraq	Islamic State (IS)	Unspecified drone	Propaganda purposes; Video of attacks in the city	Successful operation [Video of attacks in the city released]
12 September 2014	Kobani, Northern Syria	Islamic State (IS)	Unspecified drone	Propaganda purposes; Video footage of suicide and ground attacks	Successful operation [Video footage of suicide attacks released online]

Continued on next page

– Table 2.2 – continued from previous page

Date	Location	Entity	UAS Type(s)	Purpose	Result(s)
21 September 2014	Near Arsal, Northeastern Lebanon	Hezbollah	Armed drones	Killed 23 al-Nusra Front (al-Qaida linked) fighters at base; followed by ground assault [Operational Preparation of the Environment]	Successful operation [Killed 23 al-Nusra Front (al-Qaida linked) fighters at base]
Approx. 16 Mar 2014	Near Fallujah, Iraq	Islamic State in Iraq and Syria (ISIS)	Unspecified drone	Unknown; possible reconnaissance or propaganda purposes	Operator and drone destroyed in car by U.S. Coalition air strike

2.3.1 Common Commercial UASs Employed By Non-State Actors

We assess the affordability and ease of use for UAS products increases their appeal for civilian and military use. At present day, it is estimated that a few million small UASs exist in the operational environment. From the varying types of UAS products currently employed, Sandia Laboratories articulates that seven play a major role in the open market based on price, payload, range, and flight time. Table 2.3 annotates the UASs based on order of proliferation by consumers. Of note, this list is from 2017 and is subject to change as UAS technology evolves and becomes more accessible to the commercial industry.

Table 2.3. Common Commercial UASs. Source: [18].

Name	Note	Payload Capacity	Range (control)	Flight Time	Speed	Est. Price
DJI Phantom 4 	Extremely popular, many versions available	Manufacturer installed 4K video camera	4.3 mi	3 min	45 mph	$1,500
Tarantula x6 	Inexpensive beginner drone	Manufacturer installed 2MP camera	100 m	10 min	N/A	$55
Freefly Alta 8 	Professional grade cine-matography drone, GPS capable	20lb (Multi-adjustable load platform)	Varies based upon choice of controller	35min; approx. 10 min w/20lb load	35 mph	$17,000
Teal Drone 	First-Person View (FPV) racing drone	FPV camera only	Approx. 1 mi	20 min	85 mph	$1,300
DJI Mavic 	Foldable to 3.5" x 3.5" x 8"	Manufacturer installed 4K video camera	4.3 mi	30 min	40 mph	$1,000
DJI Agras 	Professional quality agriculture crop spraying	10 liters of liquid; approx. 22 lbs	0.6 mi	24 min; approx. 10 min w/full tank load	50 mph	$12,000
Fastest RC Model Aircraft 	Only included to show speed and stealth capabilities	N/A	N/A	N/A	440 mph	N/A

Even if attacks involving UASs are unsuccessful, there still exists an excessive threat to life and operations on the ground. During Operation INHERENT RESOLVE (OIR), U.S. Army Special Forces spokesman LTC Joe Salinas stated the U.S. had no control of the airspace below 3,500 feet in Syria and Iraq due to the prevalence of unauthorized UASs in the operating environment [19].

2.4 Modern UAS Threat Scenarios

The use of UASs lowers the risk of human life in the pursuit of conducting ISR and kinetic missions for the purposes of air superiority and dominance. UASs also enable near-peer adversaries the ability to augment traditional air force elements with low-cost and less attributable means of ISR as well. These actions are further codified as Grey Zone

activities, below the threshold for armed conflict but committed with the intent to support an operational or strategic means. Such activities are conducted in the Indo-Pacific Command area of responsibility by the Chinese, in support of their regional hegemonic desires of expanding their ISR coverage around the Spratly Islands and harassing U.S. Naval forces in the area [20].

Further, UASs have enabled adversaries lacking the monetary means, technological capabilities, or logistical resources to compete for air superiority against superpowers such as the U.S. As anticipated, the massive surge in sensationalism and technological advancements in C2 have made malevolent UAS employment in any theater a considerable threat to force protection and operations. Commercially available UASs and tech savvy adversaries are now capable of conducting a wide barrage of operations due to the sensationalism associated with the UAS market. Table 2.4 shows how adversaries are leveraging UASs to accomplish means that were once either unattainable or only achievable through nation state actors as a means to complement their preexisting UAS TTPs.

Table 2.4. Modern UAS Employment Options.

Type of Operation	Pictorial Application
Sustained and Long Range ISR for Operational Preparation of the Environment or Battle Damage Assessment	DJI Phantom4 Pro quadcopter w/embedded camera  Example use case of the Group 1 UAS to provide the covert capability of conducting ISR in an area of interest by means of the onboard camera and gimbal. Although the DJI Phantom4 Pro quadcopter does not come commercially with a camera, it possesses the capability, like many other brands of UASs, as depicted here to add a camera and gimbal as a payload options.
Synchronized and Coordinated C2 of Ground and Air Elements	Autonomous quadcopter piloted w/smartphone device for C2  Example use case of a generic quadcopter with a smart phone device added as a payload to support C2 between the UAS vehicle and a GCS. This payload option is generic in nature, and can be leveraged to serve and support the extension of C2 between the UAS and the GCS, or other surrounding UASs operating as a cluster or swarm.
Distributed Messaging for Information Operations	Qualcomm quadcopter w/5G, LTE network connectivity  Example use case of a Qualcomm quadcopter with a 5G LTE distributed messaging payload included to support the mass or directed dissemination of multimedia messages to personal communication devices operating on a network of interest. Although the Qualcomm quadcopter does not come with a distributed messaging payload, it possess the capability, like other brands of UASs, as depicted here to add a message distribution device as a payload.

As identified during the early onset of OIR in Syria and Iraq, there were more UASs manufactured from more countries and being flown by more state and non-state actors than in any other conflict in history. If at least half a dozen of disenfranchised groups operate a moderate variety of UASs, they would be able to tip the scales of decisive engagements in their favor [21].

2.5 UAS Modes of Operation

Due to the wide availability of commercial UAS products and technological advancements in C2, the means of employment are associated with the technology of given time frame. The means of control and communication are obtained through the use of RF-reliant protocols, which includes cellular and satellite communications, Wi-Fi, and Bluetooth technologies. It is imperative to understand which means are leveraged by UAS operators to support the procurement of the requisite CUAS products to deter and counter UAS operability.

2.5.1 Bluetooth Control (2.4GHz– 2.5GHz)

Tiny, novice, and commercially available UASs predominantly operate in the spectrum of 2.4GHz to 2.5GHz under Bluetooth control. Due to the range of control in this portion of the RF spectrum being limited to approximately 100 meters, we assess UASs leveraging this technology to be more applicable to civilian recreational use or for short-ranged, tactical adversarial operations as denoted in Table 2.4. The use of Bluetooth technology is not widely hardened, and is therefore more susceptible to interference from other forms of RF as a means of countermeasure as expounded upon in Section 4.4.2.1. As with any C2 communication link, Bluetooth technology also enables the sharing of telemetric information such as air speed, course, and altitude between UASs and their controllers. The lack of security hardening, however may make such information susceptible to forgery, eavesdropping, device spoofing, or other misuse.

2.5.2 Cellular and Wi-Fi Control (900MHz – 2.4GHz)

Most commercially available, remote-controlled UASs operate at or around 900 megahertz (MHZ), while custom hardware and more sophisticated Group One UASs operate around 2.4 GHz. The ability to maneuver through the UHF portion of the spectrum between 900MHz and 2.4GHz provides UAS operators the ability to exercise C2 and exchange data via cellular networks, Wi-Fi, and other services, extending the range and mobility of the UAS. Commercially available UASs leveraging cellular networks to support their C2 make use of ground transmitters using cellular connectivity to support the exchange of data. Cellular networks range across 2G Global System for Mobile Communications (GSM); 3G code division multiple access (CDMA), time division multiple access (TDMA), and frequency division multiple access (FDMA); 4G LTE; and 5G. The employment of these technologies

to support UAS C2 for flight and payload operations is expounded upon in Chapter 4 Section 4.4.1. The associated ground control station receives subsequent connectivity to the previously mentioned networks by means of a base transceiver station (BTS) receiving service through an associated cellular service provider. Commercially available UASs can be equipped with 802.11 Wi-Fi enabled processors as well. The handler possesses a controller that serves as the transmitter, with a receiver located onboard the UAS. Both transmitter and receiver are tuned to the exact same frequency. To avoid denial of service (DoS) from competing devices that may be operating on the same frequency, the UAS transmitter and receiver use a radio frequency identification (RFID) chip. The receiver and transmitters pertaining to one or more UASs is then paired using the RFID chip associated with its UAS. All commands sent over the designated frequency are transmitted with the prefix of the RFID, and the receiver is aware that the associated command messages are intended for it and only it [22].

2.5.3 Satellite Control (1.2GHz – 1.5GHz)

Global Positioning System (GPS) technology leverages the use of satellites operating in medium earth orbit (MEO) as a means of obtaining locational waypoints for a means of navigation. GPS enables a UAS to span a much farther distance by means of pre-programmed waypoint navigation. This form of flight allows for semi-autonomy through the use of predetermined waypoints, terrain, or celestial navigation enabling a UAS to fly on preplanned waypoints [23]. The waypoints inform the UAS where to fly and the estimated time it should take to reach a destination. The estimated time to reach the destination will include the anticipated speed the UAS should use and the altitude is should achieve and maintain for the duration of the flight. GPS satellites transmit data in the UHF portion of the RF spectrum, using satellite communications (SATCOM) L1 1575 MHz and L2 1227 MHz [24]. The L1 and L2 signals are leveraged by the GPS satellites to support the broadcasting of civil use GPS signal to support commercial needs. The legacy L1 signal was superseded by the L2 signal, which has a higher effective power output to support transmission through trees and infrastructure. The use of GPS requires that a GPS receiver onboard the UAS be capable of receiving frequencies that GPS satellites leverage to transmit data.

SATCOM is also leveraged as a means of extending the ability to exercise C2 for UAS

control beyond visual line of site (BVLOS). The use of SATCOM antennas allow for UASs to utilize SATCOM to exercise C2 when out of range of potential terrestrial RF coverage. In this regard, the SATCOM antenna utilizes an uplink to a satellite which can serve as a relay or amplifying means of RF signals between the UAS and the associated ground station. The UAS is therein able to operate in the satellite's provided field of view or footprint casted on the earth's surface. This implementation provides UAS operators over the horizon operability for exercising UAS control, and will be further elaborated on in chapter 4.

2.6 UAS Tactics Overview

The previous means of UAS control can be used solely or in conjunction with each other. These means significantly impact the differentiation in UAS tactics at the disposal of UAS operators in the operational environment. While novice UAS users may leverage commercial vehicles over a Bluetooth connection for short range control, savvy technicians can leverage cellular and Wi-Fi services to extend the range of coverage and employ multiple clusters of commercial vehicles under a single C2 node. As anticipated, UAS methods of employment can be summarized in the categories of single use, cluster use, or swarm use. To defeat any of these employment options, the tactic must be identified. The technological means of C2 between the UAS or UASs and their operator must be known. Armed with knowledge of the tactics and C2 means, an adequate form of CUAS capability can be applied to deter, degrade, or destroy the detected UAS.

2.6.1 Single Use

A lone UAS is a single UAS controlled over RF by an operator, semi-autonomously, or autonomously via pre-programming. This can be accomplished via complete human-control or through some level of semi-autonomy attained via satellite control and GPS waypoint navigation. This method of employment is vastly leveraged and attainable with commercial off-the-shelf (COTS) products and has been displayed historically by disenfranchised organizations, terrorists, and various other non-state actors. The kinetic goals of employment range from crowd dispersal through the delivery of homemade IEDs to assassination of high value targets. Moreover, the ISR means of employment can augment the lack of organic, fixed wing air force and overhead satellites, or to clandestinely extend the capability of pre-existent capabilities.

2.6.2 Cluster Use

A cluster is a grouping of single UASs used for the purposes of attaining a mutual goal. This too can be completely under human control or obtained through a level of semi-autonomy. Therefore, a cluster may be controlled under one, or many different C2 nodes.

Aspirations of semi-autonomous UAS clusters use for kinetic targeting has been exemplified in previous terrorists' plots against commercial airliners, simulating a bird strike during takeoff [25]. Similar to that of a single UAS use, the operational purposes for using a cluster range from kinetic targeting of commercial airliners, IED crowd targeting, chemical weapon dispersal, logistics, cyber and electronic warfare, and messaging. Such an employment of UASs in an already crowded commercial airspace represents a direct and imminent threat to human life at a catastrophic level. Use of clusters implies a larger scale of warfare, and therefore an increased risk to casualties and operational end state. As such, this method of employment reaches beyond tactical levels of war and to operational aspects as applied by state actors, surrogates, and proxies.

2.6.3 Swarm Use

A swarm is identified as a set of aerial vehicles working in unison to accomplish a specific mission. A swarm can be controlled either manually or autonomously using pre-processors or pre-programming [26]. Missions are singular in nature, necessitating the need for the drones to self-organize to fulfill a requirement and achieve a desired effect. The DOD further defines a swarm as demonstrating collective decision-making and adaptive formation flying [27]. Similar to the use of single UASs or clusters, the threat by the weaponization and employment of several dozens to potentially thousands of UASs in a swarm directly impacts national security and is an indication of a superior level of adversary. The use of swarms serves as an elevated demonstration of capability and war. As such, this employment method is anticipated only by state actors, although the technology and accessibility is commercially available for purchase and employment. If swarms are equipped with chemical warheads or other explosives, they carry the capability to threaten large scale military and civilian equities such as power plants, bases, large crowd gatherings, and other protected events and assets. Their range of employment also covers large scale electronic warfare and cyber effects and weapon of mass destruction (WMD) dissemination. The aforementioned acts serve as an escalated level of capability and threat to civilian and DOD infrastructure and personnel;

therefore, swarms represent a strategic means of employment in war time. Per Figure 2.5, it was assessed by the DOD in FY2017 that UAS swarm technology would not present itself until 2042 [28]. However, in light of modern events, we assess swarm technology as readily accessible for acquirement and employment in an AOR. The associated communication links associated with swarm capabilities serves as another point for the assessment of when swarm technology would become practical, as expounded upon in Chapter 4.

Table 2.5. Comprehensive Roadmap for UAS Autonomy. Adapted: [28].

		2017 . . . . . 2029 2042		
		NEAR-TERM	MID-TERM	FAR-TERM
AUTONOMY	Artificial Intelligence/ Machine Learning	- Private Sector Collaboration - Cloud Technologies	- Augmented Reality - Virtual Reality	- Persistent Sensing - Highly Autonomous
	Increased Efficiency and Effectiveness	- Increased safety & Efficiency	- Unmanned tasks, Ops - Leader-Follower	- Swarming
	Thrust	- Taking Guidance and Validation, Ethical Requirements for Human-Decisions		
	Weaponization	- DoD Strategy Consensus - Laser Weapons System assessment	- Armed Wingman/Teammate (Human Decision to Engage)	

Contradicting this claim as shown in Figure 2.1, however, is a 2005 DOD assessment that the operational fielding of fully autonomous swarm technology would appear in as little as two decades from the year 2005 [29].

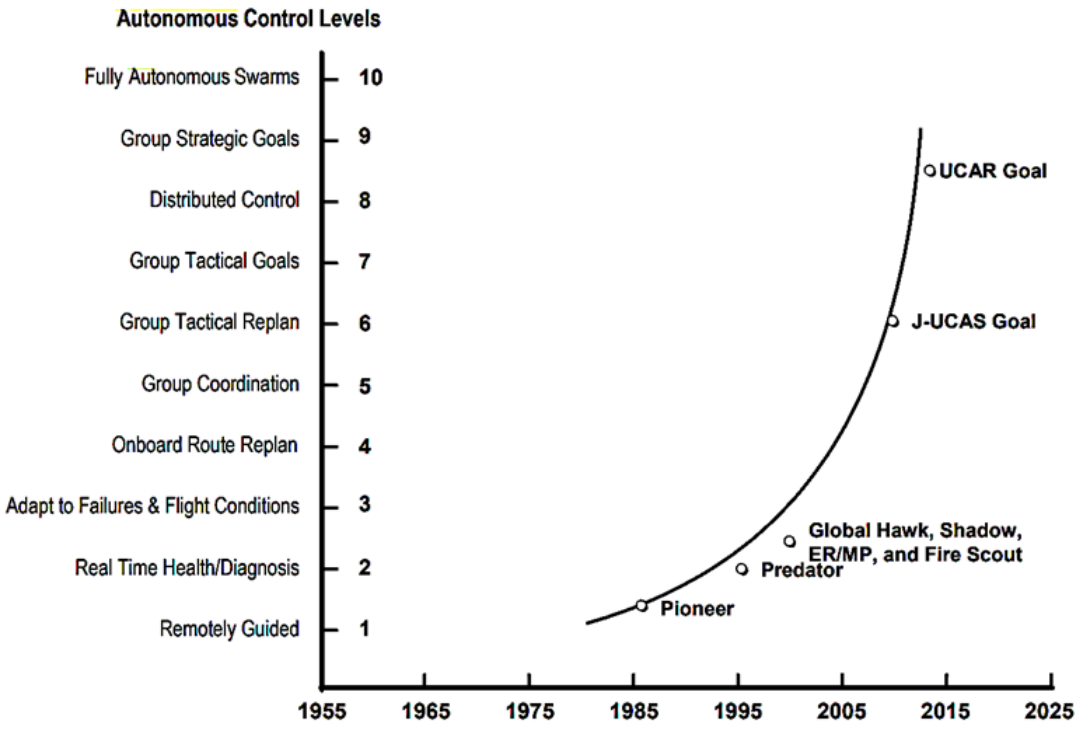


Figure 2.1. UAS Autonomy Capability Levels. Source: [29].

Figures 2.5 and 2.1 attempt to draw a comparison of similar criteria, although their conclusions vary by two decades. This ambiguity is related to what clearly defines the levels of autonomy for UASs. The levels of autonomy are based upon varying levels of intercommunication, tasks, coordination, and decision making conducted by the UASs in a swarm. The levels range from no autonomy to complete autonomy without human intervention. The University of North Dakota published an article relating autonomy of UASs to a decision cycle a UAS swarm would follow to fulfill a desired purpose [30]. The decision chain of a swarm is provided in Figure 2.2, providing a paradigm for potential autonomous decision making.

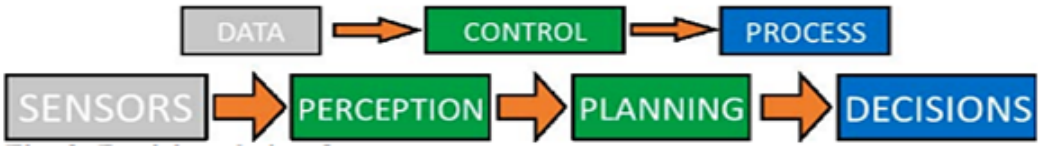


Figure 2.2. Decision Chain of an Autonomous System. Source: [30].

Furthermore, the uncertainty of when swarm technology will be operationalized is based upon the fielding of C2-capable equipment that spans the current cellular, Wi-Fi, and satellite architectures while properly satisfying the associated decision chain paradigms to meet full-autonomy. It is therefore difficult to assess if a cluster of UASs is truly operating under full autonomy and serving as a swarm.

2.6.4 UAS Tactics – Levels of War

The levels of war, as quantified by the U.S. DOD are tactical, operational, and strategic [31]. The tactical level of warfare is therefore the level that is short in duration, determining small decision points in combat. The operational level of warfare is the outcome of the tactical level decision points, and serves as an escalated phase of warfare. The strategic level of warfare is therefore considered the highest level of planning and execution, with political foresight and end state. The employment of these tactics provides a depiction for the level of sophistication an adversary possesses. It further provides indication of which level of warfare is being conducted. The use of a single UAS to augment ISR capabilities and conduct non-traditional warfare provides tactical level advantages on the field of battle. Tactical warfare is leveraged to determine small, contested conflicts in an ongoing wartime environment. The use of a cluster of UASs to support logistics or wage larger scaled kinetic effects against an opponent serves as a means of supporting operational endeavors in a wartime plan. However, the employment of a swarm for the purposes of delivering WMDs or conducting full-scale attacks serves as a strategic means, with attempts to cripple an opponent kinetically or informatively. Table 2.6 consists of a compilation of UAS tactics that have been historically used, attempted, or planned.

Table 2.6. Group 1-3 Historic UAS Tactics Used

UAS Tactic	Mode Of Employment	Description	Operational Impact
Single UAS	Human Controlled/Semi-autonomous	Rudimentary, tactical means to support terrorism against targets of opportunity or logistical compensation. Possible scenarios: ISR, IED delivery, and smuggling	Tactical level of war
Single UAS	Autonomous	Sophisticated means to enable terrorism against targets of interest. Possible scenarios: long range ISR, IED delivery, WMD delivery, smuggling, and EA.	Tactical level of war
Cluster of UASs	Human Controlled/Semi-autonomous	Air-to-air redundancy or multiple wave fronts in non-traditional warfare environments. Urban warfare enabler. Possible scenarios: ISR, IED delivery, messaging, C2, smuggling, EA, and ES	Operational level of war
Cluster of UASs	Autonomous	Sophisticated compensation to insurgency operations or state actor militaristic employment in operational environments. Urban warfare lead/primary focus of effort. Possible scenarios: long range ISR, IED delivery, WMD delivery, messaging, logistics, C2, long range smuggling, EA, and ES	Operational level of war
Swarm of UASs	Human Controlled/Autonomous	Artificially controlled through one or several nodes, sophisticated barrage attacks against crowds, venues, aircrafts, ships, vehicles, bases, and logistics. Possible scenarios: IED delivery, WMD delivery, and EW	Strategic level of war

2.7 U.S. CUAS Technology

The DOD has held a vested interest in CUAS products since 2008, following the proliferation and subsequent widespread use of commercial UAS products for terrorism and adversarial militaristic means in military conflicts [32]. This section explores these technologies.

2.7.1 U.S. Interest In CUAS Technology

The U.S.'s interest in CUAS capability spiked during OIR, when terrorist organizations such as the ISIS demonstrated the ability to procure, arm, and operationalize quadcopters at an alarming rate against American and allied forces. Central Command (CENTCOM) reported that ISIS primarily leveraged Chinese-made DJI quadcopters to serve as grenade launchers, kamikaze bombers, decoys, and to enable ISR. The need for CUAS technology was further warranted in other military conflicts such as in Yemen, when Iranian backed Huthi rebels leveraged UASs as a low-cost, high reward means to inflict heavy material and civilian casualties to the Saudi-led coalition at the Saudi and Yemini border. In 2019, the use of UASs in the Yemen war was exacerbated during the Huthis most audacious attack to date [33]. In this attack, ten UASs were used to inflict massive material damage to two critical oil installations deep inside Saudi territory. This attack leveraged the use of cheap, commercially modified UASs to defeat the world's third largest spender on military equipment. This attack also delineated a subversion of a multi-million dollar, U.S.-purchased air defense system by cheap UASs. Northern Command (NORTHCOM) became vested after a 2015 incident, when a civilian accidentally crashed a hobby DJI quadcopter on the White House lawn [34]. This incident served two purposes. First, it showed how vulnerable the most protected real estate in the U.S. was against cheap hobby kits. Second, it delineated the vulnerability of the White House and secure government facilities to attacks from novice actors, with rudimentary knowledge in the field of RF and IED making.

Europe Command (EUCOM) and CENTCOM both drew concern during a 2016 incident, when an inexpensive Russian-made UAS flew deep into Israeli territory from Syria for perceived surveillance, only to avoid being intercepted by successive Israeli Patriot Missile and Israeli fighter air-to-air missiles [35]. This failure drew heavy criticism for the inability to successfully intercept the threat, and for the failure to intercept the threat after the employment of extremely expensive, U.S.-manufactured and sold air defense systems. U.S. law enforcement, in conjunction with NORTHCOM's appetite for CUAS, swelled after law

enforcement and the U.S. Federal Aviation Administration (FAA) surmised that malicious actors could inexpensively employ UASs to jeopardize airports, large crowds, political events, concerts, sporting events, religious gatherings, and other organized functions that draw in masses of people.

The operational need for CUASs is to detect, track, classify, and interdict unidentified or unresponsive UASs operating in the vicinity of government property or displaying hostile intent. Interception is dependent on the CUAS technology. This could imply the employment of countermeasures to deny the progression of the UAS towards friendly equities, disrupt the employment of the UAS, or destroy the UAS.

2.7.2 U.S. Expenditures On CUAS Technology

The presence and potential for the malicious employment of UASs in the vicinity of civilian and military assets presents a direct threat to force protection and operations. Without intervention, this very presence could contribute to the undermining of global national security endeavors and jeopardize lives. The aforesaid examples of antagonistic UAS uses all evaded military defense radar detection. Traditional military air defense systems have shown they cannot adequately detect and track commercial UASs due to their size, altitude, manufactured materials, and speed. We assess the operational requirement to rapidly field CUAS products arose from exacerbated use of UAS products to undermine U.S. foreign policy. For fiscal year (FY) 2020, the DOD intended to spend at least $373 million on CUAS research and development and at least $200 million on CUAS acquisition and operationalization [36].

2.7.3 Legacy Air Defense System Shortfalls

We assess previously and currently employed non-CUAS air defense systems affixed upon mobile platforms such as the USN's carrier strike group (CSG) and amphibious readiness group (ARG), Marine Expeditionary Unit (MEU) and Special Purpose Marine Air Ground Task Force (SPMAGTF) assets, or upon fixed sites such as military bases are ineffective and uneconomical when tested against UASs. Traditional air defenses and their ineffectiveness against COTS UASs experience shortfalls in three areas of concern—the ability to detect the threat, the ability to classify the threat for subsequent neutralization, and neutralization of the threat with overly excessive force and monetary expense [33], [37].

The USN's Aegis combat system, designed by Lockheed Martin, is a surface-to-air missile and radar system used to identify, track and guide weapons to destroy designated aerial targets [38]. It was incepted and deployed in 1983 with the intent to track large, fast moving fixed wing and rotary aerial objects. Similarly, the USN's SPY-1 multi-function, phased-array radar is a highly mobile, land and sea-based radar that operates in the S-band portion of the RF spectrum with the intent of tracking larger, fast moving aerial targets. The S-band serves as a designated portion of the RF spectrum between 2 GHz and 4 GHz that is leveraged for aerial surveillance, surface ships radars, and communications. When combined in the maritime and expeditionary environments, Aegis and SPY-1 are only effective against traditional military assets operating in the S-band portion of the RF spectrum utilizing known or well trackable frequencies.

2.7.4 Adversarial UAS Exploitation Of Legacy U.S. Military Air Defenses

Legacy U.S. military air defense technology is actively exploited by our adversaries in locations such as the South China Sea, where China is extending and reinforcing its ISR capability with Groups 1 through 5 UASs connected to mobile and fixed C2 commercial and military sites [39], [40]. This addition provides China's preexisting ISR an all-seeing, low detectable eye in the sky. China's modified commercial drones will leverage their advantage of lightweight, high maneuverability, dynamic video payloads, against the U.S.'s inability to successfully track them in the maritime environment with legacy air defense systems.

Subsequent exploitation and usurpation of U.S. traditional air defense technology was displayed in the aforementioned Saudi oil pipeline attack on September 19, 2019 [41]. Saudi Arabia, as previously stated, is the world's third largest spender on military arms—spending $67.6 billion in 2018 alone. However, this rudimentary yet successful attack initiated by the Huthis illustrated that technological superiority does not equate to a wartime advantage. Here, Saudi Arabia's $1 billion air defense failed to defeat the low-flying, cheap, unregistered drones used to carry out the attack. Their inability to defeat the threat was partially related to the ineffectiveness of their air defense systems against small UASs and use of coastal defense cruise missiles. At the time, Saudi Arabia possessed the U.S. made Patriot missile defense system and Terminal High Altitude Area Defense (THAAD), German made Skyshield air defense cannons, and French Shahine mobile anti-aircraft systems.

2.7.5 Cost Effectiveness Of Legacy Air Defenses Against Commercial UASs

All of these systems are designed to detect and intercept traditional military targets operating at elevated altitudes. Each of the previously mentioned systems and batteries come at a price tag of several millions to hundreds of millions of U.S. dollars. Further, the price tag of a single missile averages $1 to $8 million. The cost of a single shot from the most recent variant of the Patriot missile is approximately $5 million [42].

This price begs the question if a strategic defensive capability should be used as a sole means of defense against a commercially available UAS, which could cost as low as a few hundred dollars. In June 2019, the Army Symposium disclosed a U.S. ally did indeed leverage a $3 million PAC-3 missile to intercept and shoot down a $200 Amazon purchased drone procured and operated by a non-state actor [43]. This demonstrates a horrific economic loss and a disproportionate response to inexpensive, vastly available threats. Therefore, the gap in defensive capability and the prevalence of UAS threats must be filled with more economic, practical, and effective hardware. We recommend this hardware being designed to meet this specific asymmetric threat, vice retrofitting preexisting legacy systems with lip service and further monetary losses.

2.8 CUAS Market

We assess the shortfalls of legacy air defense systems and growth of Groups 1 through 3 UASs has contributed to a growth in the CUAS market. Research shows that the CUAS market is projected to be worth $4.43 billion by 2026, making it one of the fastest growing spending categories in the defense budget [44]. The market for CUAS products is trending due to several categories, including concerns for personnel and material safety, increased use of COTS UASs in the civilian and military environments for malicious gains, an increase in availability of UAS capabilities on the open market, and the relative decrease in cost to procure and modify UAS technology for strategic, operational or tactical endeavors.

CUASs from a militaristic perspective are employed on high valued assets such as bases, secure installations, and naval, air, and ground assets to support and enhance force protection. Likewise CUASs, from a civilian perspective, are employed on high valued assets such as airports, sporting events, political events, VIP transportation, marine reserves, secure

facilities and infrastructure, and counter narcotics and weapons operations.

2.8.1 Foreign Influence On U.S. CUAS Market

We asses fiscal growth in the domestic CUAS market being attributed to global superpowers such as China, Russia, and the U.S. investing in laser-based anti-drone systems to protect high valued civilian and military equities. This is exemplified by the U.S. Army's acquisition request in August 2018 for Drone Dome Systems [44]. The army's Drone Dome system was designed and built to disable mobile UASs with a two-second concentrated laser weapon, capable of generating five kilowatts of power for hard kill. This is further delineated through the U.S. Army's contract with Raytheon in November 2018 for Ku-band RF radars, capable of detecting small, commercially available or modified UASs. In 2008, there existed no CUAS capability on the market to meet the urgent operational need to detect, classify, and neutralize malign UASs operating in critical airspace [45]. However, in 2015 it was estimated by Sandia Laboratories that just ten to twelve CUAS products existed as a result of the joint urgent operational needs fielded by the U.S. armed services and other countries. However, in 2019 it was estimated that approximately 537 CUAS products proliferated the market and operational environment [46]. The excessive growth in the market has brought upon a new challenge altogether. Now the market is inundated with CUAS products containing different claims of capabilities for detection, classification, and interdiction. Moreover, some products offer only one capability whilst others may offer one or more. The challenge now ensues on which CUAS product is best suited for the operational environment and legal authorities it is applied in.

2.8.2 Current CUAS Product Capabilities

We assess one short term goal of CUAS is to compensate for the shortfall presented by legacy and traditional air defense systems, which is to detect, locate and track, classify, and interdict small, low-flying, commercially available or modified UASs. We further assess a long term goal of CUAS is to support the intelligence community's collection of UAS signatures and technology. Figure 2.3 shows a defined CUAS kill chain of events leveraged by the DOD [47]. This figure provides a baseline of the desired effects for CUAS products. To successfully support the USN and USMC's intent of protecting its personnel and infrastructure from adversarial Groups 1 through 3 UAS threats, CUAS needs to be able to perform all of the

functions designated in the targeting cycle. Chapters 6 and 7 address the current CUAS capabilities and the need to support all aspects of the targeting cycle and interoperability amongst other CUASs. Chapters 6 and 7 further delineate the requisite supporting framework a CUAS targeting cycle requires, and demonstrate the necessity of transparency between the CUAS and other targeting cycles leveraged by the DOD shown in Figure 2.4 [47]. CUAS products' desired end state is the assured protection of forces and installations from unknown, unidentified, malign UASs. As one system may not meet all needs, there exists a goal to complement kinetic weapons deemed suitable for interdiction against commercially available UASs by providing indications and warning for queuing.

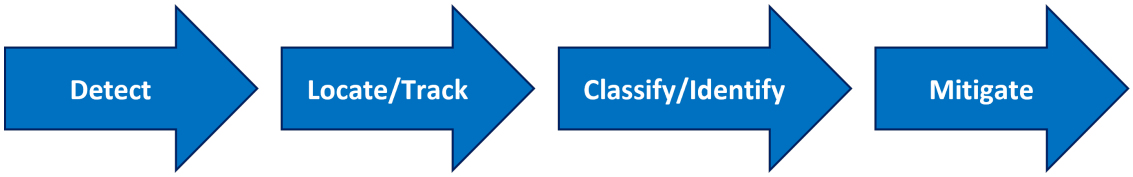


Figure 2.3. CUAS Targeting Cycle. Adapted from: [47].

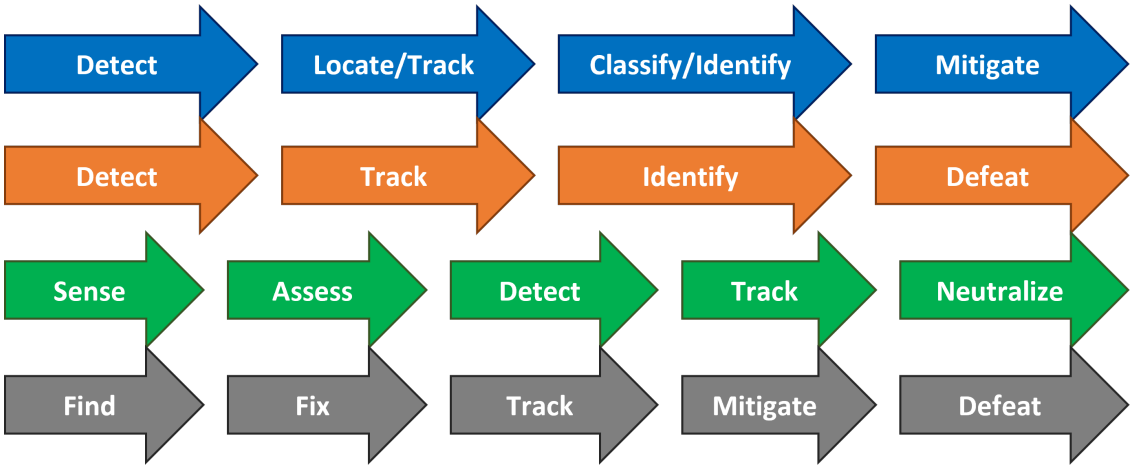


Figure 2.4. DOD Targeting Cycles. Adapted from: [47].

2.9 CUAS Targeting Cycle

2.9.1 Detection

The first step in the CUAS targeting cycle is the detection of a threat [47]. Detection of a threat implies a targeted UAS is within the range of the CUAS system's sensors. This action is followed by a subsequent alert to the CUAS operator that a potential target UAS of interest has been detected for further actions to ensue.

Detection is accomplished by first understanding how the UAS is communicating with its handler in the RF spectrum. It could also cover how the UAS emanates noise as it is propelled throughout the air, yielding an acoustic frequency that's detectable as a sound wave. It may also encompass how the UAS appears based on its surface area, dimensions, reflectivity of light, and amount of heat it emits [48]. From these differing perspectives of detectability, we assess that UASs may be discovered via sensors such as radar, RF, electro-optical (EO), infrared (IR), acoustic, or a combination of these also known as sensor fusion. The CUAS technology chosen will vary based on which techniques are used for detection. Table 2.7 provides a background overview of CUAS detection means used to identify the presence of a UAS. This table will be further elaborated upon in Section 6.2 to support applicability to current CUAS detection means leveraged by the USN and USMC.

Table 2.7. Detection, Tracking, and Classification Sensors.

Sensor	Description
Radar	Identifies the presence of commercial UASs based on the presence of a radar signatures used in the RF spectrum [47]. All radars operate by transmitting a radio signal of known frequency and power in a focused direction, and then utilizing the Doppler effect to detect the reflected signal that is returned after it impacts the target. Doppler radars differentiate whether the target is moving toward or away from the sensor, allowing the determination and discrimination of the type of object detected. The use of this method employs Doppler shifting and associated algorithms to discern between stationary objects and noise from the environment. The use of Doppler shifting is the change in frequency as an object draws nearer or farther from a source observing the object. This is an active form of emissions and sensing.
Radio Frequency	Leverages a library and rota of cataloged, known frequencies used by commercially available or modified UASs in an operational environment. The rota algorithm scans in the associated RF spectrum to search for known FOIs in an ascending order, and starts over if nothing is active. Once a FOI is identified as active, associated direction finding occurs to identify lines of bearing and enable tracking and queuing. This is a passive form of emissions and sensing [47].
Electro-Optical	The use of cameras to detect and classify a UAS based on its visual signature and unique characteristics [48]. Collects information in the visible spectrum. The uniqueness of UASs is cataloged in an updated and maintained library of known UASs, supporting the ability to distinguish between different classes and types of UASs. Differing sensors require specific features of a UAS be captured for accurate detection and classification of a UAS. The features captured on an EO/IR sensor are dependent upon the angular position of the sensor to the UAS. This is a passive form of sensing.
Infrared	The use of cameras to detect and classify a UAS based on its electromagnetic signature produced during operation [47]. Collects information in the infrared spectrum. This sensor typically includes wavelengths between 400 nanometers to 1 millimeter to support identification and discernment between short wavelength and long wavelength objects. This is a passive form of sensing.
Acoustic	The use of highly sensitive microphones to detect active UASs in an environment based on the unique sounds emitted by the UASs' propellers and the associated interference caused by air resistance [47]. This requires an updated and maintained library of catalogued sounds generated by known commercial UASs based on differing environments. This is a passive means of sensing.

2.9.2 Locate and Track

The second step in the CUAS targeting cycle is the ability to locate and track a threat once it is identified using the previously mentioned capabilities in Table 2.7 [47]. Locating an identified UAS implies the inherent ability to discern an accurate geographical location for it. This location can be provided in the form of latitude, longitude, and altitude on a display, military grid reference system (MGRS) on a grid map, or intersecting line of bearings (LOBs) on a quadrant as delineated in Section 6.2. The accuracy of this determination sets the tone for the ability to precisely track the targeted UAS's location as it maneuvers in the environment. Tracking is the anthology of the aforenoted reports over the period the UAS is active. The tracking should be presented as a legible means of points to an operator to support situational awareness.

2.9.3 Classification

The third step in the CUAS targeting cycle is classification of the threat [47]. Classification is the ability to discern a target UAS from the ambiguity of the environment it is operating in. Additionally, it is the ability to rule out background noise such as animals, debris, or commercial planes. Classification of a UAS is also based on the UAS make, model, manufacturer, and protocols used to operate and communicate between other UASs or the operator. Another means for UAS classification is made feasible through the Drone Remote Identification Protocol (DRIP), which is under development. DRIP serves as a rudimentary, trivial means to identify and classify the UAS by means of required self-broadcasting of the UAS's identification and location information for reception by other parties [49]. This form of identification intends to make the previously available remote identification (RID) protected and broadcasted publicly to support the efforts of the FAA, law enforcement, and the DOD with tracking unauthorized UASs. The ability to perform all of this requires a dynamic, living library that maintains a catalog of known UASs and their associated unique identifiers. After the detection and tracking of the UAS occurs, classification ensues based on the techniques from Table 2.7 and the comparisons against previously collected and logged UASs. Current UAS classification techniques are addressed in Section 6.2.

2.9.4 Mitigation

The final step in the CUAS targeting cycle is the mitigation of the threat by a means of interdiction [47]. Interdiction implies the use of kinetic or non-kinetic capabilities to render the detected, located, and classified threat as neutralized so that it poses no threat to designated high valued equities. Interdiction by means of non-kinetic effects is achieved through RF jamming between the transmitter and receiver of the UAS and its controller, or uplink/downlink jamming between the transmitter and receiver of the UAS and the satellite communications link being used to operate either autonomously or semi-autonomously. Another means of non-kinetic mitigation is to usurp or spoof the protocol used to control the UAS, thus seizing control of the UAS. Kinetic effects used to neutralize the UAS include the use of directed energy weapons systems. This use was exemplified by the first-ever employment of a laser weapon system (LaWS) on the USS Ponce in 2014, operating out of Manama, Bahrain in support of maritime and expeditionary force protection [50]. Another means of kinetic neutralization is the use of netting and projectiles. Both are intended to entangle or destroy the UAS upon aerial impact or subsequent impact with the ground. Depending on the CUAS product leveraged, one or more of the neutralization techniques may be applied as tiered options of escalatory use. Table 2.8 provides an overview, summarizing the interdiction means that may be leveraged by a CUAS products. This overview is further elaborated upon in Section 6.3.

Table 2.8. CUAS Interdiction Systems and Means.

Capability	Description
RF Jamming	Disrupting or degrading the RF connection (cellular, Wi-Fi, Bluetooth) between the UAS receiver and its transmitter, detrimentally impacting both the C2 and telemetric data for the system. Types of jamming may include barrage jamming, spot jamming, or sweep jamming on the desired frequency. Once the frequency's bandwidth is flooded with excessive noise, the connection between the source and receiver will be severed. Typical UAS response actions when experiencing RF jamming are as follows: (1) Remain in place, hover (2) Remain in place, land (3) Return to base (4) Continue to preprogrammed destination.
SATCOM GPS Jamming	Disrupting or degrading the UAS's GPS satellite uplink or downlink, detrimentally impacting its ability to receive temporal and spatial information in the operational environment [51]. This method detrimentally impacts a UAS's ability to operate semi-autonomously or autonomously. GPS jamming requires the jamming capability be located within the footprint of the satellite and UAS receiver. Downlink jamming disrupts the transmissions sent from the satellite to the UAS receiver by mimicking the frequency of the satellite downlink transmitter. Uplink jamming disrupts the transmissions received by the satellite receiver from the UAS transmitter and requires much more power and capability to perform successfully. Typical UASs response actions when experiencing GPS jamming are as follows: (1) Remain in place, hover (2) Remain in place, land (3) Attempted return to base if preprogrammed waypoints and another means of determining spatial orientation are available.
Spoofing	Identification and surreptitious manipulation of the RF and protocols used to control the UAS [52]. This means requires the foreknowledge of a weakness or exploitation of the communication protocol between the UAS and its controller, allowing it to be exploited, denied, and usurped for subsequent commandeering. This attack allows the UAS to continue its normal operation under the clandestine control of the spoofed signal, which is posing as a legitimate source. The capability allows the CUAS controller to consequently obtain telemetric data, point of origin, destination, and potential payload data from the UAS. Additionally, the CUAS operator may benignly snoop on the communications and data exchange between the real controller and UAS. Alternatively, the CUAS controller can send C2 commands to the UAS and augment temporal and spatial data transmitted to the UAS for the purposes of altering its flight path.
Directed Energy	The use of directed energy weapons such as the LaWS or high-powered microwaves to form and direct intense light or radio waves at a UAS [53]. The directed energy is focused into a beam and directed along the flightpath of the UAS. Directed energy is Intended to degrade or destroy a UAS by causing excessive damage to its circuitry and airframe.
Netting	The employment of netting guns to entangle a UASs propellers and render it unable to continue flight.
Projectiles	The use of small armament ammunition to destroy identified UASs within the associated range of the armament.

2.10 Current CUAS Technological and Legal Limitations

CUASs are subjected to employment limitations just as any emerging technology. In addition to this, there exists no international nor domestic standard for the construct of commercially available UASs and CUASs. We assess as product availability proliferates throughout the commercial and contracted business sectors, product performance will be varied. Thus, the level of variance between expected CUAS performance against a threat may be skewed. This challenge is exacerbated as the growth in the UAS industry continues to yield im-

proved technology and cheaper hardware. The forward momentum of the UAS market inevitably plagues the CUAS market as a reactive means of countermeasures. As the market continues to expand, CUAS technology will require more flexibility in capabilities and cost-effectiveness. Also, as countries' cellular and wireless infrastructures improves, so does the ability to leverage better forms of UAS C2 for covert means and elongated, more secure ranges of operation. Additionally, as CUAS products are operationalized we inherently train malicious UAS users to their capabilities. They gain from the ability to learn from previous and current CUAS capabilities and limitations, therein gaining better insight of the requisite modifications needed to defeat current and potential future CUAS technologies.

2.10.1 CUAS Technological Influence On Future UAS Operations

As contemplated, the incessant use of UASs in different environments supports the training and development of adversarial TTPs needed to defeat emergent CUAS capabilities. Future UASs may be employed in clusters, swarms and patterns that disguise the intent and desired outcome of their employment. This employment option also produces a large surface area and increased ambiguity of how to leverage current CUAS interdiction means. We may start to see UASs fabricated with material that lowers their radar cross section to further degrade CUAS detection capabilities. Such capabilities are used today on USN ships and aircraft. UAS operators may start to leverage dampening materials to absorb the noise emitted by their propellers, degrading acoustic detection capabilities. This technique is applied to USN submarines. Shielding could be applied to the body of the UAS and its circuitry, to buffer it from directed energy systems.

2.10.2 CUAS Legal Constraints

In addition to the CUAS technological shortcomings are the legal constraints of CUAS employment. Depending on the AOR, rules of engagement and the associated authority to leverage active means of detection and interdiction are handled and treated differently. Even for the U.S. to deploy weapons and countermeasures that ascertain directed energy as a means inside and outside the continent of the U.S., a rigorous oversight process is included. All directed energy weapons deployed both domestically and abroad must undergo a Directed Energy Weapon Review and Approval Process (DEWRAP), with approval authority resting with the office of the Secretary of Defense (SecDef) [53]. This was the

case for the installment and use of the LaWS on the USS Ponce in the Arabian Gulf between 2014 to 2018.

In allied countries, the use of directed energy weapons and electronic attack measures in the RF spectrum may be received as hazardous to operations, public safety, and health. The employment of these system may even be legally restricted or prevented in certain countries due to these circumstances. In the U.S., the use of CUAS detection means such as radar to intercept electronic communications, including telemetric data, spatial and temporal information, and associated source, destination, and operator details is considered a direct violation of the Wiretap Act [54]. Furthermore, the use of a cyber-attack to exploit and spoof a C2 RF link between the UAS and its operator could be prosecuted under the Computer Fraud and Abuse Act [55]. Furthermore, if a UAS C2 link is usurped by spoofing and results in the commandeering of the UAS, you must have and maintain a remote pilot certificate to pilot the vehicle [56].

The aforementioned legal challenges must be rigorously deconflicted and accounted for by host nation legal authorities and country teams. In some cases, a sensitive level of capabilities, limitations, and specification of CUAS means must be disclosed to ensure operational mishaps between the CUAS technology and preexisting host country public infrastructures are understood and minimized. However, such an intrusion into the intricacies of the CUAS specifications and capabilities may jeopardize the security associated with the functionality of the system. These observed restraints in the authority to operate CUAS plays a meticulous role of what CUAS means of detection and interdiction should be acquired for successive employment. We elaborate on this in Chapter 8 Section 8.4.

2.10.3 Challenges to CUAS Detection, Location, and Tracking

We assess UAS detection techniques as exceptionally challenging as the CUAS market expands in C2 capabilities, design features, and methods of operation. The use of radar and RF requires the active emission of a signal to detect an intruding UAS; therefore, requiring line of sight access to the UAS. This can become increasingly difficult for cluttered operational environments, where UAS operators may use the terrain to mask their locations and movements.

Further, radar and RF accuracy are susceptible to weathering. Precipitation and heavy

cloud cover may cause unintended absorption or reflection of emitted wave forms that are intended to detect and track a UAS. The use of radar is less reliant on a robust library for detection, but moreso for classification. However, RF must make use of a library of known UAS frequencies to validate the presence of a UAS to meet detection criteria. If a UAS has been modified, or not yet catalogued, then it may not be detected if it is not operating within LOS of the CUAS system. Therefore, a library must be maintained and updated routinely to ensure radar, RF, acoustic, and EO detection capabilities are accurate. The same criteria of library maintenance apply to acoustic and EO detection as well.

Acoustic sensors are also detrimentally affected by weather, since they rely on the receipt of sound waves unique to a UAS's propellers for detection. Adverse weather may cause distortion of sounds waves, causing a misinterpretation of a UAS or missed detection altogether. EO detection capability may only be leveraged during daylight hours, as these sensors rely on the visual observance of unique features to a UAS for detection. EO sensors are vulnerable to cluttered operational environments as well and are susceptible to misconstruing innate objects as UASs. Furthermore, EO sensors must be within visual line of site (VLOS) of the UAS to support accurate detection and are also detrimentally affected by adverse weather conditions. Infrared, however, is not affected by weather and can operate in day or night settings. However, infrared must too rely on a library to support classification of UASs upon detection. Table 2.9 provides a summation of our assessment of the CUAS detection limitations posed by each of the aforesaid sensor types.

Table 2.9. CUAS Detection, Location, and Classification Limitations. Adapted from: [47]

CUAS Sensor	**Requires LOS**	**Night Operation**	**Affected By Weather**	**Affected By Environmental Clutter**	**Ability To Classify UAS**
Radar	Yes	Yes	Yes	Yes	Constrained by library
Radio Frequency	Yes	Yes	Yes	Yes	Yes
Electro-Optical	Yes	No	Yes	Yes	Constrained by library
Infrared	Yes	Yes	No	No	Constrained by library
Acoustic	Yes	Yes	Yes	Yes	Constrained by library

2.10.4 Challenges to CUAS Interdiction

No means of CUAS interdiction has proven to be 100 percent effective all of the time. This is related to the growth and maturation of UAS technology and the TTPs leveraged to operate them. The CUAS market will have to constantly keep up with these challenges.

2.10.4.1 Challenges To UAS Jamming

Current uses of RF and GPS jamming is becoming antiquated as compared to the updated UAS market and TTPs used to avoid them. Jamming only works by disrupting the RF link between the UAS and its controller's receivers and transmitter, after the C2 link is detected. However, many UASs may now be programmed to frequency hop when a disturbance is experience on a primary frequency. This frequency hopping technique allows for sustained communications between the UAS and the operator during periods of jamming. Such a technique requires rapid detection and jamming on all observable frequencies, assuming they have already been deconflicted with local authorities. Also, some UASs are preprogrammed to operate either semi-autonomously or autonomously via waypoint navigation using GPS after launch. In the event of this instance, RF jamming is futile. However, GPS jamming is useful in this scenario. But, UASs are being equipped with means to overcome GPS jamming using methods such as hardening, GPS boosting, and encryption. Also, redundant means of navigation may be preprogrammed and leveraged such as inertial, spatial, and temporal depending on the surrounding operational environment. These methods are similar to those employed on military aircraft and missiles. Such a technique allows for the UAS to operate in GPS denied environments, as costly as it may be [57].

2.10.4.2 Challenges To UAS Link Interdiction

The use of inherent, protected communications links over an encrypted network provides for hardening against electronic attacks such as spoofing. Additionally, the use of deception tactics such as fake frequencies as bait can be leveraged to honey pot spoofing tacticians to a benign frequency of interest. Hardening of fabricated UASs' bodies and circuity may be employed to defeat directed energy weapons. The use of materials such as lightweight, highly absorbent polymers are not as sensitive to concentrated heat. This could provide time for an operator to manipulate their UAS out the LOS of the directed energy weapon. The employment of clusters and swarms also serves as a tactic to defeat directed energy and

netting weapons. This is due to the wide surface area covered by the vehicles, eradicating the ability to successfully interdict all of them.

2.11 Applications of CUAS Products

Although nascent, we assess CUAS products' being employed more throughout the operational environment in several high profile events. Its demonstrated success has fueled the market growth and variations of products. CUAS has been used to support force protection and queuing on bases, CSGs, ARGs and mobile ground assets [4]. Their inclusion into military planning has complemented existing weapons systems such as Aegis, Patriot missiles, small arms, and counter-mortar systems through the indications and warning provided by their queuing. Conversely, CUASs have been incorporated in the civilian environment to support airspace protection and awareness at sporting events, political rallies, VIP protec-tion services, and for law enforcement endeavors [4]. Figure 2.5 provides a delineation of previous CUAS uses in the U.S. for militaristic and civilian purposes.

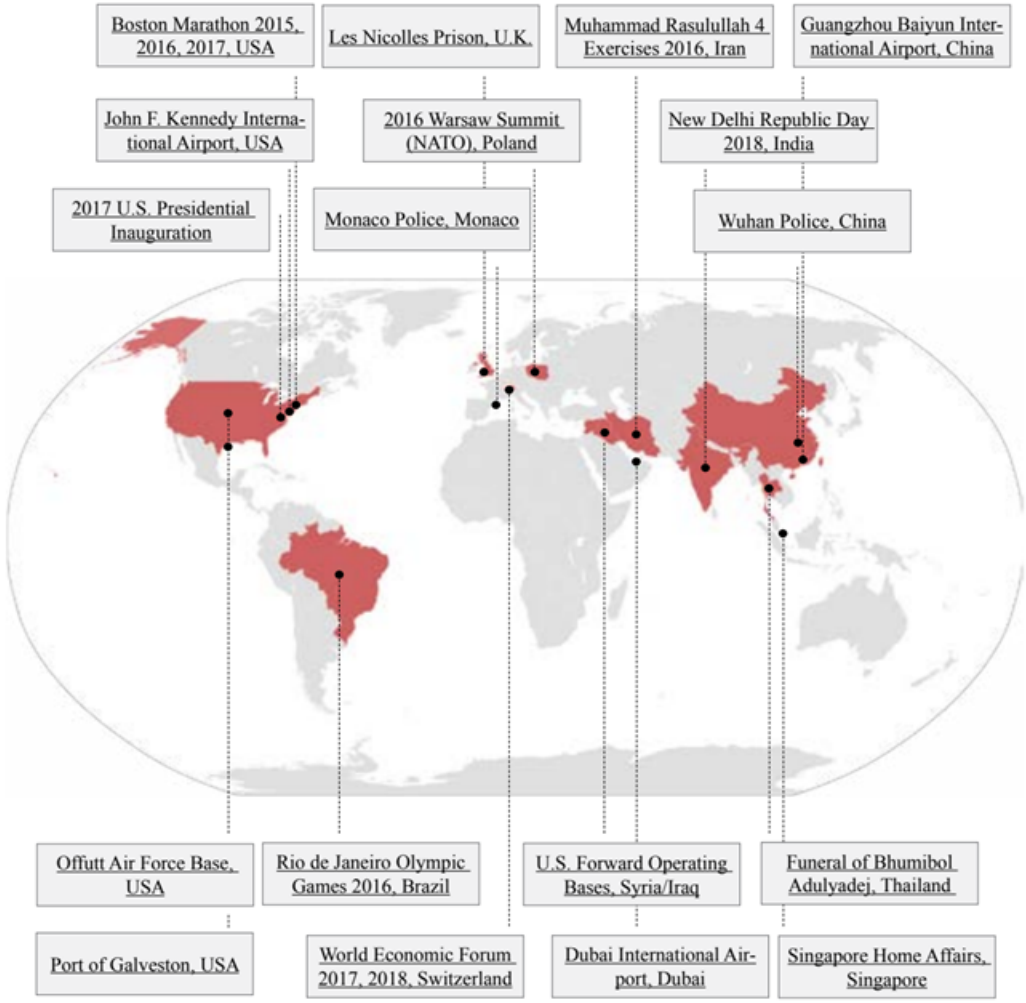


Figure 2.5. Previous CUAS Employment. Source: [4].

2.12 Summary

This chapter provides the foundational background of our research – the need for effective and interoperable CUAS employment to support force protection of USN and USMC personnel and equities. It further provides our initial background assessment of the challenges associated with satisfying the CUAS targeting cycle as UASs evolve over time due to the technological advances in specific operating areas. Lastly, this chapter introduces the legal constraints associated with CUAS employment, once effective and interoperable capabilities are identified to mitigate emergent UAS threats. Holistically, all of this must be considered

to adequately support USN and USMC CUAS operations in every AOR against current and future UAS threats.

CHAPTER 3:
Adversarial UAS Operators

This chapter addresses the current actors employing COTS Groups 1 through 3 UASs in the operational environment. This chapter contextualizes the historical application of which actors have employed UASs to address the current capabilities and limitations associated with UAS employment. Here, we define the actors employing UASs using the National Intelligence Council (NIC) interpretations for hobbyist and adversaries.

3.1 Unmanned Aerial System Employment Overview

To date, approximately 90 nations and non-state actors have been proven to own and operate UASs [58]. Similar to the pursuit of nuclear weaponry, in 2015 there were an estimated 20 additional counties with purportedly developing armed drone programs [58]. As anticipated, weaponized drones will shift from serving as a commodity to commonplace employment in the near future as described by the DOD UAS Roadmap [5]. Previously described in 2.2, many non-state actors have already leveraged COTS UASs to support rudimentary tactical endeavors to include ISR, smuggling, IED delivery, and biological attacks to undermine U.S. national strategy.

The aforementioned increase in UAS employment can be attributed to their ease of modification with complementing technology, thus exacerbating the threat. The threat of adversarial UAS operations detrimentally impacts the U.S., its allies, and its national security endeavors both domestically and abroad. The threat, its underlying technologies, and an understanding of the actors that employ them must be thoroughly understood to decisively determine, acquire, and deploy the requisite means of CUAS technology and associated training in support of USMC and USN operations and U.S. national security endeavors.

Adversarial UASs and their means of employment vary based on their quality, capability, accessibility, and affordability, which is constrained to their geographic area and the em-ploying party. This variance arrives in the form of low-cost, short range, line-of-site COTS UASs to technological advanced, six figure, state sponsored UASs that require a substantial operational infrastructure. In this chapter, we will categorize the actors employing UASs by

the degree of UAS accessibility and the underlying technological infrastructure to support their means of employment. As such, the type of adversaries employing Group 1, Group 2, and Group 3 UASs can be codified into the categories of hobbyist, non-state actors, and state actors.

3.2 Hobbyist

Hobbyist UAS operators refers to the recreational employment of COTS Group 1 UASs. Although hobbyist and the commercial development and employment of UASs are benign in nature, its nascent influence on the market asserts a crucial aspect on the procurement and modification of UASs by non-state actors. Hobbyist UASs accounted for an approximate 3000 percent increase in annual revenue for UAS use worldwide in 2014 [59]. This growth in popularity and influence on the commercial market can be originally attributed to the Chinese based Shenzhen DJI Technology Company between 2011 and 2013. The rise of consumer demand for recreation drone use has been equally met by producer supply chains supported by SZ DJI, continuing to their rise of market capital from $130 million in 2013 to $500 million in 2014 [59].

3.2.1 COTS Impact On Hobbyist UASs

As sales of COTS UASs continue to increase and the underlying technology to operate them becomes more available, the overall cost of COTS UASs will decrease. This is exemplified by the 2013 Phantom 1 DJI equipped with additional gimbal and power management unit cost of $1430. The Phantom 1 was plagued however by shortcomings associated with telemetry, range, power, interoperability for customization, and speed. The 2017 Phantom 3 DJI however, may be purchased as low as $399 and includes a three axis gimbal (as compared to the 2013 two axis gimbal), three times the flight time, double the range, third party software application to extend range and capabilities, and intelligent flight modes such as points of interest and waypoints to support semi-autonomous operation [60].

3.2.2 Software Impact On Hobbyist UASs

The ability to support third party software provides a level of customization suitable to the operational environment in which the UAS is employed, thus enabling cutting-edge capabilities that were previously monopolized by state sponsors and infrastructure. Such

inclusion of GPS waypoint navigation removes the shortcomings associated with the line-of-sight coverage of the legacy 2013 DJI Phantom, allowing the UAS to remotely determine its position, navigate, and return to its point of origin on point of programming. Additional upgrades associated with third party software include the ability to navigate to points of interest by means of a smart phone application. Chinese owned and based UAS startup, EHANG, performed and deployed commercial models capable of this feat in 2014 after procuring basing in San Francisco, California. By use of EHANG's Ghost Drone smart phone application and accelerators in tandem with COTS UASs, UAS operators may now navigate their UAS by tapping a spot on the application's map interface and controlling the angle of the UAS's attached GoPro camera. The use of a mobile application makes the navigation of drones widely accessible to any user and removes the necessity and learnability associated with radio controllers [61].

3.2.3 Hobbyist UASs Impact Against USN and USMC Operations

Although some COTS systems contain foundational firmware to preclude the overflight of airports, sporting events, or government facilities, this can be subverted through programming and aftermarket components by non-state and state actors. However seemingly innocent or unconfrontational in nature, hobbyist and their associated COTS UASs pose a significant threat to USN and USMC operations ashore and abroad due to the opportunity they provide more aggressive, malevolent actors. As Chapter 1 demonstrated, hobbyists' intentional and unintentional actions with COTS UASs demonstrate a low risk, high reward capability to non-state and state actors. Hobbyists' actions such as the DJI quadcopter downed on the White House lawn in 2015 or use of high-definition GoPro for live video feeds demonstrate the unique capabilities and room for expansion for the desiring adversary [34]. This expanded use and the subsequent proliferation of recreational UASs has indeed increased the prospects for the disruptive employment of COTS UASs by non-state actors.

3.3 Non-state Actors

The NIC defines non-state actors as non-sovereign entities asserting increased socioeconomic influence over a particular country's national interest. These organizations and subsidiary actors can include trade unions, community entities, religious followings, eth-

nic minorities or majorities, and academic institutions [62]. The NIC further regards state actors' roles based on their ability to ascertain and exercise power and influence over a population based upon the areas' political, economic, and social infrastructure. We assess these areas as weak states, developing/post-industrial states, and modernized states.

Non-state actors exercise more influence in weak and developing states such as Iraq, Syria, Yemen, Somalia, and Iran, vice modernized states such as China, Russia, India or the U.S. The NIC defines "weak states" as former holdings from western colonialism that failed to transition to a viable nation following their independence [62]. The existing governments of weak states that are subsequently formed often find difficulty providing reputable support to their people, and therein resort to violence, reprisals, and force to maintain the semblance of peace. In this regard, weak state governments are often formed from religious or tribal factions, and therein based on the biased interpretation of legacy tribal of religious practices. Developing or post-industrial states are defined as having evolved from prehistoric state sovereignty used in modern states, where nationalism only exist to protect the identity of the governing body [62]. Borders in this instance are not as relied upon as identification of statehood, and the distinction between domestic and foreign affairs is ambiguous and treated with equal calamity.

3.3.1 Non-state Actors Employment Of UASs

We assess non-state actors' employment of UASs as a function of hobbyists' demand and operationalization of UASs. Hobbyists and their associated UASs typically do have inherent high-definition cameras and EO based sensors to support sensor-based sense-and-avoid capabilities. Further, modification can be made to support the employment of semi-autonomy or autonomous operations through GPS waypoint navigation, for example. These modifications are leveraged as a method of overcoming the necessity of human control and allow for semi-autonomy or full autonomy of the vehicle to support stealth, endurance, and non-attribution of the operation. Although most hobbyist deployed COTS UASs have short ranges, limited power, and limited payload capacity, non-state actors have demonstrated the ability to overcome these with third party software, modified rotors, and added storage features to support successful nefarious actions [17].

As shown in Table 2.2, non-state actors have employed COTS modified Group 1, Group

2, and rudimentary Group 3 UASs to conduct ISR, smuggling, and IED delivery against U.S. and coalition forces domestically and abroad. Basic non-state actors will leverage Group 1 UASs to carry out simple tactics of ISR and deterrence, followed by the potential weaponization of UASs via IEDs and grenades as seen in Syria by Hezbollah and ISIS. As previously alluded to, non-state actors consists of such groups that aim to undermine U.S. legitimacy through guerrilla style tactics that yield small material affect and a minor threat to life, but serve as a deterrence nonetheless.

3.3.2 State Sponsored Impact On Non-state Actors

Non-state actors that are aligned with state sponsors such as Lebanese Hezbollah, Houthis, and Hamas are capable of receiving unacknowledged aide from state sponsors such as Iran and Russia. Such support provides the capability of access and use of Group 3 UASs such as the Iranian supplied Ababil III UAS, with an endurance of four hours and range of 100 kilometers, enabling increased loiter time to improve targeting, ISR, and C2 [63].

Due to the inability to control supply and demand of COTS UAS and non-state actors' modification of UASs, we assess the amount of damage a Group 1 through 3 UAS can inflict extends beyond country borders. As delineated, modified COTS UASs are not confined to state actors and their associated nation states. As of 2020, approximately 90 countries, operate midsize commercially available UASs which we codify as Groups 1 through 3, and up to military grade UASs we identify as Groups 4 and 5 [64]. Figure 3.1 captures the gravity of the wide dissemination of and subsequent threat imposed by COTS UASs.

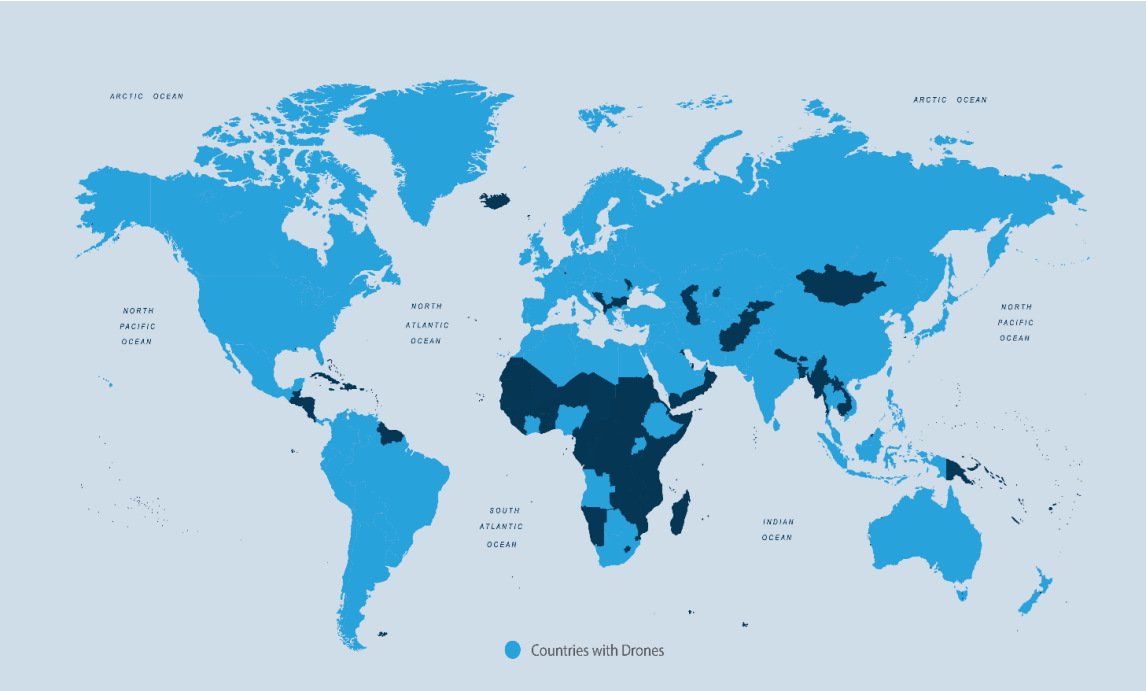


Figure 3.1. Countries with Group 1-3 UASs. Source: [64].

As depicted, the growth of the UAS market and the associated employment of UASs by countries of interest for hobbyist intended purposes can be usurped by non-state actors for the purpose of malicious endeavors against the U.S. The inherent or modified capabilities of COTS UASs hold destructive potential in the hands of non-state actors. This increased, proliferated, global use of UASs to conduct, cheap, malicious attacks provides the basis for the evolution of future warfare. As explained by American military and national security affairs journalist Yochi Dreazen, "the next evolution of warfare-by-remote-control, when weaponized robotic planes give terrorist groups de facto air forces" [65].

3.3.3 Impact Of Non-state Actors UAS Operations

The representation and subsequent damage inflicted by a non-state actor UAS holds both a psychological meaning as well as a kinetic meaning. Psychologically, it represents the ability of a low-end, non-state sponsored actor having the ability to compete with a nation state to deliver an operational or tactical level of military impact. It allows these same actors to figuratively punch above their weight class, providing them with the means of a traditional

air force, such as ISR, C2, or ordinance delivery. These mechanisms, typically reserved for state actors and nation states, we assess as strategic levels of employment. Figure 3.2 is an indication of the level of sophistication achieved by non-state actors and their use and modification of COTS UASs.

Capabilities	Limitations	Technology Trends (in addition to the technologies available to the hobbyist)
Deliver payloads of up to a couple hundred kilograms at ranges of up to a couple hundred kilometers	Vulnerable to countermeasures, including GPS-jamming and spoofing, small-arms fire (at lower altitudes), and man-portable air-defense systems (MANPADS) (at higher altitudes)	Increased range, payload, and endurance
Capture high-definition images and video at ranges of up to a couple hundred kilometers; real-time transmission at ranges of up to around 30 kilometers	Not survivable in contested or denied airspace	Releasable missiles or bombs
Persist for moderate periods (generally between 60 minutes and a few hours)	Line-of-sight communications	
Operate in communications-denied environments using fully autonomous GPS and waypoint navigation	Data links vulnerable to interception	
All-weather terrain mapping and target tracking via advanced radar	No current ability to release missiles or bombs	
Identify and designate targets via laser range finders and illuminators		
Transmit data via encrypted, high-bandwidth data links		
Limited jamming and electronic intelligence-gathering		
Communications relay function		
Ability to perform a kamikaze mission using an explosive payload		

Figure 3.2. Non-state Actor UAS Capabilities. Adapted from [64].

3.4 State Actors

State actors are entities, organizations, and persons that represent and are acting on behalf of a formally recognized world government. As expected, state actors and their associated actions are inherently held liable by the country they are affiliated with. Further, state actors and the country they are affiliated with are held to globally recognized standards, treaties, agreements, accords, and normalcies. State actors therefore tend to holistically operate Group 3 UASs due to their traditional military nature and intended uses. Their use of UASs

portray the next, and final step in this continuum of cost efficient aerial vehicles to deliver the similar effects of a traditional aerial force.

3.4.1 State Actor UAS Employment Methods

The intended uses of state actor UASs are anticipated to augment and complement a nations' preexisting, or non-existent air force in regards to ISR, logistics, weapon delivery, C2, and electronic warfare. State actors' procurement and consequential modification of UASs include increased flight time endurance, range, and ability to hold more payloads. This is exemplified by vehicles such as the Israeli Heron, with a top speed of 112 knots, 20,000 to 45,000 foot altitude barring modifications, and endurance of approximately 30 hours on station. This brand of UAS is available for distribution and flown by over 20 EU and NATO countries to date, with payload capability exemplified in Figure 3.1.

Table 3.1. Israeli Heron Group 3 Capabilities. Adapted from [66].

Payloads	Air Space Integration	Data Links
Deliver payloads of up to a couple hundred kilograms at ranges of up to a couple hundred kilometers	Identification, Friend or Foe (IFF)	Integrated ATC Communication Relay
Synthetic Aperture Radar (SAR)	Traffic collision avoidance system (TCAS)	Direct Line-of-Sight (LOS) data link
Communications Intelligence (COMINT - HF, VHF, UHF/ DF)		Satellite Communication (SATCOM)
Global System Mobile (GSM)		UAV airborne data relay (ADR) for beyond LOS missions
Electronic Support Measures /Electronic intelligence (ESM/ELINT)		Ground-based data relay (GDR) for beyond LOS missions
Maritime Patrol Radar (MPR)		
Aerial Persistence		
Customer furnished payloads & Sensor suites		

3.4.2 Weaponized UAS Programs

We assess the necessity for state actors to match the aerial capabilities of rival nations driving the pursuit of developing weaponized drone programs and payloads to accompany Group 3 UASs. As shown by the Ababil III, Mohajer IV, and Heron, these Group 3 UASs already have an inherent ability and capacity for a weapons payload. As of 2015, over 10 countries possessed armed and weaponized Group 1 through 3 UASs in their arsenal, with

more than 20 countries actively pursuing armed UAS capability as indicated in Figure 3.3. In this reference and regard, armed UASs constitutes the ability to deliver missiles, bombs, explosives, chemical or biological payloads, or using the UAS itself as a projectile.

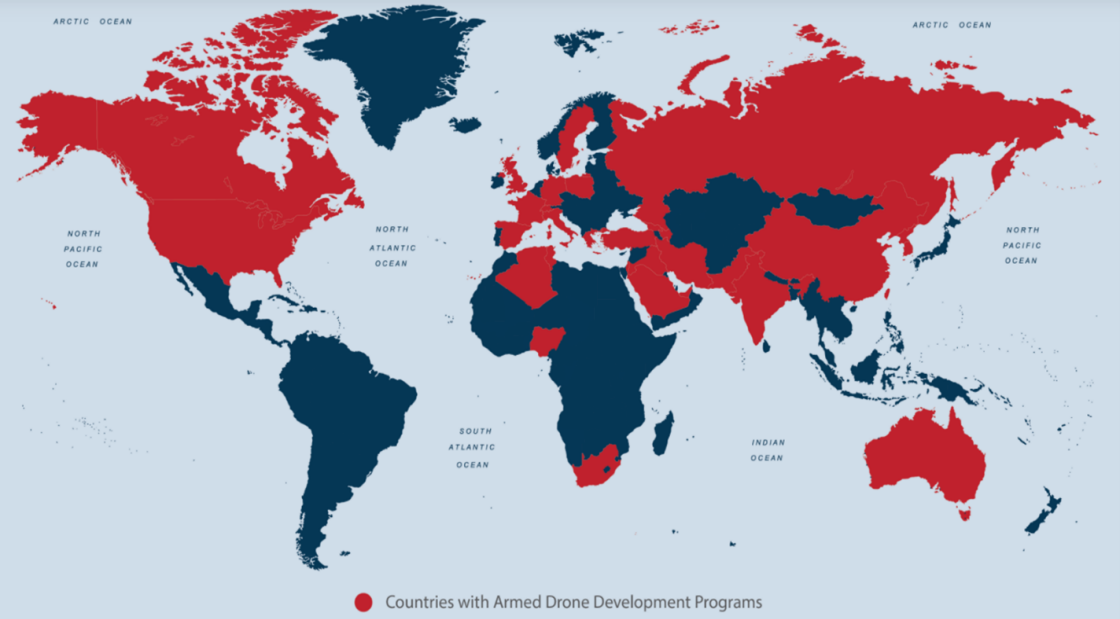


Figure 3.3. Countries with Armed UAS Programs Source: [64].

Although armed UAS programs may vary in capability, the intent and desired end state remain consistent – the use of armed UASs to support preexisting military aerial infrastructures to support regional and global pursuits. This variance in capability is exemplified between the U.S. and Pakistan armed UAS programs. Although Pakistan's armed UAS program is nascent in nature, it still demands attention due to its rapid growth and acceleration in technological achievements. Pakistan's Burraq UAS shows this, with its inherent 16,000 feet altitude, 80 knots speed, and capability to carry kinetic armaments. Further, it delineates Pakistan's ability to seek measures beyond traditional kinetic armament into the realm of directed energy.

In 2015, Pakistan stated its intention to deploy the Burraq with laser armaments in an attempt to deter and defeat non-state actors operating along its coast and within country [67]. The laser guided munitions were advertised to operate with pinpoint accuracy and operate in all-weather categories. This accelerated UAS capability is yet another indication of the

already occurring race among state actors to emulate the U.S. by acquiring and deploying UASs as an extension in their instruments of war.

3.5 Adversarial UAS Employment Association

Cumulatively, hobbyist, non-state, and state actors employment of UASs is dependent on the strategic goals associated with the operational employment and underlying technology employed, but can be summarized by Table 2.6 (see Chapter 1). Here, the use is depicted based on the level of autonomy and number of UASs being employed. The strategic goals for the employment of UASs by the aforementioned actors will be elaborated upon in Chapter 5.

3.5.1 USN And USMC CUAS Response To Adversarial UAS Employment

Although the USN and USMC present varying degrees of presence in each AOR with independently classified CUAS TTPs, their CUAS TTPs have been made publicly available through demonstration against adversarial UAS encounters. The USN and USMC's use of force under previous rules of engagements in areas of armed conflict have therein provided an affordance to the previously mentioned categories of adversaries to study, understand, and develop similar UAS capabilities. However, U.S. doctrine writ large allows geographic combatant commanders and their subsidiary service components the freedom of interpreting the adversarial problem set at their discretion. This is exemplified in every theater's posture statement to the Senate of Armed Services Committee.

Posture statements are intended to provide a transparent portrayal of a combatant commander's guidance and policies for their AOR, and issue direct and indirect guidance for their service elements to act upon. EUCOM's current posture statement is an overt display of this discretion. In February of 2020, EUCOM Commander General Lyons commented upon the vast amount of potential for the production, acquirement, and employment of autonomous UASs in his AOR [68]. He further stated, that although this threat existed on the horizon, that every U.S. military service was seeking their own solutions to prepare and remedy their shortcomings against the possibility of such a threat. The disparity in understanding the consistent and persistent threat amongst AORs while the adversaries develop

sustained programs to undermine our traditional military capabilities serves as an interoperability issue. To adequately address this concern and threat, this research is intended to subsequently understand the threat holistically as defined in this chapter, and determine suitable means of CUAS to address these adversarial threats.

3.6 Summary

This chapter defines the threat actors who are leveraging UASs in varying AORs. We utilize the definition of threat actors provided by the NIC to support our assessment of how the threat is currently employed, the associated goals for employment, and the potential for future advanced employment goals of UAS operators, regardless of AOR. The enemy and threat imposed by their use of UASs always has a vote in every operational plan. As stated in Chapter 1, the threat must be adequately understood to support adequately defeating the threat.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 4:
UAS Technologies

This chapter discusses the current technologies leveraged by UAS actors in the global geopolitical environment to support UAS C2. We define the current communication architectures available to support UAS C2, their associated vulnerabilities, and the security used by each architecture. We place emphasis on the ability to further leverage existing and emergent technologies to modify and augment COTS UAS's C2 to support flight and payload operations. We further address the ability to modify COTS UASs and GCSs using the associated programming libraries pertaining to a vendor. To accomplish this, we use the widely employed DJI platform as a case study for altering UAS flight behavior.

4.1 Unmanned Aerial Systems Architecture Overview

The ability to counter adversarial UAS use and operations is dependent on our understanding and knowledge of the art of adversarial UAS employment. Effectively countering small UASs is not met without challenges, as quoted by General Terrence J. O'Shaughnessy at the House Armed Services Committee, "Our adversaries have watched, learned and invested to offset our strengths while exploiting our weaknesses. They have demonstrated patterns of behavior that indicate their capability, capacity and intent to hold our homeland at risk below the nuclear threshold." [69]. The art of drone use, as generally discussed in Chapters 1 and 3, can be categorized based on the UAS means of achieving and maintaining flight, the C2 architecture for communication, and the modes of operation.

The UAS architecture holistically consists of the vehicle's frame, motors, power supply, and flight controller to link these components together to achieve and maintain flight and support UAS operations. The use of GCSs are leveraged to enable data exchanges between the operator and UAS using variable means of C2, which are also referred to as communication data links. For this research, we shall focus on the flight controller component of the UAS, its impact on motion pertaining to the UAS, and the potential means of modification to it.

4.2 UAS Flight Controller

The flight controller serves as the linkage between the aforementioned UAS components, the GCS and C2 associated with UAS flight operations and mission profiles. Figure 4.1 provides a graphical, exemplified depiction of the flight controller for a DJI UAS.

Flight controllers vary based upon UAS capability and employment, from hobbyist use to commercial use. Hobbyist flight controllers serve as the most common multipurpose flight controller, providing a limited range of control functionality to support recreational activities. Commercial flight controllers consist of more advanced avionics to support premeditated flight path, semi-autonomy, and the transportation of cargo. As anticipated, hobbyist and non-state actors alike typically leverage the prepackaged hobbyist flight controllers to support the rudimentary tactics described in Chapter 3. These flight controllers are typically manipulated from their COTS standard or used directly out-of-box. This is due to the previously mentioned capabilities provided by the COTS flight controllers to support inherent manual and semi-autonomous navigation, telemetry, and the ability to support the carriage of stowed materials.

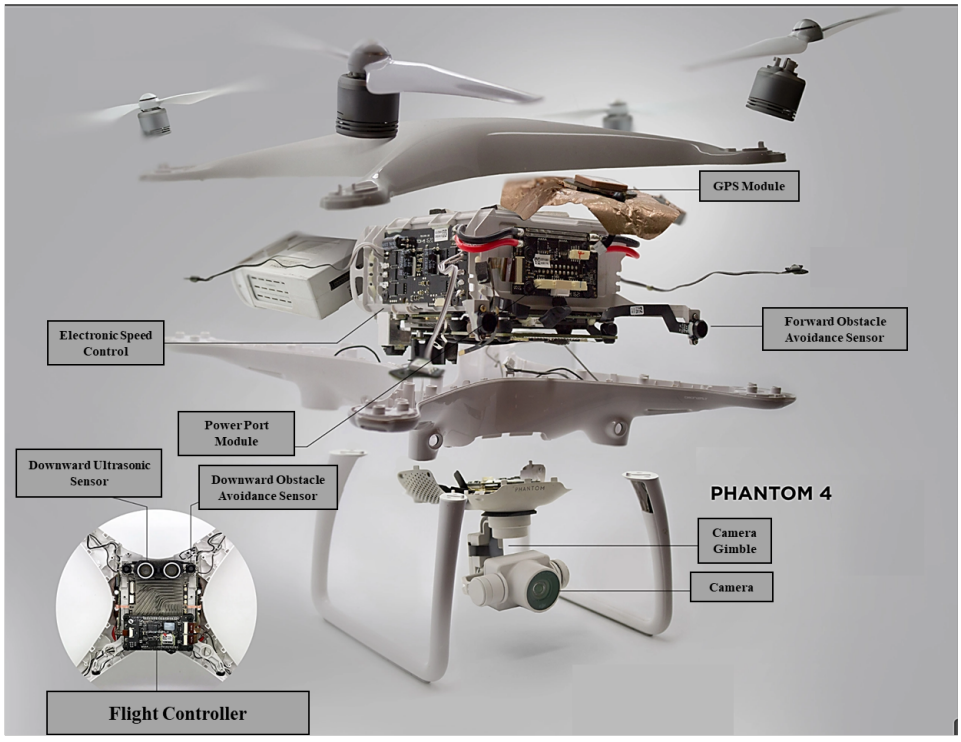


Figure 4.1. Example UAS Components. Adapted from: [70].

The flight controller on a small UAS typically resembles a circuit board and varies in size depending upon the complexity associated with the UAS's inherent or modified modes of operation. The flight controller circuit typically consists of a microprocessor, sensors, and associated input and output accessories, and serves as the central processing unit for the drone. Expectedly, the flight controller provides the UAS operator the ability to operate the UAS during flight by providing the foundational capabilities for sensing objects around the UAS, controlling the UAS, and communicating with the UAS while in flight.

4.2.1 Flight Controller – Sensory Functions

To support the sensory level functions for the UAS, the flight controller is connected to the requisite UAS instruments providing information pertaining to the UAS's altitude, speed, orientation, and heading. Typical instrumentation that supports the achievement of this are barometers to determine altitude, pitch, and angle through the use of Doppler against the terrain. Other instrumentation used to support the sensory functions of the UAS are exemplified by the use of an inertial measurement unit to determine angular momentum and subsequent orientation of the UAS.

4.2.2 Flight Controller – Controlling Functions

To support the controlling of the UAS's speed, course, and altitude, the use of speed controlling mechanisms within the flight controller articulate the desired motion from the UAS handler to the individual motors on the UAS platform. To achieve this, the flight controller can employ instruments such as Electronic Speed Controllers to articulate the speed from the GCS to the UAS platform motors, while relying on the aforementioned sensors to provide feedback to the handler regarding the status of the flight.

4.2.3 Flight Controller – Modification Through Programming

The firmware associated with UAS operations is most often coded in lower level programming languages such as C or C++. The firmware is associated with the coordination of UAS internal functionalities and their interoperability to support flight operations. At this layer, there exists direct communication among UAS components to support flight operations. There also exists further actions required at this layer of communication to support the req-

uisite reception, parsing, and reading of bytes from a controller to the UAS flight controller, dictating the required actions for the UAS to assume.

The Flight controller exists at a layer of programming that is most often coded in higher level languages such as Python or Java to support interoperability and ease of use by hobbyists and novices. This higher level of programming language is delineated by the associated user level applications associated with COTS UASs, allowing the operator to modify and customize flight methods. At this level of programming, the UAS is holistically functioning as a complete unit as attributed to the flight controller. Furthermore, Operations at this level of programming constitute take offs, landing, pre-programmed waypoints, semi-autonomous and autonomous operations. Further, at this level of programming, it is safely assumed the firmware is pre-configured and readily available to accept commands from a controller and subsequent flight controller.

4.3 UAS Ground Control Station

The GCS contains capabilities to support land or maritime based communications and hand-offs from one GCS to another to extend the range of operations and UAS coverage. The GCS provides human operators with the requisite foundation to control, monitor, communicate, and pilot their UASs and associated UAS payloads through data exchanges from source to destination over wireless communication standards or proprietary alternatives. These data exchanges are made possible via the C2 leveraged between the GCS and UAS.

4.4 UAS Command and Control

The UAS and its operator may leverage a variety of C2 options to support their means of controlling and monitoring the UAS, which are dependent upon the operational environment and inherent infrastructure they are confined to. These C2 options are often described as data links, but will be referred to as C2 for the purposes of this research. C2 serves as the ability to leverage the previously mentioned UAS networking architecture and GCS to receive and transmit data to and from the UAS to support telemetry, payload, and flight operations. Therefore, the main components that comprise the C2 payloads are the UAS control, video payload transmission, and the UAS telemetry.

4.4.1 Command and Control Radio Frequencies

The most common frequencies leveraged by COTS UASs to control and manage the vehicle and transmit telemetric information are 2.4GHz and 5.8GHz, similar to that of WiFi compatible devices. Other hobbyist UASs can be further modified to send and receive data within the ultra-high frequency (UHF) band between 433MHz and 915MHz. The ranges associated with C2 vary among UAS proprietary capabilities, terrain, atmospherics in an area of operation, the hardware serving as a transmitter or repeater, and the power output of the transmitters or repeaters. The range of 2.4GHz is limited to approximately one mile, which is considered line of site (LOS), and does not perform optimally well in heavily brushed areas due to the smaller, more susceptible wavelengths [71]. However, for the DJI setup using a 2.4GHz band for UAS control, one may expect up to 4 miles of range [52]. The most common video payload transmission C2 frequencies are 1.3GHz, 2.4GHz, and 5.8 GHz. 8GHz serves as the most popular commercial C2 frequency due to its high data rate capacity; however, it is hindered due to its shorter wavelength property and therefore generally limited to about 5 miles of range. The most common telemetric C2 frequencies are 400MHz and 900MHz due to their extended range capability, ability to penetrate obstructions, and lower probability for data loss; although they also have narrow bandwidth and data rate restraints to the longer wavelengths [52]. The ranges associated with these telemetric frequencies can expected be between 19 miles and 50 miles based on transmitter power output [72]. C2 frequencies are of particular interest for CUAS technologies, as denying the communication link to the operator inhibits control of a device.

4.4.2 C2 Varieties and Security

UASs leverage varying means of C2 to support the transfer and dissemination of data during flight and payload operations. In this case, we shall summarize the security of Bluetooth, WiFi, common virtual private network (VPN) options, cellular, and proprietary software leveraged to support data transfers between the UAS and GCS. As with C2 radio frequencies, security on the C2 channel is of particular relevance for CUAS technologies since breaking the security layer would provide the CUAS with control of the hostile device.

4.4.2.1 Bluetooth

Bluetooth serves as a means of short range wireless technology operating in the UHF portion of the RF spectrum at 2.4 GHz. It allows for the exchange of data between fixed and mobile devices, and limited to short ranges in light of the radio wave length. In this regard, this means of C2 supports LOS communication; therefore point-to-point between the UAS and the GCS.

Currently, internet of things (IoT) devices use Bluetooth 5.0 as the latest version of Bluetooth wireless communication [73]. However, Bluetooth technology is backwards compatible and therefore capable of operating in a transparent manner with older Bluetooth software running on current devices. Bluetooth 5.0 observes greater speed and ranges, however, as compared to the legacy versions of Bluetooth. Data rates range around 2 Mbps and can communicate upwards of 800 feet, as compared to Bluetooth 4.0 which was capable of half the data rates and about 200 feet of range.

Bluetooth security provides the ability to support authentication and encryption, but is only device specific and not user specific [74]. This authentication is based on the secret link key created and shared between paired devices. This secret key is necessary during the paring process between the devices attempting connection. Bluetooth insecurity arises from the inability to protect the integrity and authenticity associated with Bluetooth keys. Legacy Bluetooth capable devices leveraging versions 5.0 or previous are subjected to key vulnerability attacks such as the BLURtooth attack, which takes advantage of the cross-transport key derivation (CTKD) component during the paring process [75]. This vulnerability causes the potential for the Bluetooth key to be overridden and usurped thereafter by potential attackers, allowing for subsequent man-in-the-middle (MITM) attacks. However, rudimentary versions of Bluetooth such as versions 1.0 or 2.0, which did not require key authentication upon pairing, are extremely susceptible to security vulnerabilities that allow for basic exploitation by an attacker in range of the devices, leading to eavesdropping of data exchanges, denial of service (DoS) by preventing services from running as designed, or MITM attacks [76].

4.4.2.2 WiFi

Most COTS UASs either use WiFi or are WiFi enabled to support UAS payloads between the UAS and GCS. WiFi functions in the UHF portion of the spectrum and is therefore

limited by the distance it is capable of transmitting. This distance is dependent upon the version of WiFi used for C2, COTS manufacturer, and use of after market gear such as amplifiers, but is typically about 1 kilometer commercially [77].

802.11 WiFi serves as a wireless RF capability enabling the communication between smart devices over the internet. The frequency bands associated with WiFi use are 2.4 Ghz and 5 GHz. 802.11 serves as a cadre of variances amongst wireless local area networks. Within this cadre of wireless interfaces between clients and base stations are the following WiFi standard specifications leveraged as C2 for COTS UAS controls using 802.11, 802.11a, 802.11b, 802.11n, 802.11ac, and 802.11g [78]:

- 802.11: The most basic wireless means of communication over the internet through a local area network (LAN), functioning at the 2.4 GHz band. 802.11 provides between one to two Mpbs of data transmission and leverages frequency hopping spread spectrum (FHSS) technology or direct sequence spread spectrum (DSSS) technology as a means protection from electromagnetic interference (EMI), jamming, or exploitation. FHSS allows for the rapid changing of a carrier's frequency while transmitting data over the prescribed radio signal. The carrier's frequency is changed based on the use of a predetermined algorithm that is shared between the receiver and transmitter. DSSS achieves this reduction in potential for signal interference by modulating the bits associated with the data and altering the size of the transmitted signal to be wider in bandwidth than the actual data or information being transmitted.
- 802.11a: Serves as an upgraded extension to the legacy 802.11 infrastructure, operating in the 5 GHz band and allowing for the transmission of data at rates as fast as 54 Mbps. 802.11a uses orthogonal frequency division multiplexing (OFDM) vice DSSS or FHSS. This method of encoding is leveraged against data on multiple carrier frequencies, vice a singular carrier frequency. It provides similar protections against EMI, jamming, and exploitation, while protecting against more severities associated with attenuation and multi-path interference.
- 802.11b: Serves as a high data rate extension to the 802.11 wireless LAN over the 2.4 GHz band. 802.11b allows for the transmission of up to 11 Mbps and makes use of the DSSS for data encoding.
- 802.11g: Serves as upgraded extension to the 802.11 wireless LAN over the 2.4 GHz band. 802.11g allows for data transmission speeds in excess of 20 Mbps and leverages

the OFDM for data encoding.

- 802.11n: Serves as the upgraded extension to 802.11g, operating at either the 2.4 GHz or 5 GHz band and allowing for increased data transmission speeds up to 600 Mbps. Its intent was to serve as a means of keeping pace with the technological demands of equipment and software capabilities, to include video transmission and streaming. Similar to 802.11g, it makes use of OFDM for encoding, as well as DSSS. 802.11n is also backwards compatible to the legacy version of 802.11 to support software interoperability.
- 802.11ac: serves as yet another improvement to data transmission speeds, operating at the unlicensed band of 5.8 GHz. It is primarily leveraged as the C2 between smart phones, WiFi televisions, and video game consoles to support the high data rate demands associated with the devices and their inherent services. 802.11ac provides for data rates of transmissions between 1 Gbps to 7 Gbps. 802.11ac introduced the use of binary phase shift keying (BPSK) and quadrature phase shift keying (QPSK) for encoding. BPSK achieves encoding by representing the binary 0 and 1 in a transmission by two different states in the associated carrier signal in transmission. QPSK achieves encoding by modulating two bits at once during phase shift keying and selecting one of the four possible associated carrier phase shifts for transmission. Both allow for the transmission of more data at once, with QPSK providing for twice the amount of data transmission than BPSK.

COTS UAS furthermore typically make use of 802.11s for C2 when using WiFi [79]. 802.11s supports communication between two end systems through the interaction of airborne relays serving as a mesh network. However, 802.11s makes use of the legacy 802.11 services to support the actual transmission of the data between two end systems.

To support the encryption and protection of data in transit, WiFi makes use of wired equivalent privacy (WEP), WiFi protected access (WPA), WiFi protected access 2 (WPA2), and WiFi protected access 3 (WPA3) as the most prevalent protocols to support data encryption:

- WEP: Serves as the most common encryption protocol available to 802.11a and 802.11b LAN [79]. WEP makes use of the RC4 cipher stream [80]. WEP provides base 40 or 104 bit encryption with use of a static encryption key of 64 or 128 bits

that must be manually entered on wireless access points and is unchangeable [80]. However, WEP's rudimentary principles make for a weak encryption algorithm and is therefore legacy in nature. These weaknesses are attributed to its small key size, small initialization vector, and ability to easily forge authentication messages.

- WPA: Leverages the WEP functionality while employing temporal key integrity protocol (TKIP), which generates a new 128 bit key on the fly for each packet of data transmitted between two end devices [80]. WPA also introduces integrity check as a means of preventing potential attackers from intercepting and altering the data transmitted between two devices. However, WPA2 is vulnerable to replay attacks, allowing for a potential attacker to replay messages sent between two end devices, steal credentials, and serve as a MITM for subsequent attacks.
- WPA2: Serving as the successor to WPA, WPA2 employs the mandatory use of the advanced encryption standard (AES) for encryption. AES makes use of varying key sizes, 128 bit, 192 bit, or 256 bit [80]. It encrypts data through the use of sending the encrypted source data into the cipher text and cumulatively through a NAND gate for storage and transmission. Use of the AES 256 bit is advertised as impenetrable to brute force attacks due to the amount of time required to break the encryption. However, WPA2 is vulnerable to key re-installation attacks, which employs a replay attack during the initial four-way handshake of the protocol while in proximity of the wireless network. This vulnerability also leads to the aforementioned MITM attack.
- WPA3: Replacement to the WPA2 protocol. WPA3 employs a 192 bit encryption and replaces pre-shared keys from the previous encryption protocols with simultaneous authentication of equals (SEA) [80]. SEA provides for better security in key exchanges and is compatible with the introduced 802.11s WiFi standard used by UAS.

4.4.2.3 Cellular

The use of cellular infrastructure to support UAS C2 can provide for operations BVLOS through daisy chain-like operations through the use of BTS [81]. Cellular networks serve as high speed and high data capacity application to support the exchange of data between two or more end devices. The incorporation of BTSs in the C2 architecture for UAS data exchanges includes the use of cellular communications such as 2G GSM; 3G CDMA, TDMA, and FDMA; 4G LTE; and 5G. The use of the legacy 2G architecture for UAS C2 is exemplified through the example implementation of using an Android OS and proprietary applications

associated with the UAS to communicate with a UAS via a GSM modem onboard serving as a payload [82]. The use of the 3G and 4G C2 architectures to support UAS control is made feasible through the subsequent payload addition of onboard 3G or 4G receivers, as found in the quality of service research conducted by Aalto university [83]. Lastly, the potential use of 5G to operate COTS UASs was identified to be feasible, attainable, and help augment UAS distance to BVLOS, improve data latency required for high demand UAS payloads, and support semi autonomy or full autonomous operations [84]. The functionality of a cellular network consists of the GCS, which in this instance is the smart device used to control the UAS, the BTS, relays as appropriate, and the end device. The BTS encompasses the cellular service providers associated towers to support user connectivity and data exchanges. The varying types of security pertaining on cellular networks are identified in chronological order of introduction to the commercial market as 2G, 3G, 4G, and 5G:

- 2G: 2G GSM serves as the most primitive in current digital cellular communications, providing for rudimentary send and receipt of of voice calls and simple messages between mobile telecommunication and smart devices. 2G served as the first concept employing multiplexing for mobile communications, allowing for multiple users to leverage a single channel to exchange data [81]. 2G leverages circuit switching for the delivery of data between end devices. 2G allows for speeds up to 64 Kpbs, with a purported bandwidth of 25 MHz. 2G operates in narrowband for the provision of internet services.
- 3G: 3G Universal Mobile Telecommunications System (UMTS) expounds upon the infrastructure of 2G to provide increased data rates between end devices, leveraging packet switching. 3G allows for voice and message exchange, in addition to video and GPS use [81]. 3G operates at a range of 2 GHz with a bandwidth of 15 MHz to 20 MHz [81]. 3G provides data rates up to 2 Mbps and allows for the receipt and transmission of larges data through its increased capacity. 3G operates in the broadband for the provision of internet services.
- 4G: 4G LTE and WiMAX achieve improved data rate speeds from it 3G predecessor with its incorporation of OFDM and multiple input multiple output (MIMO) technology [81]. 4G serves as the current standard for mobile telecommunications in regards to data rates and security. 4G's application expounds upon 3G with support to application requiring high data rates, to include mobile TV. It provides data rate

speeds up to 20 Mbps and allows for the inclusion of multi hop networks, allowing for the use and inclusion of adhoc networks to support daisy chain operations to elongate the range of coverage between end devices [81]. 4G has a bandwidth of up to 100 MHz [81]. 4G operates in ultra broadband for the provision of internet service.

- 5G: 5G is the latest technology in commercial mobile communications, providing increased speeds and reliability through the use of MIMO, OFDM, and millimeter wave technology. 5G operates in the band of 30 GHz to 300 GHz, adding to the appeal of use due to the rare application of these bands. 5G makes use of small cell technology and beam forming to add to the increased coverage of an area and reduction in latency. 5G also support network slicing, which allows for the provision of tailorable services to an operators need to support dynamic application in an area of interest. 5G's application expounds upon 4G with higher resolution, less latency, and support to the control of unmanned assets such as UASs. 5G operates in the wireless world wide web for the provision of interest services.

Cellular encryption varies based upon the service used. It is therefore dependent upon the service used and shall be discussed by service. Cellular encryption is attained via the following means:

- 2G: Encrypted data over the network is accomplished through the use of the A5 algorithm [81]. A5 is a family of algorithms ranging from no encryption (A5/0) to the strongest encryption (A5/3). A cipher mode request us used to initiate the request for encryption across the network between end devices. The use of the A5 algorithm and corresponding cipher key is used to encrypt and decrypt traffic between devices. The A5/1 algorithm is a 64 bit key capable of encrypting bits as they are received [81]. The A5/3 algorithm however uses a block cipher and leverages a 128 bit key [81]. The A5 algorithm is vulnerable holistically to MITM attacks due to the weakness of the keys with modern password breaking techniques, or through key differential attacks [81].
- 3G and 4G: Encrypted data over the 3G and LTE network is accomplished by means of a 128 bit AES algorithm, which is capable of leveraging a 128, 192, or 256 bit key [85]. However, the WiMAX network makes use of the 168 bit digital encryption standard (DES) to support encryption of over the air transmissions [85]. To achieve encryption over the air, the 3G and 4G networks leverage transport layer security

(TLS) [85]. TLS provides the requisite confidentiality and data integrity between applications running on end devices communicating across a network. Although shorter key lengths are vulnerable to attacks related to brute force, dictionary, replay, or MITM, the AES 256 bit key length serves as a current Internet Engineering Task Force (IETF) standard [85].

- 5G: Encrypted data over the 5G network is accomplished by means of a 256 bit AES encryption, while also encrypted the users identity while being transmitted juxtaposed to the predecessor 2G, 3G, and 4G services [86]. However, 5Gs shift from hardware based architectures to the software defined network (SDN) concept through its implementation of small cell technology to increase coverage areas pushes the protection requirements to the software and end devices, as well as the rest of the architecture. This broadly increases the attack surface area. Furthermore, like its predecessors, 5G lacks the end-to-end encryption of data transmitted over the air, making interception and exploitation of data still a possibility [86]. Due to 5G's shorter range using millimeter wave technology, more cell towers will need to be placed to support coverage and potential network slicing capabilities [86]. This further increases the attack surface area for potential exploitation.

4.4.2.4 Satellite Communications

SATCOM is used to support BVLOS C2 for UASs in an area of operation, due to the inability or inefficiency associated with the aforementioned LOS communications. In this regard, communication capable satellites serve as relays to amplify the broadcasted RF between the GCS and UAS to support flight or payload operations. Associated SATCOM satellites are typically in either geostationary orbit (GEO) or low earth orbit (LEO). The utilization of GEO provides sustained, steady-state coverage. However, GEO satellites are encumbered with potential latency issues due to the greater distance from Earth. LEO satellites provide less latency but less sustainability due to their short dwell time over a given region on Earth's surface. The associated frequency bands provided by SATCOM in these orbits vary between L-band, S-band, C-band, X-band, Ku-band, and Ka-band dependent on order of wavelength size and frequency [87]. Expectedly, smaller wavelengths and higher frequency bands allow for less susceptibility to exploitation during over-the-air transmission and a higher bandwidth due to the availability of more channels, but are encumbered with more potential to interference by atmospheric and man-made RF. Higher frequency bands are

less susceptible to exploitation due to the requirement of exploitation techniques to be in a closer proximity to collect the signal while being transmitted over the air, due to the small wavelength properties associated with it.

Commercial satellite communications practice encryption at the network layer to ensure data is protected during transmission between the satellite and terrestrial devices [51]. To minimize the issues associated with encryption and the potential for signal degradation due to distance related attenuation, natural interference due to weather, or man made interference, keyed encryption or asymmetric keys encryption is leveraged.

4.4.3 C2 Employment

The type of C2 employed for UAS communication is based on the underlying networking infrastructure restraints of an environment. The C2 employed for UAS operations can further be codified in terms of the amount of latency and reliability that is tolerable and acceptable for operations, as well as compatible with the UAS. Of the variances of C2, UASs are reliant upon communication employment options using primarily three types of networking options:

4.4.3.0.1 UAS-to-UAS UAS-to-UAS is a steadily evolving concept, some leveraging machine learning techniques or automation through pre-programming applications to support swarm UAS tactics and protocols. Particularly, the use and implementation of neural networks-based machine learning in tandem with supervised learning models are leveraged to create, support, and adjust an intelligent UAS's wireless communication architecture [88]. UAS-to-UAS C2 allows for daisy-chaining with one or multiple UASs serving as relays between the GCS and a controlled vehicle for the purposes of supporting subsequent flight or payload operations. Characteristics associated with UAS-to-UAS communications vary within the ultra-high frequency and super high frequency ranges of the RF spectrum, with all UASs operating on the same chosen frequency. Further, all UASs within the swarm or cluster operate from the same chosen GCS. Example of this type of C2 is illustrated in Figure 4.2:

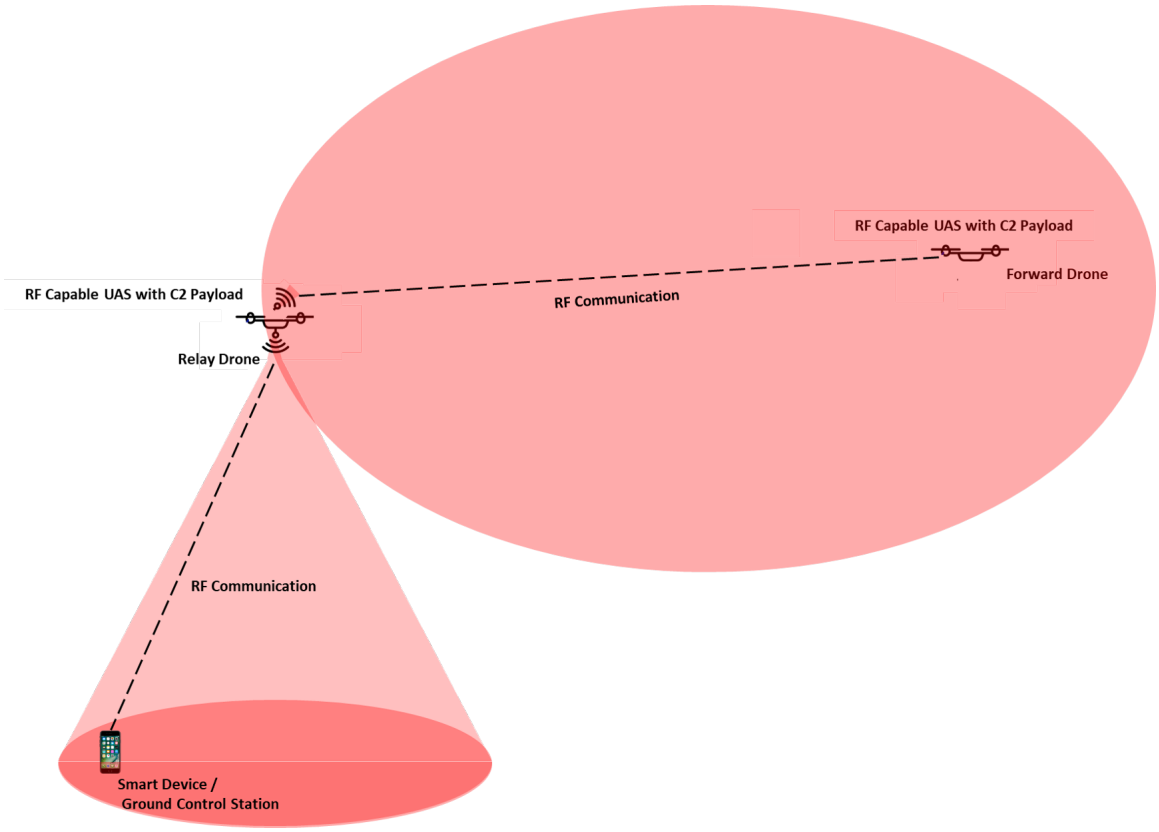


Figure 4.2. Example UAS-to-UAS C2 Architecture.

4.4.3.0.2 UAS-to-Ground Control Station The use of ground stations leverages preexisting technology associated with mobile, cellular communications. This method further leverages standard and proprietary protocols associated with wireless and cellular communications, as mentioned previously, depending on the geographic region hosting the service and the UAS's underlying C2 architecture. This C2 serves as the link to manage the flow of data between the UAS and the corresponding GCS that is within its navigational area based on terrain, distance from the GCS, and associated signal strength. The UAS distance from the GCS is categorized as within VLOS. VLOS implies C2 is exercised from the GCS to the device directly. The use of multiple ground stations serving as relays support the ability to control UASs BVLOS through the use of hand-offs with surrounding ground stations along the point of intended movement for the UAS [89]. This terrestrial relay technique is often referred to as 'daisy chaining' and is therefore an indirect form of communication from the ground controller to the UAS. This operation using cellular means of communication is

exemplified in Figure 4.3.

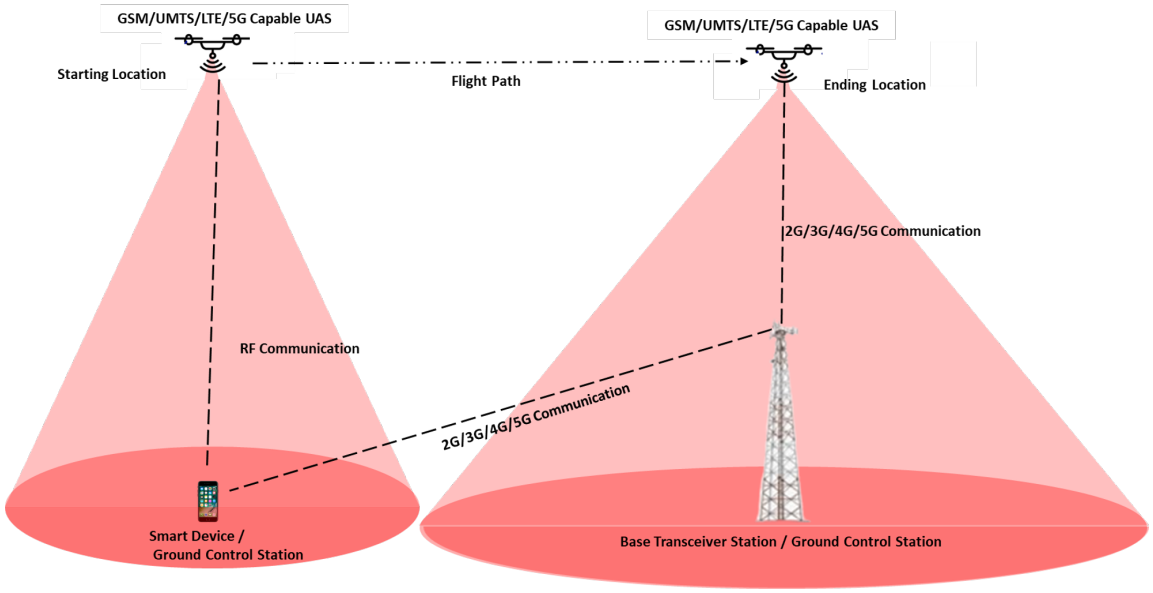


Figure 4.3. Example UAS Cellular C2 Architecture.

The C2 connection between the ground operator and UAS, and the associated data rate between them is dependent upon the level of autonomy desired for the UAS to operate. More autonomous systems require less data transfers between the operator and UAS. Conversely, semi-autonomous or complete user control require more data transfers that induce more latency due to the higher demands placed on bit rates. Semi-autonomous or complete user control missions require data transfers between the C2 architecture for operations to include hovering, landing, take-off, point-to-point navigation, telemetric data, and more. Such information inherently induces more latency across the perspective medium used for C2. However, data within completely autonomous systems includes mission-oriented details associated with navigating to specific coordinates and returning to a point of origin, as well as telemetric data associated with the flight and vehicle status. This information and associated data can be directly preprogrammed on a UAS's flight controller, or in this regard, it can be sent to the flight controller over the selected means of C2 using a smart device such as a tablet, smart phone, or laptop. As anticipated, less bandwidth requirements are required for fully autonomous UASs.

4.4.3.0.3 UAS-to-Satellite Communication The use of SATCOM enables the UAS operator to command and control the UAS BVLOS without the limitations of relying on a link to the GCS or other associated communication architectures in the geographic area. The use of SATCOM allows for the ability to relay and amplify radio or microwave frequencies and therefore data between the UAS and the GCS.

While operating within VLOS, a UAS is able to use direct radio waves to transmit flight control data between the UAS and the GCS (and consequently to the human operator for control and navigation). While operating BVLOS, the UAS requires controlled hand-offs between SATCOM to support extended coverage and subsequent communication between surrounding GCSs and human operators. The employment of SATCOM requires the UAS be physically located within the footprint of the satellite coverage area, which therefore requires more coordination and reliance on factors that cannot be manipulated by a rudimentary operator.

An example of common, commercial SATCOM coverage arrives in the form of companies such as Honeywell. Honeywell's SATCOM serves as a lightweight, compact means of providing SATCOM communications to small UASs by interoperating with INMARSAT's SwiftBroadband services [90]. The use of this provides long range C2 while delivering the capabilities such as real-time video, navigational waypoints, and telemetry data. The use of SATCOM to support C2 between a GCS and UAS is illustrated in Figure 4.4.

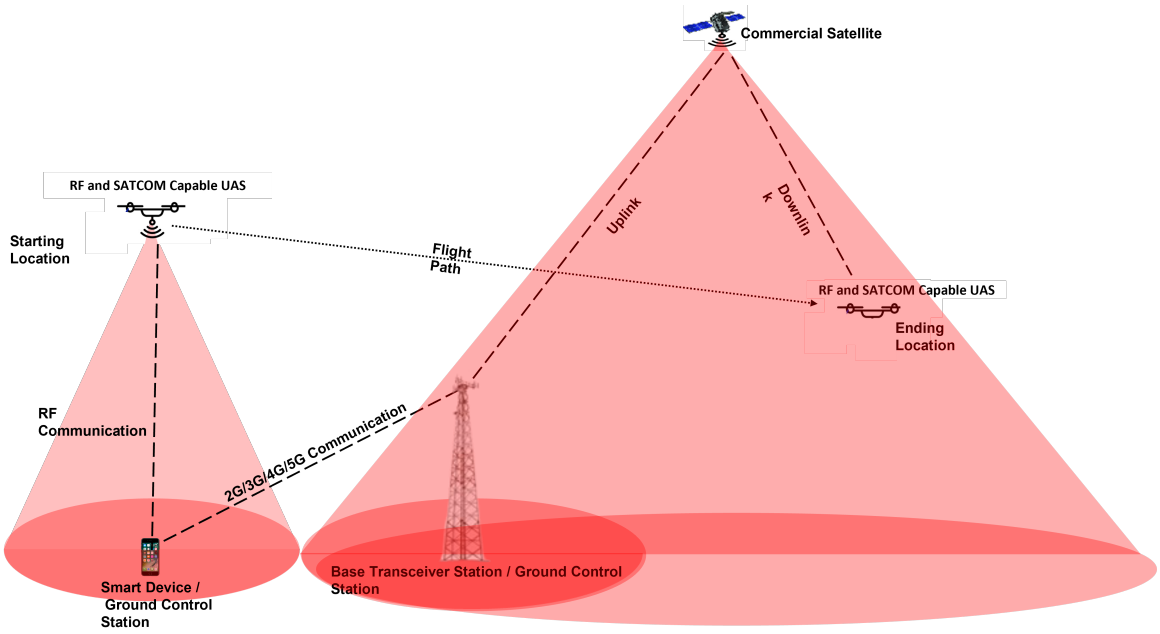


Figure 4.4. Example UAS SATCOM C2 Architecture.

Separate from the above-mentioned C2 links for operator control, there also exists the ability for a UAS to operate semi-autonomously under waypoint navigation. The use of waypoint flight navigation allows the UAS operator to pre-program sequences of actions for a UAS to assume based on topographic features, navigational locales, or infrastructural landmarks. This method of flight operation allows the UAS to fly semi-autonomously on a flight route as chosen by a UAS operator, limiting C2 link communication need.

4.5 DJI UAS Case Study

To exemplify the programmable and modifiable means of the aforementioned UAS operations pertaining to the flight controller and GCS, we shall leverage the highly popularized and widely used DJI UAS as a case study example.

4.5.1 Flight Controller – Usurpation Through Vulnerabilities

Flight controllers often leverage C2 links that are neither secured or encrypted to support the commercialization and mass dissemination of the onboard products. This lack of security and oversight by vendors and subsequent UAS operators can yield the inherent potential for

surreptitious usurpation of the UAS by means of exploitation or denial of service achieved by means of CUAS products. Examples of inherent Group 1 UAS vulnerabilities can be seen with the COTS DJI Phantom 3. Commercially, the DJI Phantom 3 arrives as a UAS vehicle with pre-programmed flight controller internals, a handheld remote controller for piloting, and an Android or iOS application for synchronization with a smart device to support the transfer of telemetry information. The frequency range is between 2.4 GHz to 2.483 GHz, where the controller in this regard serves as the requisite access point for UAS C2. When the DJI Phantom 3 is utilizing WiFi services, a basic network mapper (NMAP) scan reveals the following information pertaining to the flight controller as delineated in Figure 4.5 [91].

```
Nmap scan report for 192.168.1.1
21/tcp   open   ftp        syn-ack      vsftpd 3.0.2
22/tcp   closed ssh        conn-refused
23/tcp   closed telnet     conn-refused
2345/tcp open landesk-rc syn-ack LANDesk remote manage
5678/tcp closed rrac       conn-refused

Nmap scan report for 192.168.1.2
21/tcp   open     ftp        syn-ack     vsftpd 3.0.2
22/tcp   filtered ssh        no-response
23/tcp   filtered telnet     no-response
2345/tcp filtered unknown    no-response
5678/tcp open     tcpwrapped syn-ack

Nmap scan report for 192.168.1.3
21/tcp   open  ftp syn-ack BusyBox ftpd
(D-Link DCS-932L IP-Cam camera)
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| total 0
| drwxr--r-- 2 0 0 0 Dec 23  2016 DCIM
| drwxr--r-- 6 0 0 0 Dec 23  2016 MISC
|_drwxr--r-- 2 0 0 0 Dec 23  2016 System Volume Infor..
22/tcp   open  ssh     syn-ack OpenSSH 6.2 (protocol 2)
23/tcp   open  telnet  syn-ack BusyBox telnetd
2345/tcp filtered unknown no-response
5678/tcp filtered rrac    no-response
```

Figure 4.5. DJI Phantom 3 NMAP Results. Source: [91].

Of the services discovered from the NMAP scan, the file transfer protocol (FTP) and Telnet services present a significant vulnerability due to their open, unencrypted connections to the network if no security layer is used. Furthermore, the FTP connection's allowance of

anonymous logins affords even benign operators the ability to surreptitiously login and commit FTP related attacks against the UAS. Such deliverance of payloads via a vulnerable FTP server can yield credential harvesting and subsequent MITM attacks that allow for the potential of the UAS to be remotely usurped. The open Telnet service presents another significant vulnerability to the UAS and flight controller. Telnet serves as an application layer based protocol on a local area network to support bidirectional text communication. In this regard, it supports the communication between the operator or controller to the flight controller onboard the UAS. This connection is facilitated using a virtual connection known as Telnet. By re-enabling the Telnet services during the boot process, one may ascertain the flight controller's underlying system; therefore gaining the ability to usurp the UAS remotely, gain root level access to the UAS, and subsequent root level access to the underlying subsystems associated through the flight controller [91].

4.5.1.1 DJI Command and Control Constraints Exemplified

The use of specific C2 by varying manufacturers is exemplified by the DJI and its COTS UAS employment of the 2.4 GHz DataLink3 technology [92]. This form of C2 is intended to be interoperable with the DJI ground station, which can be a manufactured DJI DataLink3 controller, any smart device with the DJI application, or a personal computer leveraging the DJI application programming interface (API) and associated programming methods. The DataLink3 controller provides users with a default option of 2.5 mile controllable ranges and 15 hours of battery life to support UAS dwell times. Furthermore, the DataLink3 provides more security from jamming and EMI by using frequency-hopping spread spectrum technology. Additionally, the narrower bandwidth plays a positive role against the potential of interference from other common household and civilian devices that make use of the same 2.5GHz frequency band for operations. The DJI DataLink3 default remote controller is interoperable with third-party software and hardware, as long as they utilize the requisite serial bus protocol [92].

The serial bus protocol used by DJI serves as a digital communications protocol using digital, serialized data to transmit control related signals between receivers and transmitters. The serial bus protocol represents the most widely used remote control protocol amongst consumer devices and COTS UAS receivers [93]. The serial bus protocol is a digital protocol. It further carries the ability to transmit up to 16 channels with equal bands of

100Hz, which can be further codified down to enabling the 2048 different values in bits on each channel as denoted in Figure 4.6.

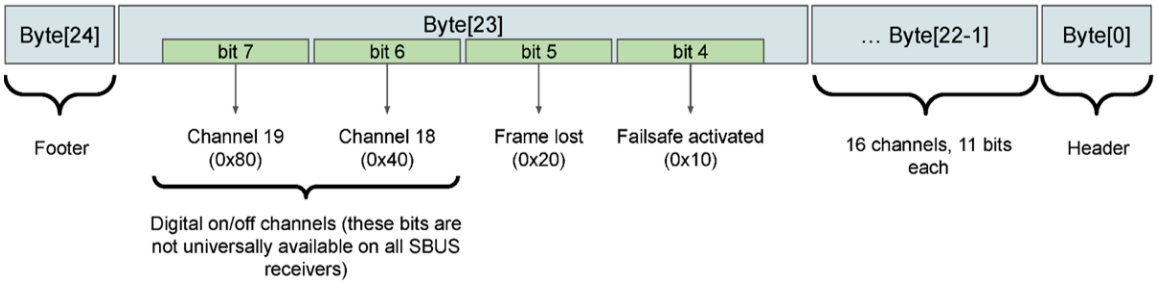


Figure 4.6. Serial Bus Data Frame. Source: [93].

As delineated in Figure 4.6, byte 0 pertains to the header information of the data being transmitted from the UAS operator controller to the flight controller, bytes 1 through 22 pertain to the data being transmitted to control the UAS, byte 23 contains optional data, and byte 24 contains the footer to conclude the message. Each channel pertaining to the data transmitted between the UAS operator controller to the flight controller in bytes 1 through 22 can carry 11 bits each. Base 2 operation therein provides a maximum of 2048 different values capable of being stored in command send and receive messages between the UAS controller and flight controller to support UAS flights and missions.

4.5.1.2 Command and Control Constraints

Aside from distance and reliability, another constraint associated with C2 pertaining to UAS operations is the interface related to the UAS and the ground operator. The interface ties the data required to be transmitted between the uplink and downlink to the operator and UAS [94]. This interface is exemplified by either benign push-button missions or more detailed and intrusively controlled missions that leverage semi-autonomy or full control from the user. These push-button missions will inherently require smaller data frames and leverage higher-level commands to support mission related tasks, and not require user input to control flight path, altitude, speed, and other related tasks through an uplink connection to the UAS. Further, user interfaces typically do not require larger data frames as they are often sporadic in nature and with less information sent in an uplink to the UAS. Regardless of the means of communication used by the UAS to support operations and receipt of commands,

the presence of a downlink and uplink for relaying and receiving information is forever present. Every UAS passes several parameters to support the sustainment of operations in flight and mission requirements. The parameters pertaining to a UAS depend on the number of UAS engines, mission, and optional add-on capabilities such as full motion video.

4.5.1.3 Downlink

The UAS downlink is leveraged to relay telemetric data to the UAS operator to support situational awareness of the UAS flight status, health, and receipt of commands. A typical message pertaining to the basic necessities of UAS flight parameters passed over the C2 network are standard in nature. These standard parameters are provided below, with exemplified contents pertaining to the parameter [95]:

Type Name: Enemy_UAS_Op1

BEGIN HEADER()
- time 16:35:23.100
- date 20071114
- uas_id GB_123_ABC
- msg_num 133
- msg_version 1.21

END HEADER()
- exit

BEGIN INERTIAL MANAGEMENT UNIT()
- gyro_x 23.105
- gyro_y 13.243
- gyro_z 12.596
- accel_x 3.933
- accel_y 0.022
- accel_z 0.223
- mag_x 15.877
- mag_y 225.112
- mag_z 8.254
- inclin_y 1.989

- inclin_z 3.850
- temp 11.213

END INERTIAL MANAGEMENT UNIT()

- exit

BEGIN FLIGHT CONTROL UNIT()

- ENGINE ON()
  - uas_id 1
  - set_speed 13000
  - actual_speed 14321
  - carb_setting 12.3
  - carb_actual 13.3
  - temp 105.2
  - fuel_flow_rate 23.23
  - vibration 12.22
  - cum_hours 128.77
- ENGINE OFF()
  - exit
- ENGINE ON()
  - uas_id 2
  - set_speed 13000
  - actual_speed 14321
  - carb_setting 12.3
  - carb_actual 13.3
  - temp 105.2
  - fuel_flow_rate 23.23
  - vibration 12.22
  - cum_hours 128.77 enditemize
- ENGINE OFF()
  - exit

Source [95].

This exemplified telemetric UAS message is approximately 3600 characters in length, which computes to 3600 bytes in length [95]. The message contains notifications pertaining

to the UAS flight path, altitude, speed, temperature, payload, and heading. These parameters are public methods for a UAS and support software associated with the flight control unit, inertial navigation movement, GPS, and UASs' ability to leverage sensing of the operational environment to avoid obstacles based on terrain. This message serves as a service list for the native software running on the UAS platform, communicating over a defined network as a medium. The data abstractions pertaining to the parameters is a generic description of the overarching hierarchy affecting the functionality required to support generic UAS operations. The outputs serve as the requisite telemetric data the operator needs to support their situational awareness of the piloted UAS, as well as the ability to make corrective actions during flight via the uplink. This example service list, although not completely inclusive, supports the construct required to enable a manual, non-autonomous UAS's flight. The universality of this message type implies that UASs operating with additional features, such as video streaming, would require additional parameters and therefore the passage of more data in the form of methods associated with their inherent class. Such additional details in data warrant the requirement for more bandwidth across the medium that is leveraged for UAS C2.

4.5.1.4 Uplink

Conversely, the uplink is used by the ground operator to control the UAS or UASs by means of adjusting or altering their flight path or mission requirements. Typical UAS flight plan parameters will therefore consist of telemetric data associated with waypoints, altimeter readings, GPS inputs, flight controls, and camera movements. An example of this uplink message is provided [95]:

Type Name: Enemy_UAS_Op1

BEGIN INIT()

- Test_MobileTelemetry
- Test_CommunicationLink
- Test_NetworkLink
- Test_FuelReading
- Test_Battery
- Test_Engine

- Test_Flaps
- Test_CameraPower
- Test_CameraTilt

END INIT()

BEGIN LEG_01

- Duration 00.00.00
- MaxFuelEfficiency
- BEGIN Camera
  - Camera_Type DELL_HP
  - Angle 180
  - Compass 45
  - MTS 250
- END Camera

END LEG_01

BEGIN WAYPOINT 1

- MGRS 4QFJ12345678
- Altimeter 200
- SEND Telemetry

END WAYPOINT 1

BEGIN LEG_02

- Duration 00.00.00
- MaxFuelEfficiency
- BEGIN Camera
  - Camera_Type DELL_HP
  - Angle 180
  - Compass 45
  - MTS 250
- END Camera

END LEG_02

Source [95].

The content of this exemplified message represents uplink parameters leveraged to control the UAS. A typical uplink message is therefore usually greater than 1000 bytes in length

based on mission complexity and requirements by the operator [95]. There exists no standard format or requirement for specific uplink message parameters to occur for every variant of UAS. Therefore, there exists no standard rate for updating these messages between the ground controller and the UAS. However, UASs that are operating using GPS waypoint navigation receive update messages between every one to ten seconds, based on the GPS receiver and necessity to update waypoints for potential error correction [95].

4.5.2 Ground Control Station Modification – DJI Employment Example

Exemplary to the DJI UAS, it provides UAS operators the ability to leverage APIs associated with the DJI library to augment, modify, and customize flight operations. Upon downloading the associated UAS user level application on any smart device, one is able to connect and interact with the UAS after importing the associated libraries pertaining to the UAS and connecting to it through the establishment of an object, as demonstrated in the Figure 4.7.

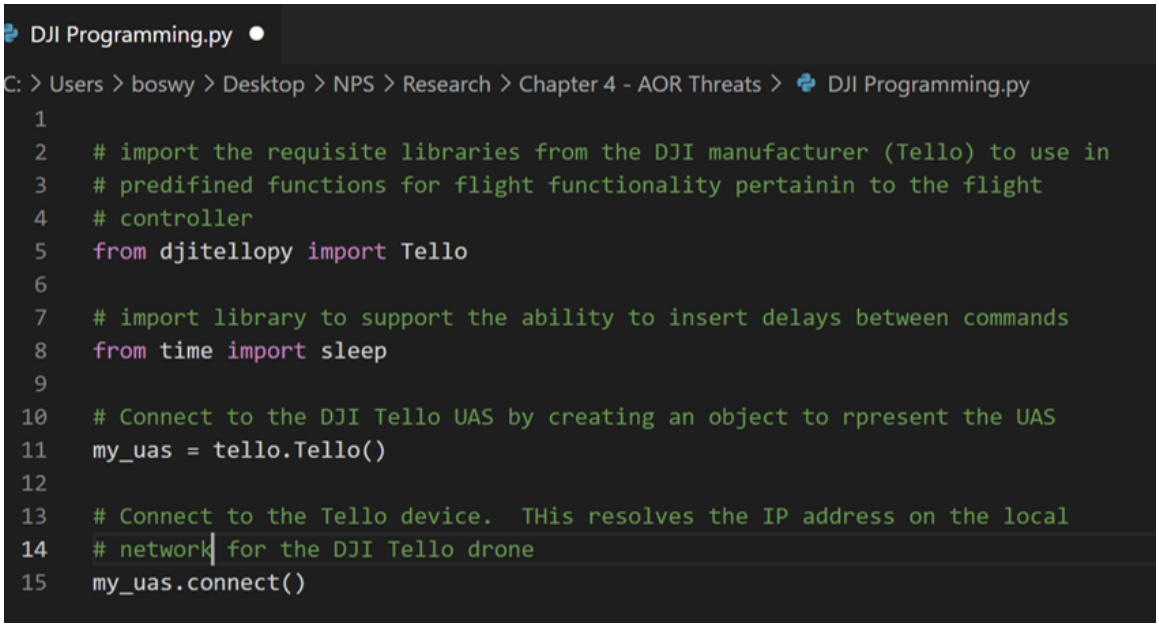


Figure 4.7. DJI Drone Python Setup. Adapted from: [96].

In this regard, the UAS Tellos object is instantiated through the creation of a variable called my_uas. This variable then allows the UAS operator to leverage the associated li-

brary function from the DJI Tellos API. These functions serve as DJI's software development toolkit, which provides the requisite operating system, hardware platform, and programming language to create the desired user behavior for the drone. It further allows for the modification of the flight profiles pertaining to the UAS, to include speed, altitude, yaw angle, pitch angle, and camera settings. In Figure 4.7, the use of the connect() function for the created my_uas object leverages the following DJI API source code to connect to the drone per Figure 4.8.

```
def connect(self, wait_for_state=True):
    """Enter SDK mode. Call this before any of the control functions.
    """
    self.send_control_command("command")

    if wait_for_state:
        REPS = 20
        for i in range(REPS):
            if self.get_current_state():
                t = i / REPS  # in seconds
                Tello.LOGGER.debug("'.connect()' received first state packet after {} seconds".format(t))
                break
            time.sleep(1 / REPS)

        if not self.get_current_state():
            raise Exception('Did not receive a state packet from the Tello')
```

Figure 4.8. DJI Drone Connection API. Source: [96].

Following connection to the UAS using Python programming and the associated DJI API library, one may make customized modifications to the vehicle's flight planning through use of subsequent UAS control functions. These functions carry the resident parameters associated with takeoff, landing, moving forward, backwards, counter clockwise, and clockwise by numerical measurements associated with centimeters by default. These functions are thereafter called in the DJI UAS's send() and receive() functions to transmit the data calls from the GCS to the onboard flight controller. As contemplated, if a terrain is previously mapped or known by an operator, pre-planned waypoints may be used as inputs to these DJI functions, thereby removing the need for sustained C2 between the UAS and a GCS and allowing for the vehicle to operate semi autonomously. Use of the send() and receive() functions is represented in Figure 4.9.

```
# Send the message to Tello and allow for a delay in seconds
def send(message, delay):
  # Try to send the message otherwise print the exception
  try:
    sock.sendto(message.encode(), tello_address)
    print("Sending message: " + message)
  except Exception as e:
    print("Error sending: " + str(e))

  # Delay for a user-defined period of time
  time.sleep(delay)

# Receive the message from Tello
def receive():
  # Continuously loop and listen for incoming messages
  while True:
    # Try to receive the message otherwise print the exception
    try:
      response, ip_address = sock.recvfrom(128)
      print("Received message: " + response.decode(encoding='utf-8'))
    except Exception as e:
      # If there's an error close the socket and break out of the loop
      sock.close()
      print("Error receiving: " + str(e))
      break

# Create and start a listening thread that runs in the background
# This utilizes our receive functions and will continuously monitor for incoming messages
receiveThread = threading.Thread(target=receive)
receiveThread.daemon = True
receiveThread.start()
```

Figure 4.9. DJI Drone Receive and Transmit Functions. Source: [97].

After setting the requisite send() and receive() functions for between the UAS operator controller and UAS flight controller, all that is required is to leverage the preexisting DJI API to manually input the desired waypoints, motion, and distance in centimeters in the associated send() and receive() functions, as delineated in Figure 4.10.

```
# Each leg of the box will be 100 cm. Tello uses cm units by default.
box_leg_distance = 100

# Yaw 90 degrees
yaw_angle = 90

# Yaw clockwise (right)
yaw_direction = "cw"

# Put Tello into command mode
send("command", 3)

# Send the takeoff command
send("takeoff", 5)

# Fly forward
send("forward " + str(box_leg_distance), 4)

# Yaw right
send("cw " + str(yaw_angle), 3)

# Fly forward
send("forward " + str(box_leg_distance), 4)

# Yaw right
send("cw " + str(yaw_angle), 3)

# Fly forward
send("forward " + str(box_leg_distance), 4)

# Yaw right
send("cw " + str(yaw_angle), 3)

# Fly forward
send("forward " + str(box_leg_distance), 4)

# Yaw right
send("cw " + str(yaw_angle), 3)

# Land
send("land", 5)
```

Figure 4.10. DJI Drone Waypoint Programming. Source: [97].

4.6 Summary

This chapter details the varying means of C2 Groups 1 through 3 UASs can leverage to support flight and payload operations. It also addresses the ranges associated with UAS flight operations, and the potential for modification using the aforesaid means of C2. Furthermore, this chapter demonstrates user modification to UAS flight behaviors can be readily

accomplished through the implementation of APIs associated with the COTS UAS. Flight modification can be accomplished to support semi-autonomous behavior by the use of waypoint navigation with the same UAS library functions. This addresses our assessment of how UAS flight and payload operations can be modified to support nefarious adversarial UAS endeavors and defeat potential CUAS means of detection, tracking, and mitigation.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 5:
UAS Threats In Each Area of Responsibility

This chapter addresses the current UAS tactics used in each AOR based upon the existing communications infrastructure and the availability of COTS hardware and software. Using each AOR's projected implementation of emergent communications technology, we make assessments for the ability to support future UAS flight and payload operations.

5.1 Adversarial Tactics by Area of Responsibility

The UAS tactics used by adversaries will be evaluated in this chapter, to evaluate the threat and therefore narrow the scope of how to counter adversarial UASs with the most appropriate means of CUAS. Further, this chapter will help provide the basis of how effective our current CUAS capabilities are against current and emerging UAS threats posed by actors in differing AORs. Although the TTPs and technology used by Groups 1 through 3 UASs against USN and USMC equities are holistically similar, their employment in each AOR is highly dependent upon the specific technology accessible to the adversarial actors and their associated aspirations.

Although each AOR's adversaries aspire to ultimately undermine, usurp, and invalidate U.S. presence and strategic endeavors abroad, the adversarial approach is also dependent upon the physical representation the U.S. presents in each AOR. This is exemplified by the U.S. former one and a half CSG presence in the Arabian Gulf located within NAVCENT's jurisdiction, per previous Global Force Management (GFM) policies. In 2015, this presence was reduced to more than half of its previous CSG presence within the Arabian Gulf in pursuit of the former SecDef General (ret) James Mattis's Dynamic Force Employment strategy [98]. This reduction in presence was also related to the manifested and emboldened threat imposed by Russia and China in the Pacific and European theaters, referred to as the GPS. As expected, the National Security Strategy and the subsequent 2017 GFM policy redirected more USN and USMC military assets to support U.S. strategic policies of power projection, deterrence, and partner nation to support the PACOM AOR. Therefore, the USN and USMC footprint within the CENTCOM AOR varies vastly from the U.S. sustained CSG and ARG presence in other theaters such as the Pacific theater. Further, in addition to

the presence of a CSG and ARG, the U.S. also maintains a continuous, short term, sustained forward deployed naval force (FDNF) within the Pacific theater to support rapid, sustained action should an operational requirement arise. As anticipated, the footprint within the CENTCOM and Pacific Command (PACOM) AORs varies vastly by location, surface area, capability, and intent. Therefore, this research will consider how adversaries leverage and adjust their Groups 1 through 3 UASs TTPs for the purposes of ISR, smuggling, C2, weapon delivery, deterrence, ruses, queuing, targeting, etc. in each AOR.

In addition to the USN and USMC presence and concomitant activities in each AOR, our research will evaluate adversarial UAS tactics as tied to the technological infrastructure associated with their operating environment. The underlying foundation supporting and enabling civilian and military communications and C2 in an AOR will inevitably determine the TTPs adversaries are able to seize and leverage against USN and USMC equities using UASs. Expectedly, technologically advanced countries and societies will observe more advanced use of adversarial UASs and their associated capabilities. Conversely, less advanced countries, perceived as third world or economically constrained, will observe simpler UAS TTPs.

5.1.1 Africa Command Area of Responsibility

AFRICOM's intent is to focus on strengthening partners ties, emboldening partner countries with the requisite ability to defend their boarders and govern themselves, and broaden communication endeavors to improve regional stability and security cooperation [99]. Within the AFRICOM AOR, the U.S. maintains a sleek, stealthy, and agile footprint with contingent quick reaction forces to further the U.S. strategic mission of enabling partner nations and touting the U.S. as a partner of choice. The USN and USMC teams maintain no major naval ports, facilities, or training sites within the AOR that provide a substantial surface area or footprint for an adversary to surveil, target, or attack [100]. Moreover, the USN and USMC's presence within the AFRICOM AOR is primarily limited to Djibouti or maintained with mobile sites, forward operating bases, and afloat forward staging bases provided through ARGs, CSGs, and independent ships [100]. The associated militarized USN and USMC forces that embark and deploy within the AFRICOM AOR serve as quick reaction forces under the auspice of special warfare, urban warfare, battalion landing teams, amphibious assault teams, and reconnaissance teams. The intended purposes for their operations are in

support of humanitarian assistance and disaster relief (HADR), noncombatant evacuation operations (NEO), embassy and consulate reinforcement, rapid response, counterpiracy, combatting terrorism, countering adversarial surrogates and proxies, conducting coalition exercises, and other associated legitimacy operations [99]. The primary locations of USN and USMC operations are focused about and towards audiences residing in the locales of the "Lake Chad Basin (Niger, Nigeria, Cameroon, Chad, and Mali); Horn of Africa (Somalia and Kenya); in the Maghreb (Libya and Tunisia); and in/around the Gulf of Guinea countries (Mauritania, Senegal, Gambia, Guinea Bissau, Guinea, Sierra Leone, Liberia, Cote D'Ivoire, Ghana, Togo, Benin, Equatorial Guinea, Sao Tome, Gabon, and Congo)" [99].

5.1.1.1 AFRICOM Communications Infrastructure

In addition to the footprint and associated operations conducted by USN and USMC forces, the inherent infrastructure of the associated African countries and their contribution towards UAS enablement must be of consideration. Although the use of telecommunications and the inherent rudimentary networks they were incepted upon commenced mass distribution in the 1970s, it did not reach the African continent until the 1990s [101]. This delayed introduction into the African infrastructure is further delineated by the reliance on legacy telecommunication networks and architecture. Within the regions of the Lake Chad Basin, Maghreb, Horn of Africa, and Gulf of Guinea, the following telecommunication networks are primarily used [101]:

- Global System for Mobile Communications (GSM) – 900/1800/2100MHz
- Long Term Evolution (LTE)
- Worldwide Interoperability for Microwave Access (WiMAX)

The choice of UASs' communication methods in these areas is therefore limited to the rudimentary communication infrastructure of the host country. In this instance, the use of GSM and LTE to support BVLOS C2 for a UAS serves as a dominant, but not sole means of operation. Although legacy in nature, the use of GSM allows for a degree of autonomy in UAS operations through the relay method mention in Section 4.4.3.0.2. It further allows a mundane solution for uplinking high-level, command-oriented data such as flight control, navigation, queuing, and subsequent mission related tasks pertaining to communications, coordination, and surveying, and the downlinking of telemetric data to the controller. This telemetric data expectedly encompasses the flight status of the UAS to the

operator. Of significance, the use of GSM also affords the UAS access to the World Wide Web. This access provides the UASs with additional accesses to bandwidth, databases, and the enablement for real-time video streaming to support tasks associated with surveillance and target queuing.

The Africa continent has a delineated the capability and desire to leverage UASs for the purposes of extending military-related coverage and capabilities, while lessening the cost of financial burdens on forces has been conceptualized since 2010 [102]. Denel Dynamics, a South African company, developed and exported combat-ready UASs to allied and partner forces and nations for profit. Denel Dynamics serves as South Africa's largest provider of defense materials and equipment, and a leading missile and UAS proponent. Denel's mass production of Groups 1 through 3 UASs for the Africa continent include capabilities ranging across the following spectrums [102]:

- Aero-engines consisting of longer and cheaper maintenance and life cycles, with reduced acoustic signatures;
- Additional sensors to support day and night methods of flight operations such as reconnaissance, targeting, and patrols;
- Improved tracking with the incorporation of range finders and laser designators;
- Automated take off and landing capabilities as of 2012;
- Dual band data links to allow for the incorporation of additional UAS payloads;
- Ranges of up to 250 kilometers using LOS C2, with the potential for the addition of SATCOM C2 in support of BVLOS communications.

Denel Dynamics continues to serve as the continent's leading producer of innovative aerial defensive and offensive solutions, as it is owned by the South African government. It also fosters partner relationships with the U.S. through foreign military sales, in addition to South America and the Middle East [103]. Its ties to governmental funding and endeavors emboldens its ability to support UAS research and development domestically and abroad.

5.1.1.2 AFRICOM UAS Threat

As anticipated, adversarial UAS actors in the AFRICOM AOR primarily manifest in the form of non-state actors and hobbyist. AFRICOM identifies the actors as the ISIS and their associated proxies or surrogates, al-Qaida and their adherents and affiliates (AQAA) which

includes Al-Shabaab per U.S. designation of violent extremist organization (VEO), and any other U.S. designated foreign terrorist organizations that are defined by the U.S. definition of VEOs operating in Africa [99].

African UAS tactics vary from single to cluster UAS employment against USN and USMC's equities and personnel. From prehistoric to modern employment, the tactics are observed as rudimentary, but threatening in nature to human life and facilities. Adversarial UAS tactics in AFRICOM range in implication and are further codified as a means of ISR, C2, and weapon employment to support information gathering of U.S. plans, intentions, and TTPs, as well as serving as a tactical deterrence.

The first noted and assessed use of Groups 1 through 3 UASs within the AFRICOM AOR was committed by the Libyan National Army (LNA) in Libya and Nigeria, as provided by the World of Drones assessment. The U.S. designates the LNA as an opposition group to the United States' backed and recognized government of Libya. The LNA gained possession of Groups 1 through 3 Wing Loong II UASs by affiliation with the UAE. As a result, the acquisition and deployment of the Wing Loong II UAS in northern Africa has resulted in the operationalization of over 2,000 aerial strikes including UASs since 2014 [104].

5.1.1.3 UAS C2 Assessment In Africa Command

The north western countries of Africa, such as Algeria, Morocco, and Senegal have taken a staunch stance for reserving the use of UASs for government security purposes only. However, other countries such as Niger, Cote d'Ivoire, Ghana, Nigeria, Namibia, Kenya, and South Africa leverage the use of the commercial UAS industry and production to support security and public services in support of safety and oversight, while allowing the general public to enjoy commercial UAS use [105]. We therefore assess the use of UASs in an expanding, novice communications infrastructure will continue to contribute to the use of nefarious UAS use in the ARFICOM AOR. This assessment is also attributed to the lack of sustained oversight in a developing AOR, where many counties and factions of leadership are continuing to vie for power and control.

AFRICOM's wide and consistent utilization of the rudimentary GSM and LTE cellular infrastructures in the many disparate, rural locations of the continent supports basic C2 architectures for UAS employment. GSM and LTE can support the transmission of flight

and payload associated data, as well as support BVLOS operation. Based on non-state and state actor acquisition and operationalization of UASs in the AOR, it is assessed future occurrences of UAS use is currently limited to VLOS, although aspirational use to BVLOS can be anticipated. These long range UAS operations would be made possible by the use of GCS to BTS communication, with BTSs serving as relays in the chain of communication between the GCS to the UAS. The ability to leverage GCS-to-UAS C2 is constrained to ability to acquire the requisite hardware capable of supporting the necessary C2 protocols to between the UAS and GCS. Additionally, the ability to achieve BVLOS through the use of existing BTSs serving as relays is dependent on the area UASs are employed in, although this too can be augmented by the GCS and associated hardware via WiFi capability. However, the African continent must first overcome its shortfall in the number of users actually leveraging smart devices to access the internet and cellular data [106]. As contemplated, UAS flight and payload operations will result in predominant BVLOS on existing 3G and 4G network infrastructures.

5.1.2 Central Command Area of Responsibility

The CENTCOM AOR has transitioned from a "Fight Tonight" mantra to a "Ready Force" mantra in light of the previous Dynamic Force Employment policy impacting the DOD's equities across the global operational environment [98]. However, the CENTCOM AOR remains a domicile of many war efforts, endeavors, adversaries, and conflicts. This is exemplified throughout recent history in the inception of CENTCOM in the 1980s to train, engage, and fight in modern warfare against the Soviet Union during the Cold War.

CENTCOM's vast history of conflict is further delineated by the twenty-year global counterterror campaign waged following the flight hijacking and subsequent strikes against the U.S. Trade Center. Simultaneously, the U.S. has been engaged in a forty-year campaign against the Islamic Republic of Iran, which has engaged in hegemonic pursuits in the Middle East under the auspice of domestic and international facilitation of terrorism.

These conflicts have led to the U.S.'s sustained military presence throughout the Middle East in the countries of Kuwait, Qatar, Bahrain, Saudi Arabia, Afghanistan, Syria, the United Arab Emirates, Iraq, Oman, and Pakistan. The U.S. presence in these countries ranges in the form of fixed naval presences with small Patrol Crafts, Mine Sweepers, Destroyers,

a Marine Expeditionary Brigade (MEB), SPMAGTF, and quick reaction force (QRF), to infrequent deployment of ARGs and CSGs with inherent MEU attachments.

The U.S. presence in CENTCOM is intended to support deterrence against Iranian endeavors to leverage the military element of national power and influence to counter U.S. and partner nation actions and policies [107]. In this regard, deterrence serves as a military, diplomatic, and political concept based upon the U.S. commitment to the region militarily, economically, and politically against the threats imposed by Iran and its surrogates and proxies. In addition to these threats imposed by Iran in surrounding countries, the U.S. competes with Russia and China on an economic scale for placement, access, and influence throughout the Middle East as well.

As contemplated, CENTCOM does not have a sole strategic focus, and must exert the ability to maintain flexibility, agility, and evolve as the character of war evolves. CENTCOM must therein remain able to balance multiple priorities and tasks as the threat evolves. We assess CENTCOM's current efforts to include deterring Iran, countering Iranian surrogates and proxies, degrading weapons, human and drug trafficking and facilitation networks, enabling partner nations, and building relationships with partner nations. Nonetheless, CENTCOM's top priority remains deterring Iran and their destabilizing activities within the AOR [107]. Iran's destabilizing activities in the Middle East is exuded by their sustained quest for nuclear capability, influence, and hegemonic behavior that has threatened the U.S. and its regional partners within the AOR. Since May 2019, Iran has publicly been condemned of its support to VEOs, surrogates, and proxies that have been codified as Shia Militia Groups (SMG) under the U.S.'s counter-Iran planning policies. Iran's support to the aforementioned groups has contributed to the attribution of attacks against U.S. interest in the Bab el Mandeb, Strait of Hormuz, Iraq, Syria, Yemen, Saudi Arabia, and Afghanistan with UASs for the purposes of ISR and kinetic effects [107]. Iran's use of UASs against U.S. equities has contributed to the increased Grey Zone threats of asymmetric warfare.

5.1.2.1 CENTCOM Communications Infrastructure

The Middle East is heavily reliant on its mobile communications infrastructure to support C2, communications, and the relay of civil safety features for their civilian and military functions of society. These forms of mobile communications range from GSM to the onset of 5G and dominate the market vice fixed broadband forms of communications. However,

fixed broadband communications play an essential role to the development and backbone of the incoming 5G network infrastructure, as well as the desire to transition cities to smart cities on the 5G architecture. This is attributed to the pre-existing infrastructure being used to transition such areas to 5G. However, the Middle East holistically lacks the foundational necessities of fixed broadband in rural or war torn countries such as Iraq, Syria, Yemen, and Afghanistan due to poor economies or successive years of conflict [108]. This lack of fixed broadband limits the subsequent development of 5G attainment in these areas.

To make up for the recent surge in demand for data and associated bandwidth requirements during the COVID pandemic, countries in the Middle East have adopted concepts of mobile tower sharing of existing 4G networks, while the desire and aspirations remain to develop 4G LTE networks and accelerate acquisitions into 5G in countries such as Bahrain, Iran, Jordan, Kuwait, Oman, Saudi Arabia, UAE, and Yemen [109].

This sharing of network and bandwidth space and capabilities is further codified by the Gulf Cooperation Council, consisting of Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and Yemen, and their establishment of the FARAJ interregional fiber-optic network [110]. This coalition of countries and their associated fiber-optic network links each country and its underlying telecommunications capabilities and infrastructure together to form a formalized conglomerate approach to network sharing and processing. Furthermore, this networked approach also links into the Fiber-optic Link Around Globe (FLAG) cable system, which serves as a fiber-optic link that is owned and operated by the FLAG corporation in support of global communication and information sharing. This data communication sharing between the Gulf Cooperation Council (GCC) and other subsidiary countries in the Middle East is indicative of a shift from basic GSM communication to 4G and LTE communications. As contemplated, such momentum bodes to support the inherent use of commercially operated and modified UAS in a means that leverages GSM, 4G, and LTE as a method for communication, control, and monitoring.

5.1.2.2 CENTCOM UAS Threats

The threat imposed by Iran is exacerbated by its facilitation and employment of nefarious UAS activity throughout the AOR [111]. The use of these supplied UASs have circumvented the traditional air force capability gap Middle Eastern non-state actors experienced. Now, these actors are able to conduct aerial surveillance and aerial kinetic strikes. CENTCOM's

posture statement acknowledges the presence and the associated threat UAS's impose against U.S. forces in the Middle East. It further acknowledges the gap in CUAS capability against the UAS threat, due to their ease of attainment and use in the AOR, and their associated ability to inflict large scale damage against U.S. critical infrastructure and personnel [107].

The first predominant instance of arming UASs for the purposes of conducting kinetic, destabilizing tactical operations within the CENTCOM AOR arose in 2016 with ISIS [104]. ISIS created and leveraged a formal drone unit known as the Unmanned Aircraft of the Mujahideen to conduct surveillance, target acquisition, and strikes against U.S. and coalition forces in Syria and Iraq [104]. Further, ISIS developed a trafficking ring for commercial drone technology in as many as 16 countries, and provided means of demonstrating how to attach small munitions to deliver kamikaze attacks [104]. ISIS leveraged their UAS surveillance techniques to further support and galvanize other state and non-state actors to conduct strikes against U.S. equities within Syria and Iraq, further popularizing and influencing the method of warfare in the 21st century. This is exemplified by the New York Times report in March 2016 from General (retied) MacFarland regarding intelligence reporting of adversarial drone surveillance techniques to support targeting:

> In March, General MacFarland and American military commanders in Baghdad received an intelligence report that the Islamic State had posted surveillance video online that had been taken by a small drone. The video footage showed a newly created series of bases in northern Iraq where American and Iraqi forces were stationed. Just days after the video was put up, a Katyusha rocket landed in the middle of an outpost of more than 100 American Marines, killing one who was rushing to get others to shelter in a nearby bunker. The strike was so accurate that military officials described it as a "golden shot" to pierce the defenses put in place, and there was speculation that a drone was used in the targeting. [112]

Further exemplified use of UASs in the CENTCOM AOR have been demonstrated by the Iranian backed Houthi rebel group in Yemen and al-Sham terrorist organization in Syria. The Harakat Tahrir al-Sham organization serves as the successor and premier jihad cell to the Jabhat al-Nusra organization after its splintering in 2017 [113]. This group demonstrated the first recorded example of UAS swarm tactics in January 2018 against the Russian naval

port of Tartus in Syria. Russian Defense officials reported the use of thirteen armed drones, rigged with explosives, flying in a synchronized, coordinated manner under a common C2 [114].

5.1.2.3 UAS C2 Assessment In CENTCOM

What can be asserted is the telecommunications infrastructure across the Middle East holistically lags in its initiative to implement new, innovative forms of communications such as 5G. Although the GCC has broken ground towards the implementation of 5G through their associated Telecommunications Regulatory Authorities, the surrounding countries lack the requisite funding, support, and coordination. It is these countries where nefarious actors originate, thrive, and usurp USN and USMC personnel and operations. This lack of synergy is attributed to the lack of centralization throughout the GCC and surrounding countries, marginalized presence of foreign investors, and the disproportionate presence of populations in desolate regions [110], [115].

Due to this knowledge, we assess the Middle East several years away from the ability to produce and leverage Groups 1 through 3 UASs on sophisticated data link architectures such as WiMAX or 5G. UAS tactics for operations and exercising C2 will inherently be reliant upon the ability to modify commercially available UASs to meet the purposes of low detection and serve as disposable should detection and usurpation be committed against them by CUAS technologies.

Adversarial employment of UASs in areas of armed conflict in the CENTCOM AOR will remain confined to either the existing communication network architectures of 2G, 3G, and 4G architectures, or the procurement of proprietary or modified hardware capable of supporting C2 between the GCS and UAS via RF means such as WiFi. In light of the foreign and domestic influence from Russia, China, and Iran in disenfranchised regions, the potential for advanced UAS employment tactics with proprietary software, hardware and C2 is anticipated. Therefore, we assess the level of UAS employment will remain innovative in nature. As contemplated, UAS employment BVLOS through the use of the current cellular infrastructure, mobile hotspots, and nation state influence is possible for UAS flight and payload operations. Flexibility can and will be augmented with the employment of WiFi and subsequent hotspots using cellular services in regions of poor connectivity to maintain C2 to support UAS flight and payload operations. Prehistoric tactics leveraged by terrorists,

surrogates, and proxies in the Middle East have encompassed the use of hotspots to support the triggering of IED from distant, BVLOS base camps [116] The aforementioned tactics all support the daisy-chaining of relays to elongate coverage to support long range operations against USN and USMC equities in the region.

5.1.3 Europe Command Area of Responsibility

EUCOM is, has been, and remains a combat-ready, war fighting theater postured for threats ranging from international terrorism, HADR, and the Great Power Competition. EUCOM, one of our few combatant command headquarters located outside the continent of the united states (OCONUS) in conjunction with AFRICOM, is located in Germany and consists of approximately 64,000 civilian and military personnel. Its role has since expanded considering the emergence of the Great Power Competition and Russia's influence in Eastern Europe, the Mediterranean Sea, Black Sea, Baltic Sea, Barents Sea, and Israel.

Russia, through military combat and non-combat operations, has expressly exerted its desire for restoration as an internationally recognized global power and influencer in geopolitical affairs. As such, Russia has previously employed its military aggressively throughout eastern Europe in Crimea, Ukraine, and Georgia to expand their influence, coerce neighboring countries, and undermine their inherent sovereignty [117]. Additionally, Russia has repeatedly operated in the Grey Zone, an area of conflict and warfare that does not illicit kinetic response options but serves as a means to undermine, exploit, and subvert the U.S. and its coalition partners. Russia accomplishes this though information operations, to include UAS operations and facilitation for surveillance, intimidation, and C2.

Expectedly, EUCOM supports and operates a range of land, air, sea, space, and cyber domain operations with regional allies and partners to dissuade and deter Russia aggression, defense the sovereignty of Israel, enable global commerce and free trade, and counter potential external threats originating from actors within the EUCOM AOR. EUCOM priorities include:

- Constantly improve the war-fighting readiness of the U.S. Joint Force
- Strengthen solidarity and unity with U.S. Allies and partners
- Foster a highly-motivated Team of Patriots [118]

In recent history, EUCOM has continued to adapt a policy that emboldens partner and coalition countries as a means of obtaining and amassing a holistic approach to countering malign threats from insurgency to state actors such as Russia. This is further emphasized in the current U.S. presidential administration's approach in improving the U.S.'s maritime posture through strategic realignment in Europe [119].

This shift in U.S. presence in Europe entails a potential transfer of military equities, assets, and personnel from Germany to elsewhere in Europe for the purposes of improving partner relations, training, and time sensitive decision making to enhance deterrence against China and Russia. The move also presents a shift in the transition of EUCOM headquarter elements to Belgium to consolidate decision makers in the vicinity of NATO's Supreme Headquarters Allied Powers Europe (SHAPE) [120]. Another decisive transition and addition to the U.S.'s footprint in Europe is encapsulated in the station of 1000 more Marine and Army personnel in Poland, which shall raise our current commitment to Poland and the corroborating Defense Cooperation Act to approximately 5500 personnel [119]. Currently, the U.S. only has a fixed maritime presence at Naval Station Rota in Rota, Spain. These USN cruiser-destroyer (CRUDES) ships operate as a means of FDNF, supporting short notice contingency operations, deterrence, and power projection where applicable in the EUCOM AOR [121]. The impending realignment of forces in Europe includes plans to add two additional forward deterrence elements in support of NATO's maritime battle groups located in Estonia, Latvia, Lithuania, and Poland [119]. This intended improvement to the U.S. and NATO's maritime and amphibious capabilities is also coupled with intended transitioning from traditional Maritime Fusion Centers to technically linked data sharing to support maritime domain awareness.

5.1.3.1 EUCOM Communications Infrastructure

The European continent leverages 3G, 4G, LTE, mobile broadband, fixed broadband, fiber, and emergent 5G capabilities as a means for connecting the civil and military forms of society to the infrastructure. The reliance on and the number of European wireless towers enabling mobile telecommunication and internet connectivity was expected to increase from 350K in 2018 to 450K by 2025 [122]. This number was met and accounted for in

light of the Coronavirus-19 pandemic that necessitated the need to supporting a transition to teleworking households. Additionally, EUCOM enjoys a large variety of machine-to-machine and IoT connectivity. Expectedly, such a reliance on and abundance of IoT devices and network connectivity have driven the growth and demand for fixed and mobile broadband services throughout Europe. Such growth has complemented the ability to research, acquire, and develop the foundational infrastructure for 5G, starting in 2018 [123]. More proof of Europe's transition towards 5G is indicated by their investment in 5G technology. The European 5G communications businesses obtained approximately $147.5 million in revenue in 2018, and are anticipated to obtain an approximate $27.74 billion in revenue by 2026. Further, the European 5G communication technology market held an estimated value of$359.3 million of net worth in 2019, and is expected to obtain $42.70 billion of net worth by 2027 [123].

The use of 5G supports the implementation of high data rate communications, increases in bandwidth, and decreases in latency and associated internet lag time. The facilitators of Europe's 5G infrastructure consist of Qualcomm Technologies Inc., Huawei Technologies Co. Ltd., Intel Corporation, Samsung Electronics Co. Ltd., Ericsson, Nokia Corporation, NEC Corporation, Vodafone PLC, Orange Labs, EE Ltd., NTT Corporation, IBM Corporation, ZTE Corporation, Fujitsu Corporation, CISCO, Interdigital Communication, Alcatel Lucent, Siemens, ATOS SE, and Orion Innovations [123].

Of concern is Huawei's contribution to the European continent's 5G infrastructure. China, as part of its Belt and Road Initiative, has procured a presence and relationship with current U.S. partners and allies in trade, infrastructure, and presence. This presence is exemplified by China's real estate investments in seaports located in critical waterways and nations such as Belgium, Italy, France, and Greece [124]. These port facilities and associated deals are an indicative link to China's initiative to link its economy and hegemonic pursuits physically and logically to Europe via sea, air, and land resources. This presence is culminated with China's presence and sustained access to 10 percent of the shipping rights entering and departing Europe, serving as the European Union's largest source of import and its second largest export market [125]. China's presence in the European communication infrastructure with Huawei 5G serves as an imminent threat to network protection and a potential compromise of technical and personally identifiable information. The deals of 5G infrastructure and trade agreements with China, and the imminent threat imposed by Russia, make the European

theater ripe for potential uncertainty with regards to the future of UAS operations and capabilities to conduct C2.

5.1.3.2 EUCOM UAS Threats

The small UAS market in Europe has become insatiable to country government officials, agencies, and organizations, as well as hobbyists and nefarious actors. It is further enabled by the broad infrastructure provided by the aforementioned service providers. The low-cost application of small UASs has given rise to the facilitation of government services such as agricultural crop management, air traffic monitoring, road traffic management, and mining [126]. In the European AOR, the rotary-wing portion of the commercial UAS market is leveraged more over the fixed-wing UAS market for the purposes of military, institutional, and civilian use. The preference of rotary over fixed wing is attributed to their versatility and ease of use with regards to in-flight operations, launch and recovery, and high maneuverability [126].

We assess adversarial actors' use of UASs in the EUCOM AOR to be limited to ISR, C2, and potential queuing for follow on targeting to support fear mongering and related insurgency acts. This is due to the asymmetric nature of warfare conducted against large governmental and civilian infrastructures with small UASs. An example includes the December 2018 incident at the London Gatwick Regional Airport, involving a small UAS causing an incursion with a commercial airliner on the runway resulting in the temporary closure of airport operations for approximately three days over the New Year period. This action resulted in the financial loss of millions of euros to airport operators, airlines, and passengers, as well as resulting in widespread confusion, panic, and chaos [127]. Furthermore, law enforcement reporting from France's counterterrorism unit has indicated the potential plotting of non-state actor groups inside Europe to leverage biological payloads on UASs as a means of conducting a biological attack on large civilian infrastructures, to include sporting events and ceremonies [128]. Additionally, German intelligence reporting has warned and thwarted the potential for kinetic UAS attacks against their commercial airports by means of carrying out intrusive tests on inbound technology to counteract the ability to amass and introduce nefarious drones into the civilian populace [128].

Although Europe's telecommunication infrastructure is supportive of new, emergent technologies, the adversarial UAS tactics exhibited in the EUCOM AOR do not serve as a

belligerent, aggressive, and a threat to USN and USMC personnel and infrastructure. This lack of threat, as compared to the CENTCOM and AFRICOM AORs, is attributable to the EUCOM AOR not containing or being an area of active conflict and warfare. Further, the EUCOM AOR contains more structure, scrutiny, and ability to prosecute UAS threats through combined policy and capabilities. As a result to the existing and potential increase of UAS threats, the EU has begun developing a combined strategy to identify and address the small UAS threat as a whole. This initiative encompasses researching each countries' threat, defense plan, and recommending subsequent CUAS capabilities that are able to interoperate and support subduing the UAS threat [129].

5.1.3.3 UAS C2 Assessment In EUCOM

The EUCOM AOR's quick adaptation to the emergent 5G infrastructure, as well as the AOR's maintenance of the legacy 2G, 3G, 4G infrastructures allows for a variety of means of UAS application over varying C2. Further, the AORs continued use of commercial SATCOM and WiFi standards allow for mobility and flexibility in areas of poor or no connectivity to support UAS flight and payload operations. The combined use of these communication architectures allows for sustained, VLOS operations to include the potential for BVLOS through daisy chaining techniques in urban areas. The use of WiFi hotspots in areas of limited connectivity also allow for the potential to support short range VLOS operations, in addition to the aforesaid operations. Further, the AORs prevalence of smart devices used to access mobile and internet services in both rural and urban countries contributes to the ability to support VLOS and BVLOS UAS flight and payload C2 [130]. UAS operations could include BVLOS obtained through daisy-chaining techniques between the GCS and BTSs, or through the use of UAS-to-SATCOM methods incorporating satellite receivers/transmitters as relays for long haul communications. The current UAS threats imposed by state and non-state actors in the AOR, including Russia, allow for more potential of these methods of C2 to be employed by use of COTS or modified UASs.

5.1.4 North Command Area of Responsibility

The inception of NORTHCOM in 2002 was intended to provide more strategic support and oversight of the DOD homeland defense endeavors to support civil authorities within the U.S. Its intent is to enable national power, freedom of action, and defend the homeland

from international aggression, malign influence, potential subsequent actions. The AOR geographically encompasses the North American continent and the waterways of the Gulf of Mexico, Strait of Florida, and portions of the Caribbean neighboring the SOUTHCOM AOR. NORTHCOM inherently houses the most USN and USMC personnel, equities, and infrastructure than any other AOR due to its support and contribution to the readiness, manning, and training of the aforesaid assets before deploying them abroad to other AORs. Concentrated presence of Sailors and Marines in NORTHCOM are in the areas of Hawaii, Washington, California, Florida, Georgia, Virginia, Washington DC, and Connecticut to name a few. Similar to other AORs, NORTHCOM is comprised of the service component commands as well as associated Joint Task Forces between the military, federal, and state law enforcement entities. The U.S. Fleet Forces Command, also referred to as U.S. Navy North, is the USN component to NORTHCOM.

NORTHCOM recognizes the emergent threat of small, commercially available UASs as a readily available means of enabling nefarious actors from the range of hobbyist to home-grown extremist. The malign UAS operations and plans presented in the CENTCOM and SOUTHCOM AORs provide a haven of techniques and ideas for hobbyist and non-state actors alike. These events represent what the procurement and follow-on modification of commercially available UASs can present to the operational environment, and serve as a warning of what the NORTHCOM AOR could become although not traditionally considered an area of armed conflict.

5.1.4.1 NORTHCOM Communications Infrastructure

The infrastructure to conduct mobile telecommunications and achieve internet access and connectivity by means of mobile and fixed broadband services, in addition to other wireless transmission means serves as a versatile and usable means of C2 in the U.S. The communication sector within the U.S. has diversified itself from traditional voice services to interconnected industrial networks using commercial and government operated satellites and associated wireless transmissions means. These services have become interconnected to support communication between satellites, ground stations, cellular towers, and wire lines providers to achieve consistent, persistent, and reliable communications across the country.

Telecommunication writ large is governed by the Regulatory Commissions, and specifically by the Federal Communications Commission (FCC). Under the FCC, the Communi-

cations Act of 1934 and Telecommunications Act of 1996 hold precedent in the governance of producing and promulgating voice and data services to the public.

The U.S. leverages a wide variety of means to provide voice and data services throughout country. These means include GSM, 2G, 3G, 4G, LTE, fixed broadband, mobile broadband, fiber optics, dial-up, SATCOM, and 5G. Of these, broadband provides the most assurance in reliability and speed across the U.S. and NORTHCOM AOR. The top broadband service providers in the NORTHCOM AOR include Comcast, Charter, AT&T, and Verizon [131].

The Cybersecurity and Infrastructure Security Agency further codify and divide the North American continent's communication sector into the following sectors to accomplish the acquisition, procurement, operationalization, management, and oversight of communication related infrastructures within the AOR:

- The Energy Sector provides power to run cellular towers, central offices, and other critical communications facilities. It also relies on communications to aid in monitoring and controlling the delivery of electricity.
- The Information Technology Sector provides critical control systems and services, physical architecture, and Internet infrastructure. It also relies on communications to deliver and distribute applications and services.
- The Financial Services Sector relies on communications for the transmission of transactions and operations of financial markets.
- The Emergency Services Sector depends on communications for directing resources, coordinating response, operating public alert and warning systems, and receiving emergency 9-1-1 calls.
- The Transportation Systems Sector provides the diesel fuel needed to power backup generators and relies on communications to monitor and control the flow of ground, sea, and air traffic. [132]

The aforementioned sectors under regulation by the FCC provide and support the use of the previously mentioned technologies, which enable communications and C2 of equities within the NORTHCOM AOR. As contemplated, this allows for a wide variety of threat vectors available to hobbyist, non-state actors, and state actors in regards to UAS operations and TTPs within the AOR.

5.1.4.2 NORTHCOM UAS Threats

The use of UASs within the NORTHCOM AOR is becoming incorporated into civil service elements of society, to include support for meteorological surveys, agriculture, traffic monitoring, criminal surveillance, safety services related to law enforcement and paramedics, and recreational use [133] [134]. However, this increased civil and governmental use has amassed and provided room for the UAS threat to promulgate under the cover of recreation. The UAS threat in the NORTHCOM AOR predominantly stems from hobbyist error and home-grown extremists. It primarily manifests in the form of ISR, C2, and propaganda, with the potential for queuing in support of intelligence gain and follow-on targeting.

These threats have often occurred over U.S. bases, facilities, and operational equities while at sea or in a training capacity. Some instances include:

- January 2015, In Washington, D.C.: a COTS UAS flew in the vicinity and over the White House fence and inadvertently landed on the White House lawn without interdiction. The incident caused no harm to U.S. equities or personnel. The operator of the UAS was observed as an off-duty intelligence official [135].
- July 2016, Savannah River Site: eight COTS UASs were identified by the sites defensive forces and work force [135].
- 2006-2007, Columbus Ohio: a modified COTS small helicopter was leveraged by al-Qaida trained operative, Christopher Paul, with the intent of carrying out drone research and acquisition for the terrorism group [136].

These threats, although apparently basic in nature, represent only a small fraction of the reportable events for apprehended and halted nefarious UAS operations. We assess the thwarting of UAS operations in the NORTHCOM AOR as more successful due to sound law enforcement and interagency cooperation, in addition to governmental policies and CUAS actions converging on a common means for detecting, locating, and neutralizing adversarial UAS operations.

5.1.4.3 UAS C2 Assessment In NORTHCOM

The cadre of UAS C2 architectures commercially available, as well as the accessibility and availability of COTS UASs and sophisticated proprietary software and hardware make the NORTHCOM AOR ripe for advanced UAS employment techniques. The use of cellular

networks ranging from 2G to 5G allow for VLOS and BVLOS communication for elongated coverage to support UAS flight and payload operations. The availability of broadband WiFi services and hotspots, in addition to the wide accessibility and employment smart devices lends itself to the use of WiFi as a means of C2 between the UAS and GCS in areas of poor coverage, enabling short range VLOS operations. Furthermore, the laws protecting civilian use of electronic communications and availability of proprietary UAS software and hardware allow for the programmable modification of UAS C2 methods to support UAS-to-UAS communications, waypoint navigation, and swarm tactics at the semi-autonomous level. It is anticipated that the NORTHCOM AOR will serve as a haven of the aforementioned UAS operations that may threaten surface, maritime, and shore based USN and USMC equities.

5.1.5 Pacific Command Area of Responsibility

The U.S. PACOM architect, now referred to as the U.S. Indo-Pacific Command (INDOPACOM) as directed by SecDef Mattis in 2018, serves as the largest of the AORs geographically and shares a nonphysical boarder with all other AORs. These factors contribute to the INDOPACOM command being arguably the most arduous of AORs consisting of the most coverage area with the most diversity in threats. This diversity consists of over 36 recognized nations, five mutual defense treaties with the U.S., and two of the three recognized super powers in the world. Additionally, INDOPACOM is composed of the world's busiest international sea lanes, largest maritime ports, five of the world's declared nuclear nations, and complex foreign military competition for assertion of land and maritime rights.

Due to the vast amount of surface area and complexity associated with the area covered by the INDOPACOM AOR, it plays host to a cadre of supporting component and sub-unified commands to accomplish the missions of power projection, strategic deterrence, and supporting coalition partners. These supporting commands consist of the individual service component commands as well as U.S. Forces Korea and U.S. Forces Japan. U.S. Pacific Fleet consists of approximately 200 ships, including five CSG and ARGs and 130,000 Sailors and civilians in support of the U.S. maritime interests [137]. U.S. Marine Forces Pacific consists of two Marine Expeditionary Forces (MEFs) and 86,000 marines in support of the U.S. land and amphibious endeavors [137]. These forces are consolidated and dispersed throughout the AOR in the countries of Japan, Guam, South Korea, Australia, Alaska, and Hawaii. This presence is dispersed through port and host nation agreements

with the counties of Vietnam, Thailand, Indonesia, New Zealand, and India.

The assertion INDOPACO provides through the presence of these forces, in addition to monetary and training facilitation, is to enhance regional stability and security through security cooperation, regional development, support to HADR, and deterring regional aggression. INDOPACOM's mission is to provide, operate, and sustain a combat ready force that is capable of denying adversaries air and maritime dominance in conjunction with emboldening partner nations. The following serve as focus areas for INDOPACOM:

- Joint Force Lethality – We must continue to develop and field capabilities necessary to deter aggression and prevail in armed conflict should deterrence fail.
- Design and Posture – We will adapt from our historical service-centric focus in Northeast Asia to a new more integrated joint forces blueprint which is informed by the changing threat environment and challenges of the 21st Century across the entire Indo-Pacific.
- Exercises, Experimentation, and Innovation – Targeted innovation and experimentation investments will evolve the joint force while developing asymmetrical capability to counter adversary capabilities.
- Allies and Partners – Through increased interoperability, information-sharing, and expanded access across the region, we present a compatible and interoperable coalition to the adversary in crisis and armed conflict. [137].

5.1.5.1 PACOM Communications Infrastructure

The socioeconomic infrastructure within the PACOM AOR in both allied and non-allied countries is influenced by physical Chinese presence or pressure. China's military modernization in the domains of land, air, sea, space, and cyber provide new risks to previously forged U.S. alliances as well as threats to the U.S.'s strategic stability policies within the region. These actions are exemplified by China's military expansion and agreements in the PACOM AOR and into the neighboring AORs within the past decade, to include EUCOM, CENTCOM, and AFRICOM. It is further exemplified by China's vested activities and reliance in defense spending and cooperation with Russia. Their combined defensive tactics

consist of cyber espionage, theft of intellectual property, information operations against public target audiences, the funding of long range ballistic missiles, and the controlling of international waterways and maritime commerce [138].

The countries in Asia and their inherent mobile telecommunications, mobile broadband, and fixed broadband infrastructures vary based on economic status and cooperation with neighboring countries. Expectedly, Asia writ large exercises the use of 3G, 3G+, 4G, and LTE throughout the continent. 2019 and 2020 have also showed a shift from mobile voice to mobile data, with emerging nations such as Japan, Korea, Taiwan, and Singapore following in the pursuit of mobile broadband as a means of supporting C2 across the country. In light of the emergence of 5G, many countries in Asia already have or have commenced investing in the requisite foundational broadband infrastructure to support the operationalization of 5G. Countries exhibiting a stronger mobile penetration testing delineated a stronger chance for succeeding in the transition to 5G, which consisted of the previously mentioned countries.

In 2016, the global average for broadband speeds were assessed at 6.1Mbs on fixed lines and 11.8Mbs when leveraging a mobile device. However, in Asian countries such as South Korea, they enjoyed approximately 27Mbps on fixed lines and 11.1Mbs when leveraging mobile devices. India suffered the worst speeds on the Asian continent, with fixed lines at 3.6Mbs and mobile at 3.3Mbps [139]. This information is graphically depicted on Figure 5.1, showing Asia's leading efforts towards broadband speeds and the ability to provide consistent, reliable, fast data rates to their general public.

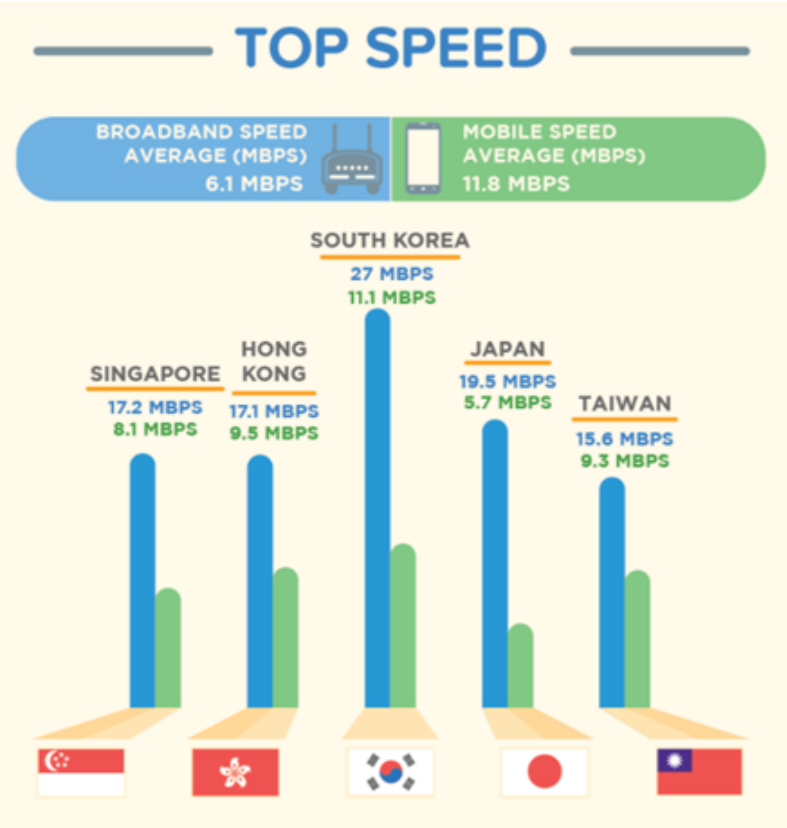


Figure 5.1. Asia's Internet Speeds in 2016. Source: [139].

The Asian continent and AOR lead the world in global broadband speeds. The best peak speeds are too exhibited in the INDOPACOM AOR between Singapore at 157Mbps on broadband and Australia at 171Mbps on cellular. This assertions provided about the PACOM AOR's mobile telecommunications and broadband infrastructure provide consistent, nearly assured, and unconstrained access to fast data rates and the capacity to conduct unique, advanced means of C2 with UASs.

5.1.5.2 PACOM UAS Threats

The 2021 UAS threat in the PACOM AOR arises primarily in the form of aerial surveillance and propaganda. The threat actors take the form primarily of hobbyist and non-state actors. Within the continent of Asia, non-state actors leverage drones as an extension of a non-aerial traditional service element to provide aerial vantage points of political events, monitoring

civilian socioeconomic infrastructures, and propaganda to include spreading fear about the potential of weaponizing UASs [140] [39]. Hobbyist government officials primarily leverage UASs for the purposes of monitoring illegal activities, agricultural support, advertisements, and recreational use [141]. The commercial drone market accounted for less than three percent of the $127.3 billion global COTS UAS market in the INDOPACOM AOR; however, this is anticipated to grow well beyond 25 percent of this calculation in the impending years. This growth is highly attributed to the commercialization, cheapening, and variance of UAS use over the last decade [140].

The use of UASs by hobbyist and non-state actors for the purposes of conducting ISR against U.S. Naval assets such as CSGs, ARGs, and independent CRUDES deployers transiting narrow traffic corridors and ports in the INDOPACOM AOR, in addition to overflying USN and USMC equities such as bases is of constant routine [142]. The use of small UASs as a means to harass USN vessels serves as a low cost power projection for the Chinese military. The South China Sea has divulged into an area of constant aggression from Chinese UASs conducting aerial surveillance. The actions have become exacerbated to the point of contention between Taiwan and China, resulting in Taiwanese declaration to shoot down Chinese UASs flying in the vicinity of the Taiwan-occupied Pratas Islands in the South China Sea. This aggression and increase in aerial surveillance in Taiwan's airspace and defenses is observed as an escalation in Grey Zone warfare, deepening the level of tensions in the region as a result of China's excursions and aspirations for regional and global hegemony [20]. The use of UASs to conduct ISR in the vicinity of bases by hobbyist, state actors, and non-state actors is also exemplified at Andersen AFB in Guam, which houses both USN and USMC equities in support of contingency operations [143].

Although the use of UASs in the INDOPACOM AOR has been limited largely to non-kinetic uses such as ISR, C2, and propaganda, the forethought of using them as a means of conducting kinetic operations to fulfill terrorist related aspirations exists. In 2020, several arrests were executed by Indonesia's Police Detachment 88 against the Jemaah Islamiyah extremist group based in Bekasi. These arrests revealed plots and intentions to use UASs as a means of conducting weaponized strikes against local law enforcement, with the suspects ascertaining both commercial grade UASs and associated batteries [140]. Another instance of aspirational weaponized UAS employment deterred by law enforcement was observed in Malaysia by the pro-ISIS militant Mohammad Firdaus [140]. In this instance, Firdaus

planned a bomb attack with a commercial grade UAS against the Bukit Aman Federal Police headquarters in Putrajaya and a Free Mason Temple in Bukit Jalil as a means of demonstration against government institutions. The use of these tactics were observed to support a means of conducting low cost, high reward tactical level operations against government infrastructure to support the means of kinetic effects and the end state of regional political disturbance and public fear.

It is assumed that these kinetic means of using UASs against U.S. interests have yet to materialize in the INDOPACOM AOR, as similar to the CENTCOM and AFRICOM AORs, due to the lack of incentive and initiative. Non-state actors in the INDOPACOM AOR have observably desired to leverage legacy, traditional tactics for spreading fear and mass panic such as bombings and shootings. These means are not only legacy, but also require less scheming to plan, procure, and initiate. Additionally, non-state actors have been unable to operationalize the few instances of aspirations to use UASs for kinetic effects due to the apprehension and hindrance presented by local law enforcement in the associated countries. As such, the infrastructure, similar to the EUCOM AOR, presents as more of a challenge to operationalize UASs for nefarious means.

5.1.5.3 UAS C2 Assessment In PACOM

The PACOM AOR's pre-existing legacy 3G and 4G communication infrastructure and shift to 5G allow for the emergence of and employment of steady state VLOS and BVLOS UAS range operations. Its expeditious broadband internet speeds and commercial WiFi industry help augment the preexisting cellular communication infrastructure in rural areas of limited network resources. The use of daisy-chaining related operation using fixed and mobile BTSs and SATCOM is a currently employed concept in telecommunications, and can lend itself to elongating and sustaining BVLOS UAS flight and payload operations overland as well as the maritime environment in the South China Sea [144]. Further, China's militarization of its commercial satellite infrastructure to support its strategic objectives of global and regional hegemony also lends itself augmenting the existing C2 infrastructure to support state sponsored over the horizon UAS operations in the land and maritime environment [145].

5.1.6 South Command Area of Responsibility

Housed in southern Florida, the SOUTHCOM AOR encompasses all of South America, the Caribbean Sea, and the associated landmasses in and around the Caribbean Sea. The intent and mission of SOUTHCOM is to strengthen partnerships with surrounding nations consistent with the U.S.'s strategic priorities, countering malign threats in the AOR and those entering into the U.S., and building a team of nations to support the response to steady state and potential crisis endeavors in the AOR. The use of partnerships within the SOUTHCOM AOR is intended to support developing a whole-of-government approach, similar to other AORs, to support and advance the promotion of security, governance, and economic growth in the AOR and with the U.S. The threats addressed by SOUTHCOM range in the form of transnational criminal organizations, extremist organizations, and malign regional and external state actors to include the presence of China, Russia, and Iran in the AOR. The instability in the SOUTHCOM AOR is exemplified by the occurrence of drug, weapons, and human trafficking committed by nefarious governments and VEOs. Global powers such as China, Russia, and Iran are capitalizing from the instability in the AOR through influence and coercion campaigns to support their hegemonic pursuits [146]. The intent of countering these threats is to foster a relationship with the countries in the SOUTHCOM AOR, making the U.S. a partner of choice for military, economic, and political support and consultation. Further, the end state is to prevent Chinese, Russian, and Iranian governments from developing an influence and subsequent presence in the region that threatens the U.S.'s strategic policies of peace and stability in the region, as well as the U.S.'s homeland security due to the proximity of the SOUTHCOM AOR to the U.S. The mission of the AOR is similarly carried out by its supporting service component commands.

U.S. Naval Forces Southern Command employs maritime forces to maintain SOUTHCOM's initiatives of freedom of navigation, partner nation interoperability, and building regional partnerships through the use of combined coalition exercises [147]. U.S. Naval Forces Southern Command's lines of operations are as follows:

- Security Cooperative Activities
- Maritime Security Operations
- Contingency Operations [147]

Although SOUTHCOM hosts no distinct FDNF maritime forces, nor any fixed presence

of CSGs or ARGs, it leverages the Optimized Fleet Readiness Plan and congressional approved movement of forces to other AORs to support any required presence of power projection and forward deterrence as needed. The mission of maritime security operations consists of the use of smaller patrol crafts and associated coast guard ships to support counter piracy operations, counter smuggling operations, and patrolling of strategic choke points such as the Panama Canal to ensure freedom of navigation.

U.S. Marine Forces Southern Command serves as a means to provide the requisite manning and equipment all marine elements assigned to SOUTHCOM. As such, U.S. Marine Forces Southern Command directs the requisite timelines, planning, and execution of requirements associated with training, deployment, and redeployment of assigned forces.

SOUTHCOM leverages only one percent of the DOD's intelligence resources to detect, identify, and thwart threats in their operational environment. To meet and maintain mission requirements, SOUTHCOM leverages open-source intelligence techniques of publicly available information, advanced analytics techniques such as machine learning and artificial intelligence, and collaboration with allies and regional partners. This work occurs in their Technical Network Analysis Cell and Asymmetric Target Acquisition Center [148]. These two entities, supported and run by SOUTHCOM service component commands, work with domestic and foreign law enforcement entities in the U.S. and SOUTHCOM AOR to support interagency coordination, information sharing, and the allocation of foreign and domestic intelligence resources to achieve the SOUTHCOM mission and corroborating lines of effort.

5.1.6.1 SOUTHCOM Communications Infrastructure

The telecommunications, mobile broadband, and fixed broadband infrastructure in South America and throughout the SOUTHCOM AOR is of the lowest in the global market [149]. Currently, countries in the SOUTHCOM AOR leverage an archaic centralized form of telecommunications infrastructure, which is geographically focused on large urban centers of more affluence, vice a recommended decentralized model that places emphasis on regional support and coordination with neighboring countries. This stove-piping of architecture stifles the ability to support inter-country communications, data sharing, and the inherent ability to lift a region up as countries become economically more capable of progression. It further causes countries to rely on country controlled, unorthodox models, inhibiting the desire for international businesses to invest and support in the expansion of

the infrastructure. Wireless network connectivity is a preferred means of communications, inherently tied to the broadband infrastructure in the region it is employed in. Mobile devices and smart phones, similar to the other AORs, are the preferred means of accessing wireless content. However, the countries throughout SOUTHCOM are limited to 2G and 3G technology, with struggles to provide 4G coverage to more rural areas of the South American continent and the Caribbean.

The infrastructure of deploying large scale towers to provide subsequent fixed broadband access remains an emergent and stagnant concept in the SOUTHCOM AOR. The explanation for this stagnation in their C2 infrastructure is two-fold [150]. It is first related to the inconsistent and disproportionate policies across the continent due to the political and economic strife between their elected national governing bodies and local municipality leadership. This division is exacerbated by the systemic fear of government encroachment on local policies, infrastructure, and quality of life. The second is related to the policies associated with acquiring and operationalizing the endeavors to support communication infrastructure improvements and funding. This is caused by the disproportionate fees, spending, zoning, and use of monopolized equipment to support the development of the infrastructure. Expectedly, the roll-out of 5G within the SOUTHCOM AOR will inevitably be much further behind than any other AOR, despite external state actors encroachment.

5.1.6.2 SOUTHCOM UAS Threats

Although the C2 infrastructure in the SOUTHCOM AOR lags behind the rest of the global market, the lack of government synchronization, coordination, and policy against combating internal and external nefarious actors provides a haven for malicious UAS actors and their associated TTPs. There currently exists no regional or international legal framework or regulatory policy regarding the ownership, registration, oversight, or employment of UAS use in South America, with the exception of Brazil [151].

The primary control over known UAS technology is withheld for military means and operations. Therefore, the precedent of the UAS threats in SOUTHCOM is primarily attributed to non-state actors, with the potential for facilitation through state actors such as Iran's Qods Force, Lebanese Hezbollah, China, or Russia [104]. These external state actors seize the initiative of the disenfranchisement of the state actors within the SOUTHCOM AOR, enabling their operational endeavors by the means of funding and facilitating their

plans with commercially available UASs and training. The SOUTHCOM and CENTCOM AORs are the only AORs to experience routine, successful use of UASs to support both surveillance and propaganda activities, as well as kinetic activities against government and civilian infrastructures. This is exemplified by the following previous uses of UASs by non-state actors in the SOUTHCOM AOR [104]:

- 2002: The disclosure of UAS plans and TTPs for the FARC, a paramilitary group. The TTPs contained details of UAS operations to support drug smuggling as early as the year 2000. In 2002, several UASs were discovered by the Colombian military at a FARC camp.
- 2017: The discovery of several armed, commercially available drones in the inventory of the Cartel de Jalisco Nueva Generacion, intended to be used for subsequent violent attacks against government and civilian infrastructures.
- August 2018: Venezuelan military defectors from the Venezuelan military leveraged and armed two independent, GPS-guided, commercial UASs to attack President Nicolas Maduro during a speech at a military parade. The attack resulted in the detonation over the parade, while President Maduro delivered an address to commemorate the 81st anniversary of the Bolivarian National Guard.

The SOUTHCOM AOR has already demonstrated the capability to go kinetic with the use of UAS operations. It has further displayed the intent to leverage UAS for the foreseeable future as a means of enabling and augmenting aerial operations and endeavors to support nefarious activities. As the AOR catches up with the global market for 5G connectivity and capability, the ability to leverage UASs in the surrounding areas will become more feasible and difficult to detect and track with legacy forms of CUAS capabilities. These drone attacks delineate a similar pattern of employment and use as the CENTCOM AOR. These TTPs serve as the most dangerous options of employment, and require the most attention and supporting deterrent capability to identify, detect, locate, and neutralize.

5.1.6.3 UAS C2 Assessment In SOUTHCOM

The SOUTHCOM AOR lacks the robust C2 infrastructure experienced in the neighboring NORTHCOM AOR. Further, SOUTHCOM's limitation to 2G and 3G technology, with limited coverage in rural areas provide for rudimentary C2 tactics UAS operators can leverage to conduct long-range UAS flight and payload operations. 2G and 3G coverage will

permit the use of singular and potential cluster UAS flight and payload operations in the vicinity of a BTS or with an associated GCS. However, BVLOS UAS operations is assessed by our research as a limited possibility. Until 2G and 3G technology becomes more prevalent in more rural regions, the possibility of augmenting wireless communication with personal hotspots via smart phones is restricted. C2 serves as a limiting factor in SOUTHCOM, limiting UAS flight and payload operations to VLOS.

5.2 Summary

As stated in Chapter 1, in order to counter a threat the threat must first be understood. This chapter takes the data pertaining to C2 used to support UAS flight and payload operations in Chapter 4, and applies it to every AOR to support the distinction of current UAS operations in a region. This chapter further supports our assessment of emergent UAS employment techniques and tactics in every AOR based upon the emergent communications infrastructure and capabilities used to enable communications.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 6:
Current USN and USMC CUAS Technologies

This chapter discusses current CUAS USN and USMC technology limitations in detection and mitigation capabilities along with interoperability shortfalls and UAS advancements. We identify solutions using current technologies to address the limitations and interoperability shortfalls. USN and USMC level of efforts and requirements must be aligned to achieve CUAS interoperability and to maintain superiority in the joint operational environment.

6.1 The Counter Unmanned Aerial Systems Kill Chain

The CUAS kill chain is a "structure-of-attack" concept comprised of detecting, identifying, locating, tracking, and mitigating a perceived threat UAS. Current CUAS technology is designed with the ability to affect one or more phases of the CUAS kill chain. State actors, non-state actors, and hobbyist operate UAS in areas of close proximity to USN and USMC operations of multiple mission sizes, location conditions, and communication environments. These malicious UAS operations involve ISR, targeting, interference, or strike missions against strategic, operational, and tactical USN and/or USMC interests. Under these conditions, UAS pose a threat and require the employment of CUAS technology with appropriate and proportionate capabilities against the kill chain to accomplish the desired effect in the given environment. Current USN and USMC CUASs employ capabilities using the techniques described in Table 6.1 for initial detection and subsequent identification/classification of threatening UAS. These techniques also enable locating and tracking.

Table 6.1. Detection and Tracking Techniques. Source: [4]

[Technique]	[Description]
Radar	Detects the presence of small unmanned aircraft by their radar signature, which is generated when the aircraft encounters RF pulses emitted by the detection element. These systems often employ algorithms to distinguish between drones and other small, low-flying objects, such as birds.
RF	Identifies the presence of drones by scanning for the frequencies on which most drones are known to operate. Algorithms pick out and geo-locate RF-emitting devices in the area that are likely to be drones.
EO	Detects drones based on their visual signature.
IR	Detects drones based on their heat signature.
Acoustic	Detects drones by recognizing the unique sounds produced by their motors. Acoustic systems rely on a library of sounds produced by known drones, which are then matched to sounds detected in the operating environment.
Combined Sensors	Many systems integrate a variety of different sensor types in order to provide a more robust detection capability. For example, a system might include an acoustic sensor that cues an optical camera when it detects a potential drone in the vicinity. The use of multiple detection elements may also be intended to increase the probability of successful detection, given that no individual detection method is entirely fail-proof.

After detecting, locating, and tracking the targeted UAS, current USN and USMC CUASs employ capabilities using the techniques described in Table 6.2 for mitigation and desired effects (kinetic or non-kinetic).

Table 6.2. Mitigation Techniques. Source: [152]

[Technique]	[Description]
RF Jamming	Disrupts the radio frequency link between the drone and its operator by generating large volumes of RF interference. Once the RF link, which can include Wi-Fi links, is severed, a drone will either descend to the ground or initiate a “return to home” maneuver.
GNSS Jamming	Disrupts the drone’s satellite link, [(e.g.: GPS, GLONASS, BeiDou)] which is used for navigation. Drones that lose their satellite link will usually hover in place, land, or return to home.
Spoofing	Allows one to take control of or misdirect the targeted drone by feeding it a spurious communications or navigation link. (Included within this category is a range of measures such as cyber attacks, protocol manipulation, and RF/GNSS Deception).
Dazzling	Employs a high intensity light beam or laser to "blind" the camera on a drone.
Laser	Destroys vital segments of the drone’s airframe using directed energy, causing it to crash to the ground.
High Power Microwave	Directs pulses of high intensity microwave energy at the drone, disabling the drone’s electronic systems.
Nets	Designed to entangle the targeted drone and/or its rotors.
Projectile	Employs regular or custom-designed ammunition to destroy incoming unmanned aircraft.
Collision Drone	A drone designed to collide with the adversary drone.
Combined Mitigation Elements	A number of [CUASs] also employ a combination of [mitigation] elements to increase the likelihood of a successful [mitigation] ; Many jamming systems have both RF jamming and GNSS jamming capabilities in the same package. Other systems might employ an electronic system as a first line of defense and a kinetic system as a backup measure.

In 2014, the USN and Office of Naval Research fielded and tested an operational directed-energy weapon, the LaWS 2.0, a 30-kilowatt (kW) directed-energy system aboard the USS Ponce (LPD-15), an amphibious transport dock ship. This testing positively demonstrated the effective use of directed energy against UASs as a means to support the CUAS kill chain. In November 2019, the USN installed and operationalized Optical Dazzling Interdictor, Navy (ODIN) onboard the USS Dewey (DDG-105), a Flight IIA Arleigh-Burke class guided-missile destroyer. ODIN leverages a standalone optical dazzler as a means to temporarily degrade/distort a UAS’s optical sensor. The subsequent High-Energy Laser with Integrated Optical Dazzler and Surveillance (HELIOS) program rapidly developed and fielded a 60kW class high-energy laser (with growth potential to 150kW) and dazzler in an integrated weapon system. This demonstrated a maturation in technology and an increased capability for use in countering UAVs, small boats, and ISR sensors. It further provides a means for combat identification and battle damage assessment [153].

The management for CUAS systems in the USMC is the responsibility of the Ground Based Air Defense (GBAD) program office. In [154], GBAD states that Marine Air Defense

Integrated System (MADIS), the USMC's modernization of GBAD capabilities, relies on a complementary pair of Joint Light Tactical Vehicles to host MADIS Mk1 and MADIS Mk2. GBAD program office states further, MADIS Mk1 is "primarily responsible for neutralizing fixed and rotary-wing aircraft" and MADIS Mk2 predominantly fulfills the [CUAS] "mission, while also providing radar and C2 for the pair". The MADIS Mk2 variant includes a multi-function EW capability, 360-degree radar, direct-fire weaponry, electro-optical infrared (EO/IR) optic, and supporting C2 communications suite with BVLOS gateway/server capability [154]. The stated MADIS Mk2 capabilities are hosted on a Polaris MRZR all-terrain vehicle to form Light-MADIS (L-MADIS). In July 2019, Marines aboard the USS Boxer (LHD-4), an amphibious assault ship, employed L-MADIS to neutralize a UAS Group 1 threat located within the vital area of the warship [155]. Although onboard the ship, L-MADIS was not integrated with USN targeting equities and performed as a standalone system. This points to a instance where systems are capable of interoperability but it was not implemented. The USN's and USMC's CUAS endeavors should be improved to achieve sufficient coordination in support of joint amphibious and expeditionary operations. ODIN and HELIOS are designed to support afloat maritime CUAS missions but have power margin and power management as limiting factors [153]. At times when ODIN and HELIOS operations are impacted because of the aforementioned limiting factors, L-MADIS can serve as bridge between other ship sensors for CUAS operations utilizing its interoperable C2 communications suite. With L-MADIS serving as bridge, information associated with UAS threats to the ship's vital area can be exchanged between L-MADIS and other ships sensors. The exchanged information can be utilized by L-MADIS and/or the ship's sensor to employ detection and/or mitigation techniques against UAS threats. L-MADIS presents a mechanism to mitigate these limiting factors through future interoperability.

In December 2019, the DOD made the decision to streamline various counter-small unmanned aerial system (C-sUAS) programs and named the U.S. Army as the executive agent. In support of this decision, the DOD established (Jan 6. 2020) the JCO Joint C-sUAS led by the U.S. Army and issued DOD Directive 3800.01E, DOD Executive Agent for C-sUAS for UAS Groups 1, 2, and 3. In [2], it is stated that JCO identified eight C-sUAS solutions categorized into three systems-of-systems approaches and one C2 system:

1. Fixed/Semi-Fixed Systems
    - Fixed Site-Low, Slow, Small Unmanned Aircraft Integrated Defeat System

(FS-LIDS): sponsored by [U.S.] Army.
    - Negation of Improvised Non-State Joint Aerial-Threats (NINJA): sponsored by [U.S.] Air Force.
    - Counter-Remote Control Model Aircraft Integrated Air Defense Network (CORIAN): sponsored by [U.S.] Navy.
2. Mounted/Mobile System
    - L-MADIS: sponsored by [U.S.] Marine Corps.
3. Dismounted/Handheld Systems
    - Bal Chatri: sponsored by Special Operations Command.
    - Dronebuster: no sponsor [but] commercial off-the-shelf capability.
    - Smart Shooter: no sponsor [but] commercial off-the-shelf capability.
4. Command and Control
    - Forward Area Air Defense Command and Control (FAAD-C2): sponsored by [U.S.] Army.
        - FAAD-C2 [includes] interoperable systems like the Air Force's Air Defense System Integrator (ADSI) and the Marine Corps' Multi-Environmental Domain Unmanned Systems Application Command and Control (MEDUSA C2) [2].

Currently, the USN employs CORIAN while the USMC employs L-MADIS. CORIAN detects, identifies, tracks, and mitigates UAS threats for Groups 1-3 using CACI's Skyview passive RF sensors and combined mitigation elements with precision techniques to mitigate damage to the surrounding RF spectrum and existing communications. The components of L-MADIS are: RPS-42 multi-mission hemispheric air surveillance Active Electronically Scanned Array radar system, CM202 multi-sensor imaging system, SkyView-Directional Indication Version 2 passive RF detection architecture, and Modi II Electronic Countermeasure system. The dismounted/handheld systems are standalone without requirements for data retention and passing of information when utilized for UAS engagement.

Advances in technology have positively attributed to the augmentation in UAS aerodynamics, communications, sonar, propulsion, precision navigation, and digital signal processing sensors [156]. With these advances, USN and USMC CUAS future technology must incorporate and ascertain the requisite levels of sophistication and interoperability to maintain superiority in the joint operational environment.

6.2 Detection and Tracking Techniques

6.2.1 Radar

CUASs with sensors utilizing radar techniques operate by actively transmitting RF signal on a specific frequency, with a certain amount of power, and in a chosen direction then subsequently detecting the signal reflected from the target. Radars are typically two dimensional, providing range and direction, or three dimensional, providing range, elevation angle, and azimuth. The type of radar most common in CUASs is the Doppler radar which uses the Doppler effect to determine velocity of the reflected signal.

L-MADIS's RPS-42 radar is software-defined and pulse-Doppler which uses pulse-timing techniques to determine range and the Doppler effect to determine velocity. RPS-42 applies time to understand the three dimensional (3D) environment with regard to elevation to create what is considered the four dimension. RPS-42 operates in S-band (2-4 GHz) with frequencies within the super high frequency (SHF) and UHF bands; it detects, tracks and classifies UAS Groups 1 and 2 at ranges of up to 10km [157].

The USN's Advanced Refractive Effects Predication System (AREPS) is a Microsoft Windows-based software application that provides an electromagnetic (EM) system propagation assessment tool designed to provide assessments for communications, radar, strike and electronic countermeasures, electronic support measures (ESM) vulnerabilities, and many other applications with its advance propagation model and its other embedded propagation models [158]. The performance of a radar system is dependent on the environment in which it operates and the radar cross-section of the targets. Pulse modulations techniques are used to address the varying radar cross-sections observed with target UASs. Current CUASs do not provide radar probability of detection, propagation loss, signal-to-noise ratio, passive RF sensor/receivers vulnerability, and radar capability versus range, height, and bearing from the radar transmitter. AREPS has the capability to compute and display the aforementioned information using its advance propagation model, a hybrid ray-optic and parabolic equation model [159]. AREPS's advance propagation model is accredited by the Chief of Naval Operations for EM propagation modeling in the 2MHz to 57GHz range for use in USN systems [158]. Integration of AREPS into future CUASs can provide the capability to adjust radar and RF detection and tracking techniques for the real-time environment and mitigate potential vulnerabilities and shortfalls.

6.2.2 Radio Frequency

In Department of Homeland Security (DHS)'s CUAS technology guide [47], it is stated that sensors utilizing RF techniques "rely on antennas to [passively] receive and computers to [process and analyze] RF signals associated with communications between the GCS and the unmanned aerial vehicle (UAV)". Next, the intercepted signals go through analysis to examine RF signatures and modulation characteristics for correlation to UAS signals. The technology guide further states, the analysis provides the capability to identify UAS models and manufacturers and locate where the transmitted signal originates whether it is the UAV and/or the GCS It is recognized that CUASs utilize libraries of known UAS RF signatures and modulation characteristics for comparison and correlation to the detected signals for the purpose of UAS classification and/or identification. The DHS suggests signature libraries should be periodically updated to include additional UAS signatures and update existing signatures [47]. There are several methods designed to assist in locating the origin of a detected UAS associated signal but the more common methods are: direction finding (DF), time difference of arrival (TDOA), and frequency difference of arrival (FDOA) [47]. The difference between the methods is the technique use in the calculation/estimation of location [160]:

- DF utilizes angle of arrival (AOA) involving one or more detection sensors.
- TDOA utilizes the time difference between the same signal received at two or more different detection sensors.
- FDOA utilize the frequency difference due to the Doppler shift observed in same signal received at two or more different detection sensors.

The detection ranges of RF sensors are affected by many factors which include terrain, electromagnetic interference, RF reflecting surfaces (e.g. structures introducing multi-path), and line of sight to target UAS. These factors create complex operational conditions for RF sensors which affects the effective range of the sensor. Due to the complexity associated with the environment conditions RF sensors are employed in, detection ranges are specified under ideal conditions. CORIAN and L-MADIS both utilize the CACI Skyview RF sensor which has a vendor specified detection range of more than 9.9km. Their effective detection ranges for the passive RF sensor are dependent on mission size, geographic conditions, and RF environment. The ability to compute and display passive RF probability of detection, similar to the capabilities of AREPS, would inform the employment of other detection and

tracking techniques.

As stated in Chapter 4 Section 4.4 UASs utilize radio frequencies within the 433MHz to 5.8GHz range. The most common radio frequencies include, but not limited to, 433MHz, 915MHz, 2.4GHz, and 5.8GHz. Current CUASs' RF sensors have the ability to detect in the frequency band of 20MHz to 6GHz. With 5G technology at the center of future communications, it is expected that UASs will increasingly shift to 5G. 5G frequency range designations are [161]:

- Frequency Range 1: defined as sub 6GHz range; 450MHz-6GHz.
- Frequency Range 2: defined as the millimeter wave range; 24.25GHz-52.6GHz.

In addition to the aforementioned frequency ranges, there is interest and support in exploring the 6GHz-24GHz range for 5G use [162]. Current CUAS RF sensors implemented within CORIAN and L-MADIS lack the capability and modularity to address the 5G frequency range above 6GHz. Future CUASs should be capable of detecting and tracking UASs operating at frequencies above 6GHz.

Current technology exists to address the limitations for 5G detection but requires testing before integration into future CUASs. An example of available technology is CRFS's RFeye Node 100-40, a 9KHz-40GHz intelligent wideband receiver. CRFS is United Kingdom based company that specializes in RF spectrum monitoring, management, and geolocation. The RFeye Node 100-40 is a single channel receiver with switchable RF inputs. Its signal analysis features are 100MHz bandwidth with a tuning resolution of 1Hz. The detailed specifications of RFeye Node 100-40 [163] provide an example baseline of technical considerations for future RF sensor integrated into CUASs.

6.2.3 Electro-Optical/Infrared

EO/IR techniques collect visible and infrared light information in the electromagnetic spectrum. Visible light is limited to daytime collection while infrared light can be collected daytime or nighttime. CORIAN's current configuration does not have an EO/IR capability while L-MADIS utilizes Ascent Vision Technologies' CM202U for the capability [1]. CM202U is gyro-stabilized and its software utilizes two Ascent Vision Technologies proprietary threat detection algorithms; moving threat and static threat. The algorithms are

designed to assist the CUAS human operator with a high probability of detection. The probability is not advertised. The IR capability operates in the medium wavelength infrared (MWIR) range of 3.0-5.0 µm. CM202U is configured with fields of view of 9 degrees to 1.1 degrees and 28.7 degrees to 1.7 degrees for EO and IR, respectively. The azimuth is a continuous 360 degrees and the slew rate is 360 degrees per second. Image resolution is 1280x720 for EO and 640x512 for IR. Elevation capability is reported as +130/-30 degrees. The EO/IR detection technique is limited by environmental conditions which directly affect detection ranges. The IR detection technique in the MWIR range provides the longest detection ranges when compared to short wavelength infrared (SWIR) and long wavelength infrared (LWIR) range . It is also less susceptible to absorption and scattering than LWIR. Line of sight is a necessity for both EO and IR.

Also in the DOD's inventory of EO/IR capability for CUAS is Ascent Vision Technologies' CM262, designed for ground-based CUAS. A maritime version of CM262, CM262M, is designed for the maritime use. CM262 is gyro-stabilized and has the additional capabilities of SWIR and a laser range finder with range of up to 10km [164]. The SWIR capability has image resolution of 640 x 512 and a field of view of 14-1.4 degrees. The MWIR capability differs from CM202 with an image resolution of 1280x1024 and field of view of 46.2-2.4 degrees. Elevation capability is reported as +90/-10 degrees . The addition of SWIR detection and the laser range finder, inherent in the CM262, would complement current L-MADIS EO/IR capabilities. Current EO/IR capabilities have detection range and image resolution limitations because of the laws of physics. To increase detection ranges and image resolution for future CUAS EO/IR capabilities, adapting a larger focal plane array is a solution but comes with a trade-off between size, weight, and power consumption of the overall sensor.

6.2.4 Acoustic

Acoustic detection techniques are not implemented in CORIAN nor L-MADIS as a primary detection source. Future USN and USMC CUASs should adapt acoustic detection techniques for the appropriate mission size, geographic conditions, and acoustic environment secondary to the primary sensor(s). The adaptation could allow the acoustic detection technique to validate or further identify a target UAS by uniquely identifying sound signatures associated with particular UAS. A major factor to consider is the technique's sensitivity to ambient

noise. Acoustic detection ranges vary based on the environment which limits acoustic sensor capabilities.

6.2.5 Combined Sensors

With the aforementioned detection techniques, numerous combinations are implemented in CUASs to provide detection, tracking, and identification capabilities for the operational environment. A comparison of detection techniques capabilities against the UAV and GCS are described in Table 6.3. Detection limitations are described in Table 2.9. Table 2.9 and Table 6.3 describe the information taken into consideration when choosing a singular detection technique or a combination of techniques with respect to the operation environment of employment.

Table 6.3. Comparison of CUAS Detection Techniques against UAV/GCS. Source: [47].

Modalities	Active/Passive	Detect UAV	Detect GCS	Locate/Track UAV	Locate/Track GCS
Radar	Active	Yes	No	Yes	No
EO	Passive	Yes	No	Yes	No
IR	Passive	Yes	No	Yes	No
RF	Passive	Yes	Yes	Yes	Yes
Acoustic	Passive	Yes	No	Yes	No

The capability to detect, track, and locate both components of a UAS, UAV and GCS, currently resides with only one method/technique; RF.

6.3 Mitigation Techniques

Mitigation techniques are divided into two categories; kinetic and non-kinetic. Of the techniques described in Table 6.2, RF jamming, GNSS jamming, and spoofing are considered non-kinetic, while dazzling, laser, high power microwave, nets, projectile, and collision drone are considered kinetic. Several techniques from both categories are utilized in CUASs against current threats. Emerging UAS threats present challenges to current CUAS mitigation techniques in which some are attributed to UAS adaptation of:

- 5G communication technology and protocols.
- Low probability of intercept/detection waveforms.

- Anti-jamming capabilities integration.

In addition to the adaptations listed above, further development of automation and UAS collaboration add to the challenges and the need for improved interoperability. UAS automation is described as shown in Table 6.4.

Table 6.4. UAS Automation Level. Source: [165]

Level 1: Slave	Assisting piloting, [with] reaction to disturbance [environment/interference].
Level 2: Automated	Maintains its flying order and receives higher level orders[; automation minimal].
Level 3: Automated Navigation	a priori mission plan.
Level 4: Response from Contextual Data	Collision Avoidance [without] human intervention; [Requires] minimum knowledge of surrounding environment, reacts to events, uses active [sense and avoid system], and requires mission plan.
Level 5: Decision-Maker (Expert System)	[Decision are made] from contextual data: navigation in unknown environment, complex missions, coordination and collaboration of signals.

UAS Groups 1, 2, and 3 commonly have the capabilities of Level 1 and Level 2 automation. There is an increase in the availability of Level 3 and Level 4 automation while Level 5 automation has current limited availability commercially. Level 5 automation consists of artificial intelligence and advance sense and avoid systems. The objective is to provide decision making with networked computing, perceptive sensors for time and space, intelligent adjustment capabilities, and adaptive control [165]. Often employed with a type of automation, UAS collaboration is divided into four types as describe in Table 6.5.

Table 6.5. UAS Collaboration Types. Source: [165]

Type 1: Isolated Individual UAS	Advantages [of use]: piloted or autonomous [with] specific mission to perform; [affordability].
Type 2: Group of Individuals UASs (Isolated with own mission but not coordinated)	Advantages [of use]: sphere of action may be different for each mission, increased numbers, and increases success of attacks by defenses saturation.
Type 3: Team of UASs (All members assigned specialized tasks and coordinated by [master controlling node])	Advantages [of use]: particularly effective against divided attack targets, Level 3 [automation] allows automatic navigation, synchronized actions, but no update to mission plans based on field activities.
Type 4: UAS Swarm	Uniform mass of undifferentiated individual UAS [without a master controlling node] at Level 4 or 5 [automation]. Advantages of use: efficient based on numbers, emergent large group behaviors and reactions, not controllable or automated, decentralized intelligence.

UAS Group 1, 2, 3, and threats employing combinations of high level automation (Table 6.4 Levels 3 and above) and certain types of collaboration (Table 6.5 Types 2, 3, and 4) present

challenges (i.e., saturation limitations) for defensive measures utilizing current CUASs. The combinations are also in line with UAS use tactics presented in Section 2.6.

6.4 USN and USMC CUAS Interoperability

The Chairman of the Joint Chiefs of Staff states that interoperability is "the ability to act together coherently, effectively, and efficiently to achieve tactical, operational, and strategic objectives" [166]. In the DOD's C-sUASs Strategy [32], interoperability shortfalls in interim CUASs are identified as:

- Lack of common architecture standard as basis for systems.
- Need for common C2 standards to meet future joint common architecture.
- Lack of modularity for plug-and-play.
- Need for central repository for common UAS threat database.

It is recommended that a common baseline architecture be used as the foundation for DoN CUASs to enable interoperability and supported by applying:

- Configuration management to develop and apply procedures and standards to manage evolving software.
- Change management to manage change requests created by requirements or mission shifts.

Along with configuration and change management, applying the Doctrine, Organization, Training, Material, Leadership, Personnel, and Facilities (DOTMLPF) framework to leverage a joint vantage point can assist in meeting joint requirements and interoperability while developing capabilities and training to obtain the best effects possible.

6.5 Summary

In summary, current CUAS USN and USMC technologies have limitations in detection and mitigation capabilities along with interoperability shortfalls (Section 6.4). Coupled with the limitations and shortfalls is UAS adaption of 5G technology, low probability of intercept/detection waveforms, and anti-jamming capabilities. UAS are also being developed with advanced automation, collaboration, aerodynamics, communications, sonar,

propulsion, precision navigation, and digital signal processing capabilities [156]. Current technologies exist to address the limitations and we identified solutions to address interoperability shortfalls. To counter UAS technological advances, future CUAS must adapt the technology that:

- extends its RF detection frequency ranges to encompass 5G frequency ranges,
- provides radar and RF propagation modeling,
- extends EO/acIR detection ranges and image resolution, and
- incorporates two or more techniques for each of its detection and mitigation functions.

Interoperability shortfalls are addressed by adapting a common baseline architecture and applying configuration management, change management, and the DOTMLPF framework. USN and USMC level of efforts and requirements must be aligned to ascertain the requisite levels of sophistication and interoperability to maintain superiority in the joint operational environment.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 7:
Modeling and Simulation of the Effectiveness of CUAS Technologies

This chapter discusses the effectiveness of the current CUAS technologies against current and emergent UAS threats. We leverage generic modeling and simulations based upon current CUAS subsystems to highlight shortfalls and limitations associated with varying degrees of UAS threats. We further establish recommended means to address current and emergent UAS threats. ***For the full code set see https://gitlab.nps.edu/allen.golphin/cuas-simulation-and-modeling***.

7.1 Counter Unmanned Systems Effectiveness Factors

Factors in the effectiveness of CUAS technologies are the detection and mitigation techniques, discussed in Tables 6.1 and 6.2, selected for employment against the CUAS kill chain. A CUAS can consist of a singular or multiple subsystem configurations. A probability of detection or probability of mitigation can be determined for the subsystems in the CUAS. With interoperability, the introduction of a new subsystem or removal of a current subsystem can affect the overall effectiveness and reliability of the system or an individual subsystem. To assess overall effectiveness of a CUAS, a model was designed and simulated to demonstrate how the probabilities and reliabilities of individual subsystems affect the overall effectiveness of the CUAS in addition to the factors of range, targets, and terrain. The model is applied to current and emerging UAS threats with hypothetical probabilities for detection and mitigation functions of the subsystem. All probabilities are represented in decimal format.

7.2 Model Description, Limitations, Assumptions, and Constraints

We define the following reserved terms for this chapter.

Definition 7.2.1 (Effectiveness)**.** We define *Effectiveness* as the degree to which a CUAS is successful in detection and mitigation functions against UAS threats.

Definition 7.2.2 (Reliability)**.** We define *Reliability* as the degree to which a system and/or subsystems can be depended on to be functionally operable, as perceived, regardless of accurate functionality.

Definition 7.2.3 (Probability of Detection)**.** We define *Probability of Detection* as the likelihood of a CUAS accurately discovering the presence of UAS threats.

Definition 7.2.4 (Probability of Mitigation)**.** We define *Probability of Mitigation* as the likelihood of a CUAS meaningfully disabling the UAS threat, with *meaningful* defined dependent on system goals (e.g. denial of service, kinetic destruction, disorientation, etc.).

The model is able to simulate effectiveness against current UAS threats or emerging UAS threats. Equation (7.1) gives a description of the model.

$$E_{(CUAS)} = R_{(CUAS)} \times PofD_{(CUAS)} \times PofM_{(CUAS)} \tag{7.1}$$

Where $E_{(CUAS)}$ is Effectiveness of the CUAS, $R_{(CUAS)}$ is Reliability of the CUAS, $PofD_{(CUAS)}$ is Probability of Detection for the CUAS, and $PofM_{(CUAS)}$ is Probability of Mitigation for the CUAS. The model is limited to CUASs that have a detection capability and a mitigation capability. Each capability has one or more subsystems employing a specific technique discussed in Chapter 6. The overall reliability is calculated assuming the CUAS subsystems are in a series as shown in Figure 7.1. The detection system and mitigation system represent the underlying subsystems shown in Figure 7.2. Equation (7.2) gives a description of the $R_{(CUAS)}$ component of the overall model, $E_{(CUAS)}$.

$$R_{(CUAS)} = R_D \times R_M \times R_{(UI)} \tag{7.2}$$

In Equation (7.2), R_D is the Reliability of the Detection subsystem, R_M is the Reliability of the Mitigation subsystem, and $R_{(UI)}$ is the Reliability of the User Interface which is constant for this model and represents a user interface that has a very low failure rate.

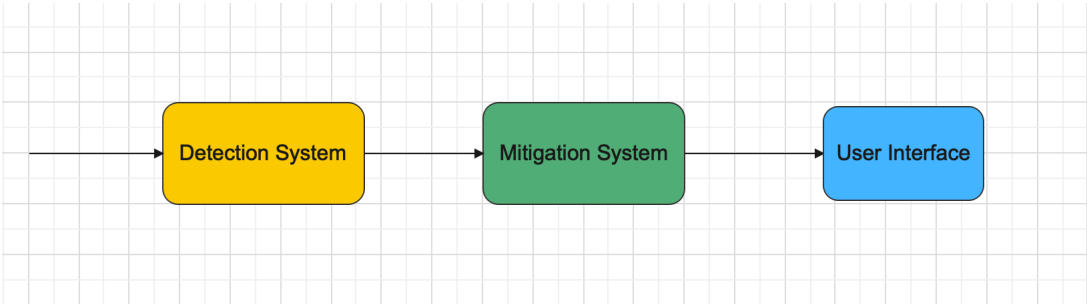


Figure 7.1. CUAS Reliability Block Diagram.

The detection capability consists of a base configuration of three detection subsystems each representing a detection technique discussed in Chapter 6. This is assumed for the mitigation capability as well. It is assumed subsystems are operating as an active redundant parallel system each requiring 1 of 3 parallel branches to operate. Figure 7.2 shows the relationship and dependency of the subsystems, reflected as parallel subsystems.

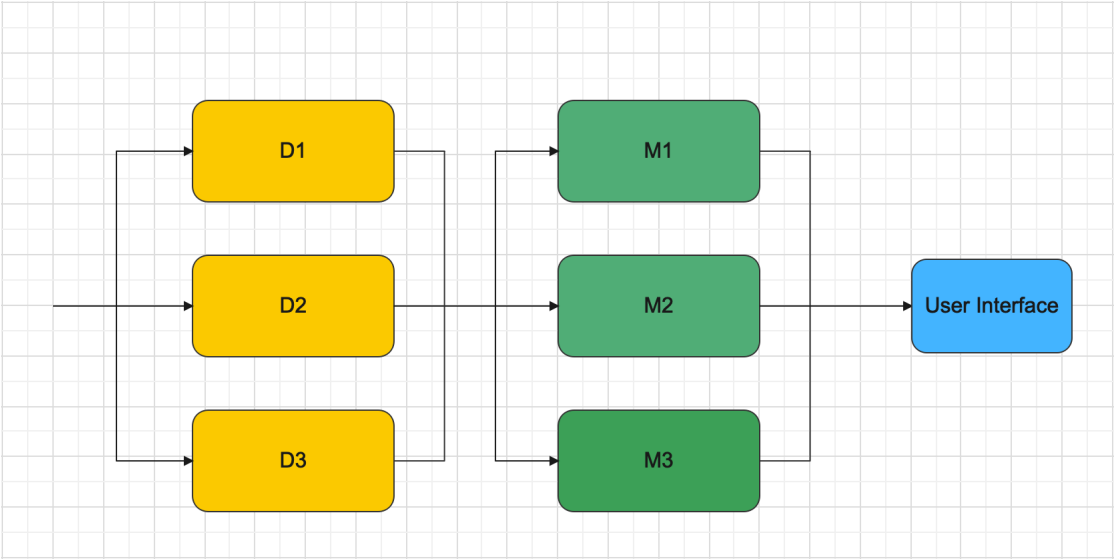


Figure 7.2. CUAS Subsystems Reliability Overview.

The reliability for the detection and mitigation subsystems are components of the $R_{(CUAS)}$ are described as:

$$R_D = (1 - R_{D_1}) \times (1 - R_{D_1}) \times (1 - R_{D_3}) \tag{7.3}$$

$$R_M = (1 - R_{M_1}) \times (1 - R_{M_2}) \times (1 - R_{M_3}) \tag{7.4}$$

where R_{D_n} and R_{M_m} are each calculated using the formula $e^{-\lambda t}$ [167]. The *mean time between failures (MTBF)* is assumed different for each subsystem and will be applied and allocated in the model as hypothesized for mission time for 30-90 days which converts to 720-2160 hours of mission time, respectively. The $failures$ are the estimated number of equipment failures that occur over the course of total mission time. In the formula, $\lambda = 1/(\text{MTBF})$, t is the mission time represented in hours, and $e \approx 2.718281828$. *MTBF* is represented by the ratio $t/failures$. The purpose is to show variation that is observed during the different mission sets and environments. The model allows for the addition or subtraction of subsystems with the appropriate application of subsystem dependency for reliability.

The probability of detection, $PofD_{(CUAS)}$, component of $E_{(CUAS)}$ is determined by the hypothetical probability of detection, $HP_{CUAS_{(Detect)}}$, which is limited to the factors of range, targets, and terrain to show their effects on the overall effectiveness of the CUAS. Equation (7.5) represents the probability of detection with factors of range, targets, and terrain taken into account.

Definition 7.2.5 ($targetsFactor$)**.** We define $targetsFactor$ as the degree to which the number of simultaneous UAS threats affects the probability of detection and mitigation of the CUAS.

Definition 7.2.6 ($terrianFactor$)**.** We define *terrainFactor* as the degree to which the physical features of the environment and terrain where the CUAS is employed affects the probability of detection and mitigation of the CUAS.

$$PofD_{(CUAS)} = HP_{CUAS_{(Detect)}} - targetsFactor_D - terrainFactor_D \tag{7.5}$$

where $HP_{CUAS_{(Detect)}}$ probability ranges are hypothesized based on UAS tactics described in Section 2.6. $HP_{CUAS_{(Detect)}}$ is a continuous variable with uniform distribution. We define

the hypothetical ranges for probability of detection as:

- If the range is 1 mile, $HP_{CUAS_{(Detect)}} = .97 - .99$.
- If the range is 2 mile, $HP_{CUAS_{(Detect)}} = .85 - .97$.
- If the range is 3 mile, $HP_{CUAS_{(Detect)}} = .75 - .85$.

Definition 7.2.7 ($targets_{(weight)}$)**.** We define $targets_{(weight)}$ as the degree of degradation for the number of simultaneous UAS threats.

Definition 7.2.8 ($terrain_{(weight)}$)**.** We define $terrian_{(weight)}$ as the probability range to the physical features of the CUAS's environment and terrain where the CUAS is employed affects the probability of detection and mitigation of the CUAS.

The number of targets factor, $targetsFactor_D$, and terrain factor , $terrainFactor_D$, affects the hypothetical probability of detection as such:

$$targetsFactor_D = HP_{CUAS_{(Detect)}} \times targets_{(weight_D)} \tag{7.6}$$

$$terrainFactor_D = HP_{CUAS_{(Detect)}} \times terrain_{(weight_D)} \tag{7.7}$$

where the weights of targets and terrain are hypothetically as follows to demonstrate an effect on the hypothetical probability of detection:

- $targets_{(weight_D)} = .01 - .15$.
- $terrain_{(weight_D)} = .01 - .25$.

The variables $targets_{(weight_D)}$ and $terrain_{(weight_D)}$ are continuous and uniformly distributed.

The probability of mitigation, $PofM_{(CUAS)}$, component of $E_{(CUAS)}$ is determined the by hypothetical probability of mitigation, $HP_{CUAS_{(Mitigate)}}$, which is limited by the same factors as $HP_{CUAS_{(Detect)}}$. Equation (7.8) represents the probability of mitigation with factors of range, targets, and terrain taken into account.

$$PofM_{(CUAS)} = HP_{CUAS_{(Mitigate)}} - targetsFactor_M - terrainFactor_M \tag{7.8}$$

where $HP_{CUAS_{(Mitigate)}}$ probability ranges are hypothesized in the same manner as $HP_{CUAS_{(Detect)}}$. $HP_{CUAS_{(Mitigate)}}$ is a continuous variable with uniform distribution. The hypothetical ranges for probability of mitigation are defined as:

- If the range is 1 mile, $HP_{CUAS_{(Mitigate)}} = .90 - .99$.
- If the range is 2 mile, $HP_{CUAS_{(Mitigate)}} = .80 - .90$.
- If the range is 3 mile, $HP_{CUAS_{(Mitigate)}} = .65 - .80$.

The number of targets factor, $targetsFactor_M$, and terrain factor , $terrainFactor_M$, affects the hypothetical probability of mitigation as such:

$$targetsFactor_M = HP_{CUAS_{(Mitigate)}} \times targets_{(weight_M)} \tag{7.9}$$

$$terrainFactor_M = HP_{CUAS_{(Mitigate)}} \times terrain_{(weight_M)} \tag{7.10}$$

where the weights of targets and terrain are hypothetical to demonstrate an effect on the hypothetical probability of mitigation:

- $targets_{(weight_M)} = .01 - .25$
- $terrain_{(weight_M)} = .01 - .20$.

The variables $targets_{(weight_M)}$ and $terrain_{(weight_M)}$ are continuous and uniformly distributed.

The model is limited to UAS Groups 1, 2, and 3 as identified in Figure 2.1 employed by adversarial operators as describe in Chapter 3. Table 7.1 provides the assumptions of the capabilities and reliability factors of CUASs against current UAS threats. The assumed values in Table 7.1 are estimations and are hypothetical based on professional experience and generic vendor statements. There is no correlated data or actual use of documented data to avoid inadvertently compromising any sensitive information. The model can be used with actual data values to provide a system specific representation but should be used in a facility and on a system at the appropriate classification level.

Table 7.1. CUASs Assumptions against Current UAS Threats.

	Nominal	Min	Max
$failures_{D_1}$ (# of failures)	3	1	12
$failures_{D_2}$ (# of failures)	2	1	16
$failures_{D_3}$ (# of failures)	4	1	9
$failures_{M_1}$ (# of failures)	2	1	4
$failures_{M_2}$ (# of failures)	4	1	10
$failures_{M_3}$ (# of failures)	3	1	6
t (hours)	1350	720	2160
e	2.718281828	-	-
$HP_{CUAS_{(Detect)}}$	.95	.75	.99
$targets_{(weight_D)}$	.04	.01	.15
$terrain_{(weight_D)}$	.05	.01	.25
$HP_{CUAS_{(Mitigate)}}$	.95	.65	.99
$targets_{(weight_M)}$	.03	.01	.25
$terrain_{(weight_M)}$	.05	.01	.20

The model was applied against CUAS assumptions for emerging UAS threats. The emerging UAS threats are assumed to be utilizing combinations of high level automation Levels 3 and above as described in Table 6.4 and collaboration of Types, 2, 3, and 4 from Table 6.5. In addition to the automation and collaboration, emerging UAS threats are assumed to be utilizing alternate communication channels in which current CUASs have limitations in RF detection as identified in Section 6.2. It assumed emerging UAS threats have reduced their radar, EO/IR, acoustic detection signatures to an acceptable level of risk for stealth [165]. It is assumed the aforementioned advances for emerging UAS threats results in a conservative reduction in $HP_{CUAS_{(Detect)}}$ and $HP_{CUAS_{(Mitigate)}}$ by five percent each with all other factors remaining the same. This resulted in the ranges for hypothetical probability of detection for emerging threats is defined as:

- If the range is 1 mile, $HP_{CUAS_{(Detect)}} = .92 - .94$.
- If the range is 2 mile, $HP_{CUAS_{(Detect)}} = .81 - .92$.
- If the range is 3 mile, $HP_{CUAS_{(Detect)}} = .71 - .81$.

The new weight of targets to show a 15-25% effect on hypothetical probability of detection for emerging threats is defined as:

- $targets_{(weight_D)} = .15 - .25$.

The variable $targets_{(weight_D)}$ is continuous and uniformly distributed.

The new ranges for hypothetical probability of mitigation for emerging threats is defined as:

- If the range is 1 mile, $HP_{CUAS_{(Mitigate)}} = .86 - .94$.
- If the range is 2 mile, $HP_{CUAS_{(Mitigate)}} = .76 - .86$.
- If the range is 3 mile, $HP_{CUAS_{(Mitigate)}} = .62 - .76$.

$HP_{CUAS_{(Mitigate)}}$ is a continuous variable with uniform distribution.

The new weight of targets to show a 15-30% effect on hypothetical probability of mitigation for emerging threats is defined as:

- $targets_{(weight_M)} = .15 - .30$

The variables $targets_{(weight_M)}$ is continuous and uniformly distributed. With the adjustments for emergent UAS threats, Table 7.2 provides the assumptions of the capabilities and reliability factors of CUASs against emerging UAS threats.

Table 7.2. CUAS Assumptions against Emerging UAS Threats.

	Nominal	**Min**	**Max**
$failures_{D_1}$ (# of failures)	3	1	12
$failures_{D_2}$ (# of failures)	2	1	16
$failures_{D_3}$ (# of failures)	4	1	9
$failures_{M_1}$ (# of failures)	2	1	4
$failures_{M_2}$ (# of failures)	4	1	10
$failures_{M_3}$ (# of failures)	3	1	6
t (in hours)	1350	720	2160
e	2.718281828	-	-
$HP_{CUAS_{(Detect)}}$	.90	.71	.94
$targets_{(weight_D)}$	.15	.15	.25
$terrain_{(weight_D)}$	.05	.01	.25
$HP_{CUAS_{(Mitigate)}}$	.90	.62	.94
$targets_{(weight_M)}$	.15	.15	.30
$terrain_{(weight_M)}$	.05	.01	.20

The model was run as a Monte Carlo Simulation under each set of assumptions discussed in Table 7.1 and Table 7.2, separately. The number of simulations in the Monte Carlo Simulation was set to 10,000.

7.3 Effectiveness Against Current UAS Threats

The results from the model run under Table 7.1 assumptions showed reliability for detection subsystems varied between a minimum probability of 0.3301 and a maximum probability of 0.9985 as seen in Table 7.3. The data is skewed to the left with 75% of the probabilities above 0.7588 and the remaining 25% below 0.7588, see Figure 7.3. The graph shapes shows that the majority of the simulations produce detection subsystems that are calculated to be reliable 75.88% of the mission time. This translates to only 3/4 of CUAS detection subsystems operating with reliability at or above 75.88%. The standard deviation is 0.1293 and considered high with the probabilities more spread out from the mean of 0.8486. The model indicates the detection subsystems would be up and operating at an average of 84.86% of the time. The data spread is also reflected in the large interquartile range (IQR) probability of 0.2009. In the data, it is assessed that a probability value of (1.5×IQR) more than the 75th quartile or $(1.5 \times \text{IQR})$ less than the 25th quartile is an outlier. Therefore, any probability values lower than 0.4575 are considered outliers. There are outliers present below the probability of 0.4575 which is attributed to when the number of $failures$ for the detection subsystems occur near or at the max value for the course of their respective total mission time. This results in a low *MTBF* (represented in hours), which means the detection subsystems failures are occurring closer together in time. CUAS detection subsystems experiencing low *MTBF* show reduced reliability probabilities. This highlights that all detection subsystems of a CUAS must demonstrate very low number of $failures$ or no number of $failures$ for the entire duration of the mission to maintain high probability of reliability. High probability of reliability in the detection subsystems contributes to the overall effectiveness and reliability of the CUAS for operations against current UAS threats. Future CUASs development and design must feature improved operating functionality to get better system reliability. Discounting the outliers, the reliability probability would range from probabilities of 0.4575 to 0.9985 indicating uncertainty in the reliability of the detection subsystem.

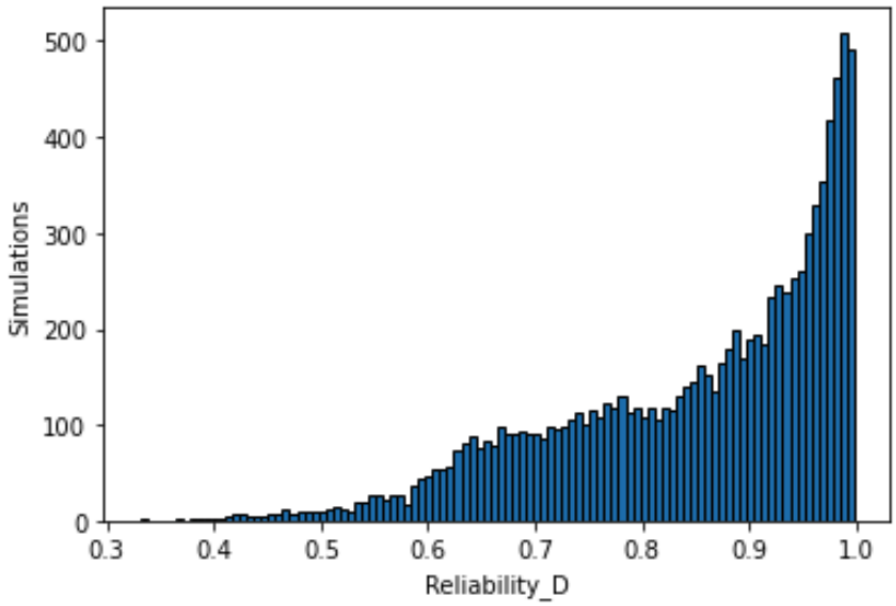


Figure 7.3. Detection Subsystem Reliability Histogram (Current).
Note: Scale 0-500 for number of simulations and 0.3-1.0 for reliability probability.

Table 7.3. Detection Subsystem Reliability Summary Stats (Current).

mean	0.8486
median	0.8858
standard error	0.0013
max	0.9985
min	0.3301
standard deviation	0.1293
range	0.6684
75th Quartile	0.9597
25th Quartile	0.7588
IQR Quartile	0.2009

Reliability for the mitigation subsystems varied between a minimum probability of 0.2866 and a maximum probability of 0.9788 as seen in Table 7.4. The data is skewed to the left with 75% of the probabilities above 0.6897 and the remaining 25% below 0.6897, see Figure 7.4. The graph shapes shows that the majority of the simulations produce mitigation subsystems that are calculated to be reliable at least 68.97% of the mission

time or greater. This translates to only 3/4 of CUAS mitigation subsystems operating with reliability at or above 68.97%. The standard deviation is 0.1307 and considered high with the probabilities more spread out from the mean of 0.7854. The model indicates the mitigation subsystems would be up and operating at an average of 78.54% of the time. The data spread is also reflected in the large IQR probability of 0.2058. In the data, it is assessed that a probability value of $(1.5 \times \text{IQR})$ more than the 75th quartile or $(1.5 \times \text{IQR})$ less than the 25th quartile is an outlier. Therefore, any probability values lower than 0.3810 are considered outliers. There are outliers present below 0.3810 which is attributed to when the number of $failures$ for the mitigation subsystems occur near or at the max value for the course of their respective total mission time. This results in a low *MTBF* (represented in hours) which means the mitigation subsystems failures are occurring closer together in time. CUAS mitigation subsystems experiencing low *MTBF* show reduced reliability probabilities. With 75% of the reliability probabilities below 0.8955, there is an indication that a majority of mitigation subsystems $failures$ were moderate to high for their respective mission times. This highlights that all mitigation subsystems of a CUAS must demonstrate very low $failures$ or no $failures$ for the entire duration of the mission to maintain a high probability of reliability. High probability of reliability in the mitigation subsystems contributes to the overall effectiveness and reliability of the CUAS for operations against current UAS threats. Discounting the outliers, the reliability probability would range from probabilities of 0.3810 to 0.9788 indicating uncertainty in the reliability of the mitigation subsystem. The differences between Figure 7.3 and Figure 7.4 is attributed to the minimum and maximum values estimated for the number of $failures$ in the detection and mitigation subsystem. It highlights the need for the number of $failures$ to be low as possible when considering a CUAS.

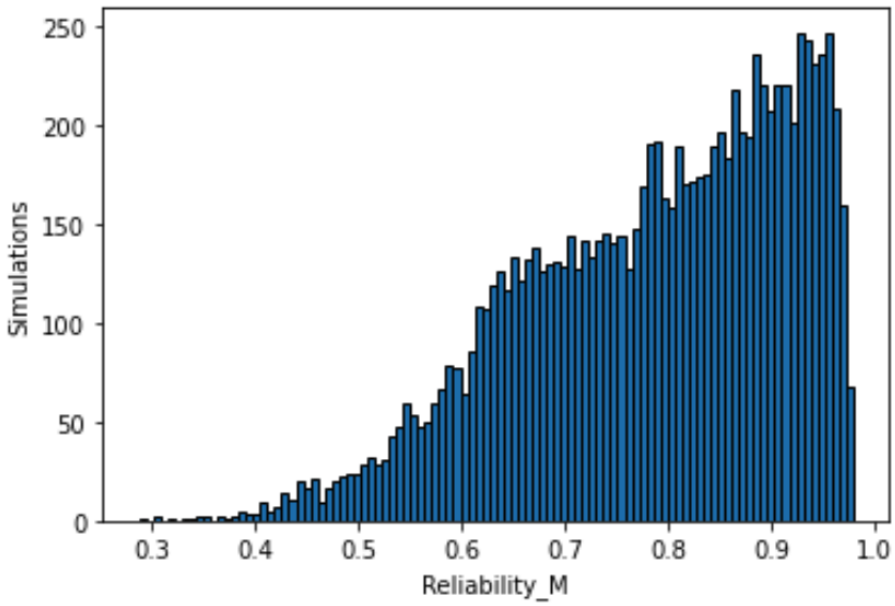


Figure 7.4. Mitigation Subsystem Reliability Histogram (Current).
Note: Scale 0-250 for number of simulations and 0-1.0 for reliability probability.

Table 7.4. Mitigation Subsystem Reliability Summary Stats (Current).

mean	0.7854
median	0.8060
standard error	0.0013
max	0.9788
min	0.2866
standard deviation	0.1307
range	0.6922
75th Quartile	0.8955
25th Quartile	0.6897
IQR Quartile	0.2058

With the reliability of the individual subsystems calculated, they collectively formulate the overall reliability of the CUAS defined in the model by Equation (7.2). The reliability for CUAS varied between a minimum probability of 0.1691 and a maximum probability of 0.9624 as seen in Table 7.5. The data is slightly skewed to the left with 75% of the

probabilities above 0.5516 and the remaining 25% below 0.5516, see Figure 7.5. This translates to only 3/4 of CUASs operating with a reliability at or above 55.16%. The standard deviation is 0.1504 and considered high with the probabilities more spread out from the mean of 0.6599. The model indicates the CUAS would be up and operating at an average of 65.99% of the time. The data spread is also reflected in the large IQR probability of 0.2275. In the data, it is assessed that a probability value of $(1.5 \times \text{IQR})$ more than the 75th quartile or $(1.5 \times \text{IQR})$ less than the 25th quartile is an outlier. Therefore, any probability values lower than 0.2104 are considered outliers. There are outliers present below the probability of 0.2104 which is attributed to when the reliability probabilities for either the detection or mitigation subsystems exhibit low probabilities because the number of $failures$ in the respective system(s) is near or at a high value for the course of the total mission time. This shows how the number of $failures$ each individual subsystem may experience affects the overall reliability of the CUAS. When designing or selecting the detection and mitigation subsystems for a CUAS, consideration should be given to each subsystem's reliability for the effects it could have on CUAS reliability.

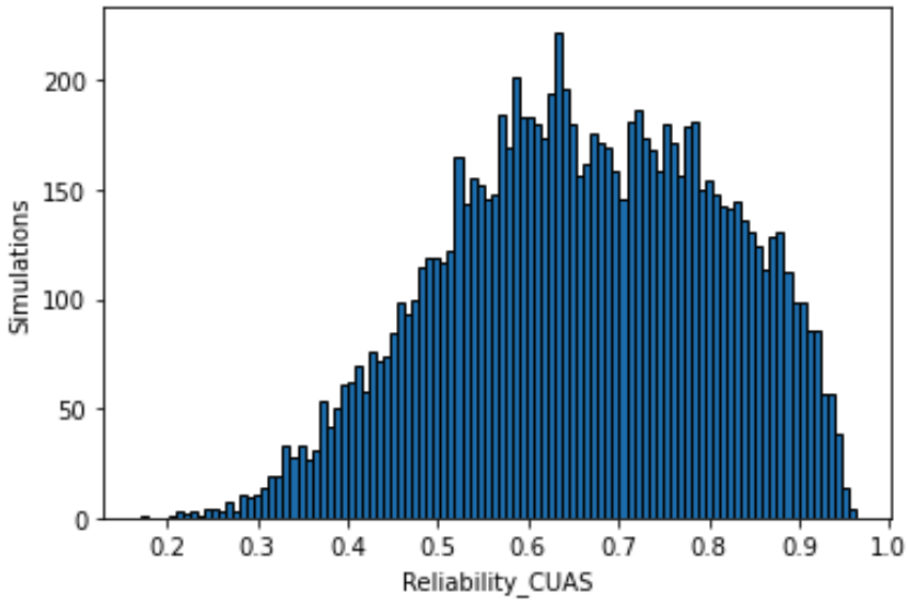


Figure 7.5. CUAS Reliability Histogram (Current).
Note: Scale 0-200 for number of simulations and 0-1.0 for reliability probability.

Table 7.5. CUAS Reliability Summary Stats (Current).

mean	0.6599
median	0.6614
standard error	0.0015
max	0.9624
min	0.1691
standard deviation	0.1504
range	0.7933
75th Quartile	0.7790
25th Quartile	0.5516
IQR Quartile	0.2275

Equation (7.5) defined the hypothetical probability of detection for CUAS which resulted in probabilities varying between the minimum value of 0.5231 and maximum value of 0.9378 as seen in Table 7.6. Figure 7.6 indicates the distribution a fairly normal with 75% of the probabilities above 0.6617 and the remaining 25% below 0.6617. This translates to only 3/4 of CUASs operating with a probability of detection at or above 66.17%. The standard deviation is 0.0780 and considered low with the probabilities less spread out from the mean of 0.7200. The data spread is also reflected in the small IQR probability of 0.1148. In the data, it is assessed that a probability value of $(1.5 \times \text{IQR})$ more than the 75th quartile or $(1.5 \times \text{IQR})$ less than the 25th quartile is an outlier. Therefore, any probability values greater than 0.9487 and lower 0.4895 are considered outliers. There are no outliers present that could skew the data. The input values for Equation (7.5 were varied to demonstrate the effects the factors of range, number of targets, and terrain can have on a CUAS's probability of detection against current UAS threats. In the data produced by the simulations, the average hypothetical probability of detection was 0.7200 which equates to 72.00%. The model indicates that when the CUAS is operating, it has an average 72.00% chance of detecting current UAS threats. Examining Figure 7.6 and Table 7.6, only 25% of the hypothetical probabilities of detection occurred above 0.7765 which indicates a majority of probabilities were at or lower than 0.7765 which equates to 77.65%. The data suggests that to overcome these factors CUAS capabilities should consider designs or developments that provide:

- high probability of detection at extended ranges.
- sensor placement taking into account threat axis and geometry for terrain.

- high probability of detection for a high number of targets simultaneous targets.

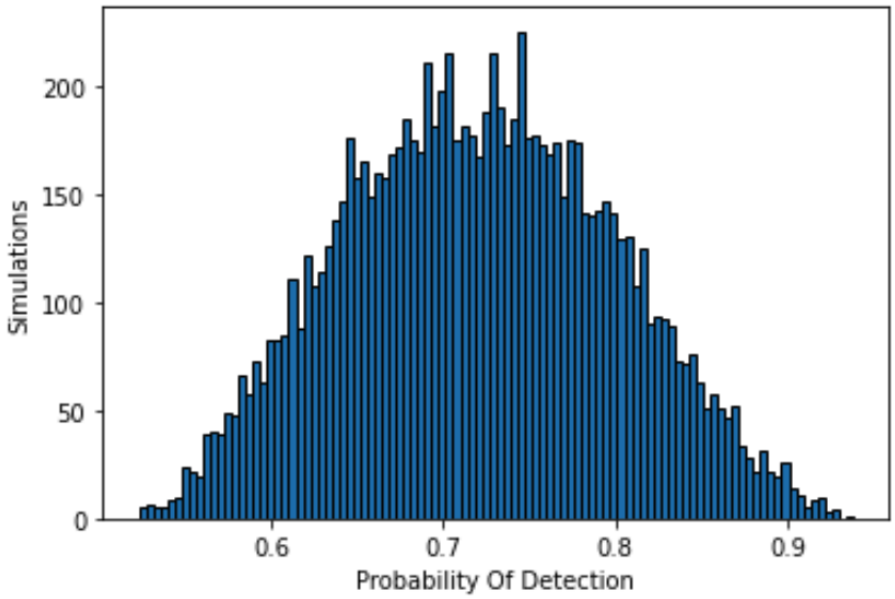


Figure 7.6. CUAS Probability of Detection Histogram (Current).
Note: Scale 0-250 for number of simulations and .5-1.0 for probability of detection.

Table 7.6. CUAS Probability of Detection Summary Stats(Current).

mean	0.7200
median	0.7192
standard error	0.0008
max	0.9378
min	0.5231
standard deviation	0.0780
range	0.4147
75th Quartile	0.7765
25th Quartile	0.6617
IQR Quartile	0.1148

Equation (7.8) defined the hypothetical probability of mitigation for CUAS which resulted in probabilities varying between the minimum value of 0.4532 and maximum value of 0.8670 as seen in Table 7.7. Figure 7.7 indicates the distribution is fairly normal with 75%

of the probabilities above 0.5938 and the remaining 25% below 0.5938. This translates to only 3/4 of CUASs operating with a probability of mitigation at or above 59.38%. The standard deviation is 0.0781 and considered low with the probabilities less spread out from the mean of 0.6505. The data spread is also reflected in the small IQR probability of 0.1112. In the data, it is assessed that a probability value of $(1.5 \times \text{IQR})$ more than the 75th quartile or $(1.5 \times \text{IQR})$ less than the 25th quartile is an outlier. Therefore, any probability values greater than 0.8718 and lower 0.4270 are considered outliers. There are no outliers present that could skew the data. The input values were varied to demonstrate the effects the factors of range, number of targets, and terrain can have on a CUAS's probability of mitigation against current UAS threats. Additionally, the factors of range, number of targets, and terrain weighed differently than in the detection subsystems to simulate the difference that could be present in detection and mitigation subsystems. The data produced an average (mean) probability of mitigation of 0.6505 which equates to 65.05%. The model indicates that when the CUAS is operating, it has an average 65.05% chance of mitigating current UAS threats. Examining Figure 7.7 and Table 7.7, only 25% of the hypothetical probabilities of mitigation occurred above 0.7050 which indicates a majority of probabilities were at or lower than 0.7050 which equates to 70.50%. It demonstrates how those factors affect a CUAS's probability of mitigation against current UAS threats. It cannot be expected that successful detection equates to mitigation because range, number or targets, and terrain dictate which mitigation technique is optimal for employment.

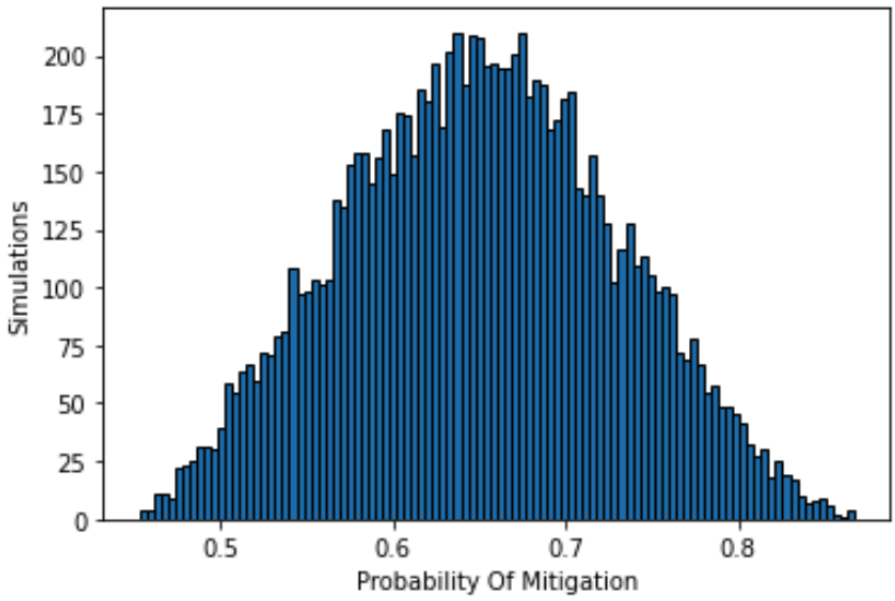


Figure 7.7. CUAS Probability of Mitigation Histogram (Current).
Note: Scale 0-200 for number of simulations and 0.4-0.9 for probability of detection.

Table 7.7. CUAS Probability of Mitigation Summary Stats (Current).

mean	0.6505
median	0.6504
standard error	0.0008
max	0.8670
min	0.4532
standard deviation	0.0781
range	0.4138
75th Quartile	0.7050
25th Quartile	0.5938
IQR Quartile	0.1112

With all components of Equation (7.1) calculated, the effectiveness of CUAS for the simulations resulted in an approximately normal distribution as displayed in Figure 7.8. The effectiveness probabilities varied between the minimum value of 0.0678 and maximum value of 0.6573 as seen in Table 7.8. The standard deviation is 0.0869 and considered low with the probabilities less spread out from the mean of 0.3090. The data spread is also

reflected in the small IQR probability of 0.1220. Calculating for outliers, any probability values greater than 0.5503 and lower 0.0623 are considered outliers. There are outliers present above 0.5503. The model produced an average effectiveness against current UAS threats of 30.90%. The highest observed effectiveness was 65.73% but could be viewed as a rare occurrence. Only 25% of the calculated effectiveness occurred above 0.3673. This demonstrates that when the probabilities for reliability, detection, and mitigation are not at optimal levels, they directly affect a CUAS's overall effectiveness against current UAS threats.

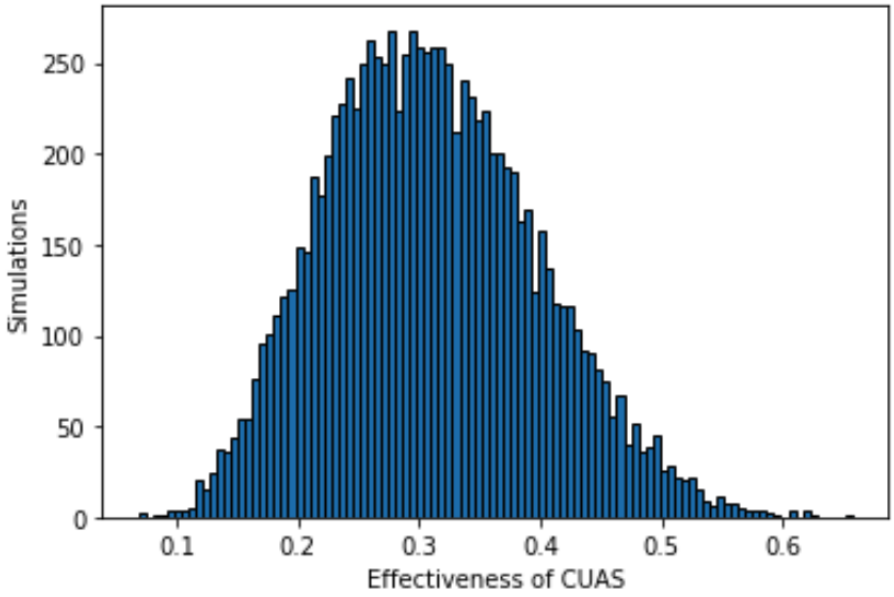


Figure 7.8. CUAS Effectiveness Histogram (Current).
Note: Scale 0-275 for number of simulations and 0-0.7 for effectiveness probability.

Table 7.8. CUAS Effectiveness Summary Stats (Current).

mean	0.3090
median	0.3037
standard error	0.0009
max	0.6573
min	0.0678
standard deviation	0.0869
range	0.5895
75th Quartile	0.3673
25th Quartile	0.2453
IQR Quartile	0.1220

The model indicates that CUAS reliability, probability of detection, probability of mitigation, range, targets, and terrain all are significant factors in calculating the effectiveness of a CUAS. With the conservative values in the model, effectiveness as defined by the model was relatively low. When considering interoperability in future system, addressing the shortfalls and establishing a foundation as discussed in Section 6.4 should be done with respect to the effects they could have on effectiveness of the CUAS.

7.4 Effectiveness Against Emerging UAS Threats

A 5% conservative reduction in $HP_{CUAS_{(Detect)}}$ and $HP_{CUAS_{(Mitigate)}}$ along with the adjustments to $targetsFactor_D$ and $targetsFactor_M$ are reflected in Table 7.2 assumptions. All other factors remain the same. The reduction and adjustments is to account for technological advances (discussed in Section 6.3) that are expected to be present in emerging UAS threats. The reliability for detection subsystems varied between a minimum probability of 0.3316 and a maximum probability of 0.9985 as seen in Table 7.9. The histogram from Figure 7.9 is skewed to the left with 75% of the probabilities above 0.7559 and the remaining 25% below 0.7559. This translates to only 3/4 of CUAS detection subsystems operating with reliability at or above 75.59%. The standard deviation is 0.1300 and considered high with the probabilities more spread out from the mean of 0.8471. The model indicates the detection subsystems would be up and operating at an average of 84.71% of the time. The data spread is also reflected in the large IQR probability of 0.2028. Any probability values lower than 0.4517 are considered outliers. There are outliers present below the probability of 0.4517 which is attributed to when the number $failures$ for the detection subsystems

are near or at the max value for the course of their respective total mission time. Similar to the discussion in Section 7.3, this results in a low *MTBF* (represented in hours) which means the detection subsystem failures are occurring closer together in time. CUAS detection subsystems experiencing low *MTBF* show reduced reliability probabilities. This highlights that all detection subsystems of a CUAS must demonstrate very low number of $failures$ or no number of $failures$ for the entire duration of the mission to maintain high probability of reliability. High probability of reliability in detection subsystems contributes to the overall effectiveness and reliability of the CUAS for operations against emerging UAS threats. Discounting the outliers, the reliability probability would range from 0.4517 to 0.9985 indicating uncertainty in the reliability of the detection subsystem. Detection subsystems exhibiting a high number of $failures$ in future CUAS will negatively impact the CUAS's ability to apply detection techniques discussed in Table 6.1 thus reducing the CUAS's effectiveness and reliability.

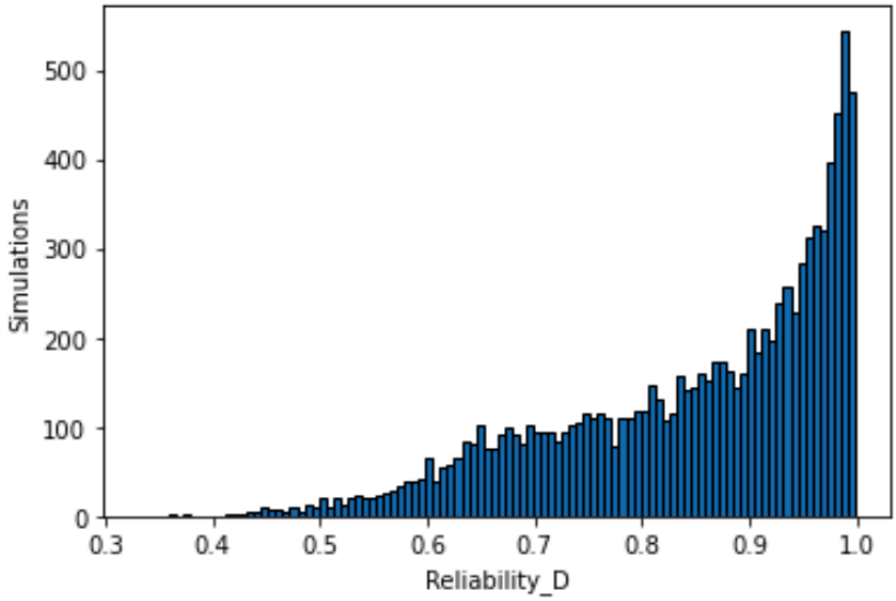


Figure 7.9. Detection Subsystem Reliability Histogram (Emerging).
Note: Scale 0-600 for number of simulations and 0.25-0.1 for reliability probability.

The summary statistics in Table 7.9 show the central tendency and spread of the reliability probabilities for the detection subsystem in the model updated for emerging UAS threats.

The reliability probabilities of the detection subsystem remained relatively the same which it attributed to no changes made for the minimum and maximum input values for number of $failures$ and t represented in hours in Table 7.2 for the detection subsystem.

Table 7.9. Detection Subsystem Reliability Summary Stats (Emerging).

mean	0.8471
median	0.8827
standard error	0.0013
max	0.9985
min	0.3316
standard deviation	0.1303
range	0.6669
75th Quartile	0.9587
25th Quartile	0.7559
IQR Quartile	0.2028

The reliability for the mitigation subsystem varied between the minimum probability of 0.2947 and maximum probability 0.9791 as displayed in Table 7.10. The data is skewed to the left with 75% of the probabilities above 0.6879 and the remaining 25% below 0.6879, see Figure 7.9. This translates to only 3/4 of CUAS mitigation subsystems operating with reliability at or above 68.79%. The standard deviation is 0.1311 and considered high with the probabilities more spread out from the mean of 0.7845. The model indicates the mitigation subsystems would be up and operating at an average of 78.45% of the time. The data spread is also reflected in the large IQR probability of 0.2081. Any probability values lower than 0.3758 are considered outliers. There are outliers present below 0.3758 which is attributed to when the number of $failures$ for the mitigation subsystems occur near or at the max value for the course of their respective total mission time. Similar to the discussion in Section 7.3, this results in a low *MTBF* (represented in hours) which means the detection subsystem failures are occurring closer together in time. This highlights that all mitigation subsystems of a CUAS must demonstrate very low number of $failures$ or no number of $failures$ for the entire duration of the mission to maintain high probability of reliability. High probability of reliability in mitigation subsystems contributes to the overall effectiveness and reliability of the CUAS for operations against emerging UAS threats. Discounting the outliers, the reliability probability would range from 0.3758 to 0.9791 indicating uncertainty in the reliability of the mitigation subsystem. The differences

between Figure 7.9 and Figure 7.10 is attributed to the minimum and maximum values estimated for the number of $failures$ in the detection and mitigation subsystem. This highlights the need for the number $failures$ to be low as possible when considering a CUAS. Mitigation subsystems exhibiting a high number of $failures$ in future CUAS will negatively impact the CUAS's ability to provide kinetic or non-kinetic mitigation effects thus reducing the CUAS's effectiveness and reliability.

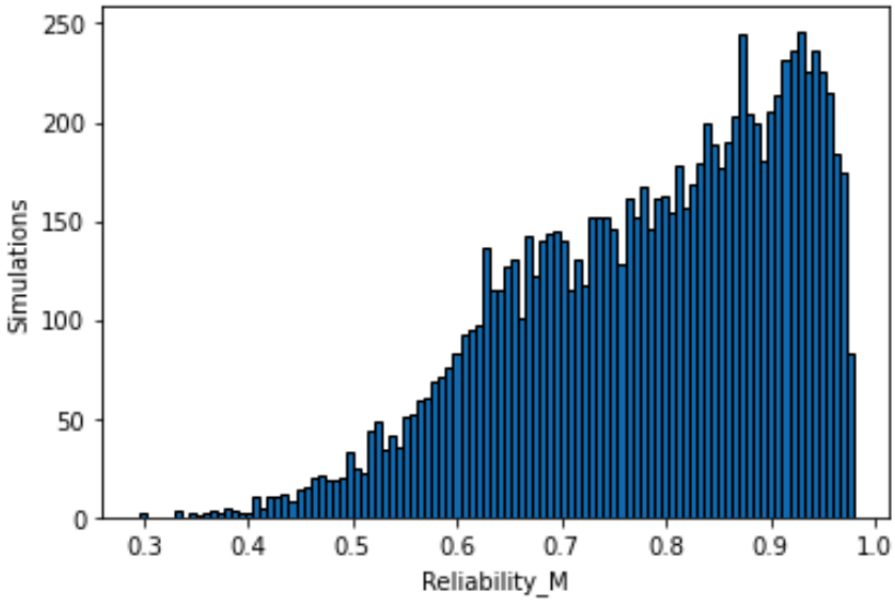


Figure 7.10. Mitigation Subsystem Reliability Histogram (Emerging).
Note: Scale 0-250 for number of simulations and 0.32-1.0 for reliability probability.

The summary statistics in Table 7.10 show the central tendency and spread of the reliability probabilities for the mitigation subsystem in the model. The reliability probabilities of the mitigation subsystem remained relatively the same which it attributed to no changes made for the minimum and maximum input values for number of $failures$ and t represented in hours in Table 7.2 for the mitigation subsystem.

Table 7.10. Mitigation Subsystem Reliability Stats (Emerging).

mean	0.7845
median	0.8056
standard error	0.0013
max	0.9791
min	0.2947
standard deviation	0.1311
range	0.6843
75th Quartile	0.8961
25th Quartile	0.6879
IQR Quartile	0.2081

With the reliability of the individual subsystems calculated for emerging UAS threats, they collectively formulate the overall reliability of the CUAS defined in the model by Equation (7.2). The reliability for CUAS varied between a minimum probability of 0.1936 and a maximum probability of 0.9657 shown in Table 7.11. The data is skewed to the left with 75% of the probabilities above 0.5491 and the remaining 25% below 0.5491, see Figure 7.11. This translates to only 3/4 of CUASs operating with a reliability at or above 54.91%. The standard deviation is 0.1496 and considered high with the probabilities more spread out from the mean of 0.6575. The model indicates the CUAS would be up and operating at an average of 65.75% of the time. The data spread is also reflected in the large IQR probability of 0.2276. Any probability values lower than 0.2077 are considered outliers. There are outliers present below the probability of 0.2077 which is attributed to when the reliability probabilities for either the detection or mitigation subsystems exhibit low probabilities because the number of $failures$ in the respective system(s) is near or at a high value for the course of the total mission time. This shows how the number of $failures$ each individual subsystem may experience affects the overall reliability of the CUAS. The model assumptions input values for $failures$, e, and t in Table 7.2 is kept the same to reflect current CUAS with no improvements added. This is to focus on how emerging threats affect the detection and mitigation subsystems with respect to probability of detection and probability of mitigation. Therefore, it is expected that system reliability for a CUAS when dealing with emerging UAS threats would remain relatively the same in the absence of improvements designed to reduce the occurrence of $failures$ in the CUAS.

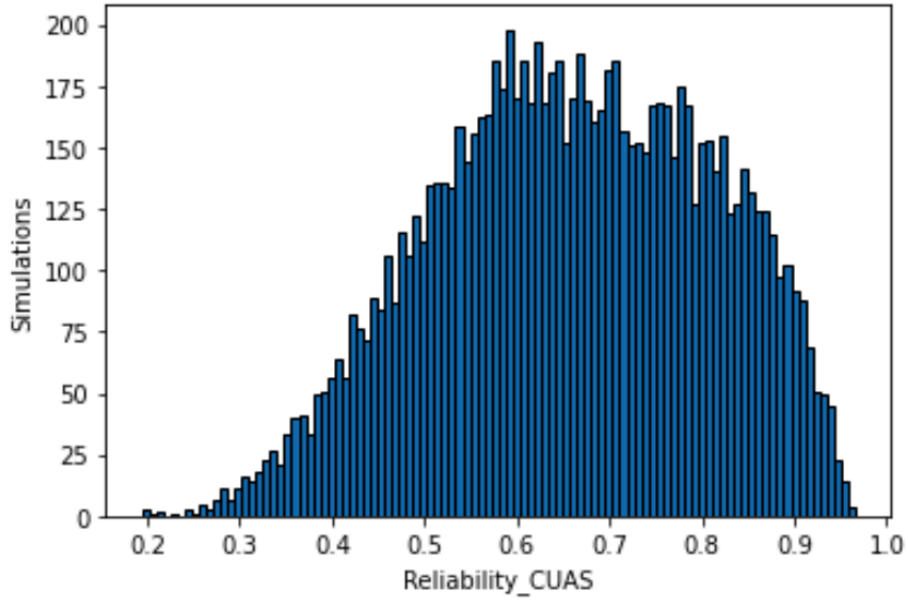


Figure 7.11. CUAS Reliability Histogram (Emerging).
Note: Scale 0-215 for number of simulations and 0.1-1.0 for reliability probability.

The summary statistics in Table 7.11 show the central tendency and spread of the reliability probabilities for the CUAS in the model. No significant changes observed when compared to Table 7.3.

Table 7.11. CUAS Reliability Summary Stats (Emerging).

mean	0.6575
median	0.6602
standard error	0.0015
max	0.9657
min	0.1936
standard deviation	0.1496
range	0.7712
75th Quartile	0.7767
25th Quartile	0.5491
IQR Quartile	0.2276

Equation (7.5) defined the hypothetical probability of detection for CUAS. The component

of $HP_{CUAS_{(Detect)}}$ in Equation (7.5) was reduced by 5% for each range which affected the overall probability of detection against emerging UAS threat. The probabilities of detection varied between the minimum value of 0.3613 and maximum value of 0.6713 as seen in Table 7.12. Figure 7.12 indicates the distribution is fairly normal with 75% of the probabilities above 0.4634 and the remaining 25% below 0.4634. This translates to only 3/4 of CUASs operating with a probability of detection at or above 46.34%. The standard deviation is 0.0603 and considered low with the probabilities less spread out from the mean of 0.5098. The data spread is also reflected in the small IQR probability of 0.0923. Any probability values greater than 0.6942 and lower than 0.3249 are considered outliers. There are no outliers present that could skew the data. The input values for Equation 7.5 were varied to demonstrate the effects the factors of range, number of targets, and terrain can have on a CUAS's probability of detection against emerging UAS threats. In the data produced by the simulations, the average hypothetical probability of detection was 0.5098. The model indicates that when the CUAS is operating, it has an average 50.98% change of detecting emerging UAS threats. The 50.98% average is a 21.02 percentage point reduction from what was observed in the hypothetical probability of detection for current UAS threats. It demonstrates that a reduction in detection capabilities is compounded by the effects range, number of targets, and terrain for emerging UAS threats. To address potential reductions in detection capabilities that could be present in emerging UAS threats, CUASs developments should consider detection subsystems with techniques identified in Table 6.1 that provide high probability of detection against emerging UAS threats operating with a high level automation (Table 6.4 Levels 3 and above) and certain types of collaboration (Table 6.5 Types 2, 3, and 4) leveraging command and control discussed in Section 4.4.

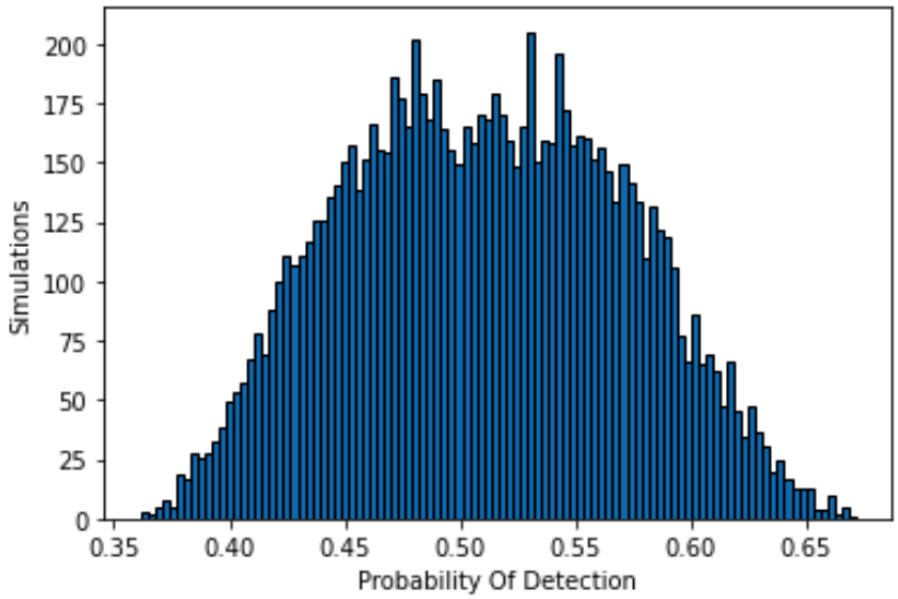


Figure 7.12. CUAS Probability of Detection Histogram (Emerging).
Note: Scale 0-225 for number of simulations and 0.32-0.70 for probability of detection.

The summary statistics in Table 7.12 show the central tendency and spread of the probability of detection for the CUAS with the changes observed from the reduction in capability.

Table 7.12. CUAS Probability of Detection Stats (Emerging).

mean	0.5098
median	0.5092
standard error	0.0006
max	0.6713
min	0.3613
standard deviation	0.0603
range	0.3101
75th Quartile	0.5557
25th Quartile	0.4634
IQR Quartile	0.0923

Equation (7.8) defined the hypothetical probability of mitigation for CUAS. The component of $HP_{CUAS_{(Mitigate)}}$ in Equation (7.8) was reduced by 5% for each range as well. The

reduction affected the overall probability of mitigation against emerging UAS threat. The $targets_{(weight_M)}$ component in Equation (7.9) was adjusted to show a 15-30% effect on the hypothetical probability of mitigation from the number of simultaneous UAS targets. The probabilities of mitigation varied between the minimum value of 0.3186 and maximum value of 0.6281 as seen in Table 7.13. Figure 7.13 indicates the distribution is fairly normal with 75% of the probabilities above 0.4207 and the remaining 25% below 0.4207. This translates to only 3/4 of CUASs operating with a probability of mitigation at or above 42.07%. The standard deviation is 0.0557 and considered low with the probabilities are less spread out from the mean of 0.4622. The data spread is also reflected in the small IQR probability of 0.0799. Any probability values greater than 0.6209 and lower 0.3009 are considered outliers. There are outliers present above 0.6209. The input values for Equation 7.8 were varied to demonstrate the effects the factors of range, number of targets, and terrain can have on a CUAS's probability of mitigation against emerging UAS threats. Additionally, the factors of range, number of targets, and terrain weighed differently than in the detection subsystems to simulate the difference that could be present in detection and mitigation subsystems for emerging UAS threats just as it was done for current UAS threats. In the data produced by the simulations, the average hypothetical probability of mitigation was 0.4622. The model indicates that when the CUAS is operating, it has an average 46.22% chance of mitigating emerging UAS threats. The 46.22% average is a 18.83 percentage point reduction from what was observed in the hypothetical probability of mitigation for current UAS threats. As seen with the detection subsystems, it demonstrates that a reduction in mitigation capabilities is compounded by the effects range, number of targets, and terrain for emerging UAS threats. To address potential reductions in mitigation capabilities CUASs development should consider mitigation subsystems with techniques identified in Table 6.2 that provide high probability of mitigation against emerging UAS threats operating with a high level automation, collaboration, and advance command and control.

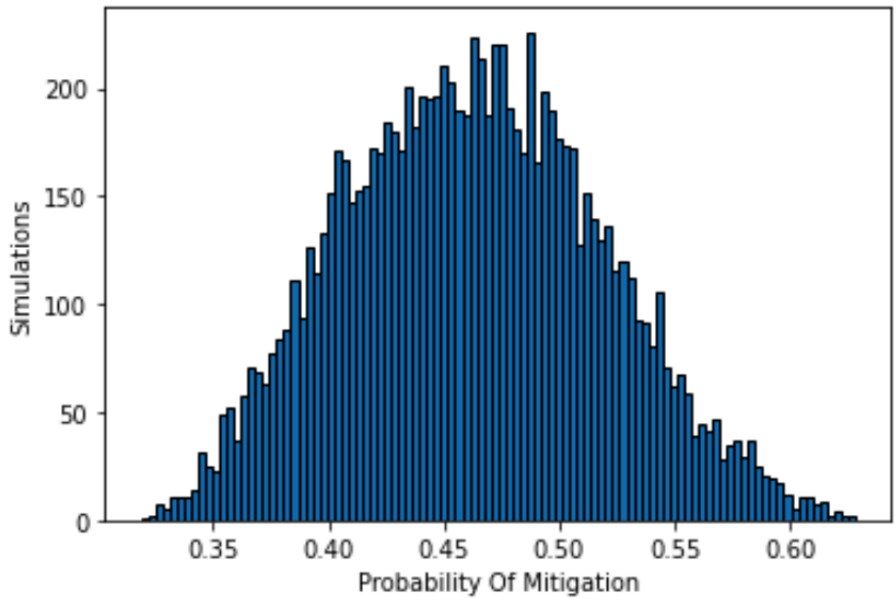


Figure 7.13. CUAS Probability of Mitigation Histogram (Emerging).
Note: Scale 0-225 for number of simulations and 0.30-0.70 for probability of mitigation.

The summary statistics in Table 7.13 show the central tendency and spread of the probability of mitigation for the CUAS in the model with the changes observed from the reduction in capability.

Table 7.13. CUAS Probability of Mitigation Summary Stats (Emerging).

mean	0.4622
median	0.4618
standard error	0.0006
max	0.6281
min	0.3186
standard deviation	0.0557
range	0.3095
75th Quartile	0.5009
25th Quartile	0.4207
IQR Quartile	0.0799

With all components of Equation (7.1) calculated for emerging UAS threats, the effec-

tiveness of CUAS for the simulations resulted in an approximately normal distribution as displayed in Figure 7.14. The effectiveness probabilities varied between the minimum value of 0.0341 and maximum value of 0.3296 as seen in Table 7.14. The standard deviation is 0.0446 and considered low with the probabilities less spread out from the mean of 0.1549. The data spread is also reflected in the small IQR probability of 0.0624. Any probability values greater than 0.2782 and lower 0.0286 are considered outliers. There are outliers present above 0.2782. The model produced an average effectiveness against emerging UAS threats of 15.49%. The highest observed effectiveness was 32.96% but could be viewed as a rare occurrence. Only 25% of the calculated effectiveness occurred above 0.1846 which indicates a majority of calculated effectiveness were at or lower than 18.46%. This demonstrates that when the probabilities for reliability, detection and mitigation are not at optimal levels, they directly affect a CUAS's overall effectiveness against emerging UAS threats.

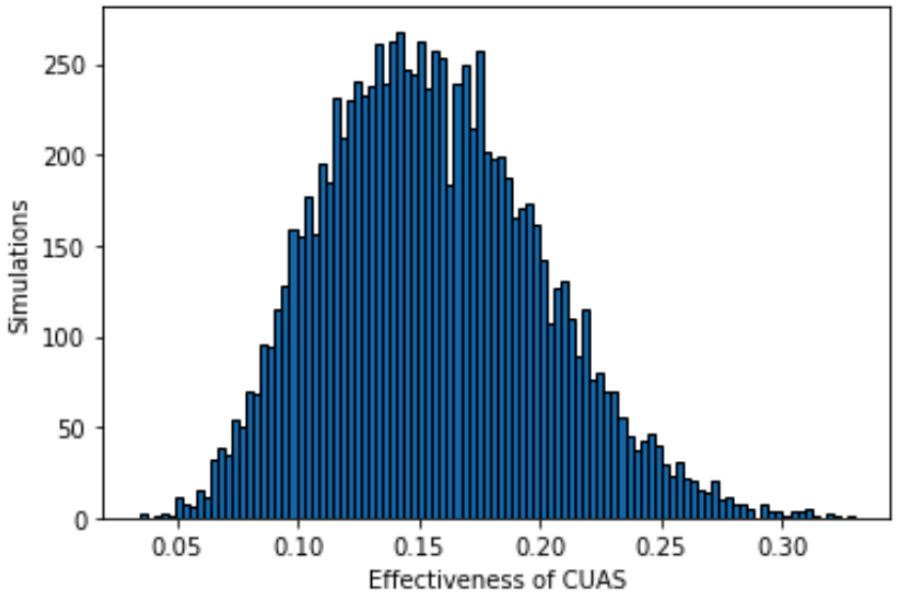


Figure 7.14. CUAS Effectiveness Histogram (Emerging).
Note: Scale 0-300 for number of simulations and 0-0.65 for effectiveness probability

Table 7.14 show the central tendency and spread of the effectiveness CUAS as defined by the model with the changes for emerging UAS threats.

Table 7.14. CUAS Effectiveness Summary Stats (Emerging).

mean	0.1549
median	0.1519
standard error	0.0004
max	0.3296
min	0.0341
standard deviation	0.0446
range	0.2955
75th Quartile	0.1846
25th Quartile	0.1222
IQR Quartile	0.0624

The model indicates that CUAS reliability, probability of detection, probability of mitigation, range, targets, and terrain all are significant factors in calculating the effectiveness of a CUAS. Table 7.15 provides a side-by-side comparison of the differences observed in the simulations from the significant factors. With a conservative 5% reduction of ($HP_{CUAS_{(Detect)}}$ and $HP_{CUAS_{(Mitigate)}}$), the model demonstrated how probability of detection and probability of mitigation would be affected which subsequently reduced the effectiveness of the CUAS against emerging UAS threats. Future interoperability should take into account the factors identified in the model to increase effectiveness, address shortfalls, and balance the trade-off between effectiveness and interoperability. Interoperability should not come at the cost of effectiveness against emerging UAS threats.

Table 7.15. Comparison of Model Results based on a 5% estimated reduction and $targetsFactor$ adjustments in the hypothetical probability of detection and hypothetical probability of mitigation.

	CUAS vs. Current UAS threats	**CUAS vs. Emerging UAS threats**
Reliability ($R_{(CUAS)}$)	65.99%	65.75%
Probability of Detection ($Pof D_{(CUAS)}$)	72.00%	50.98%
Probability of Mitigation ($Pof M_{(CUAS)}$)	65.05%	46.22%
***Effectiveness* ($E_{(CUAS)}$)**	30.90%	15.49%

The rationale for a 5% reduction and $targetsFactor$ adjustments for detection and mitigation capabilities was to be conservative and demonstrate that even with a small degradation in capabilities, effectiveness would be reduced against emerging UAS threats.

It is expected that emerging UAS threats effects on detection and mitigation probabilities will be greater than 5% which would result in even lower effectiveness percentages. We assess current CUASs are not adequately effective and future CUAS will be inherently inadequate if improvements are not made to increase effectiveness and implement interoperability.

7.5 Summary

This chapter provides a foundational level of research to support the arguments for USN and USMC CUAS effectiveness against current and emergent UAS threats in a generic operating environment, as identified in Chapters 3, 4 and 5. The values used to support our calculations and generic models in Sections 7.3 and 7.4 are intentionally hypothetical in nature to obfuscate the classified values associated with the currently employed USN and USMC CUASs. Further, these values should be tailored to the reader's specific CUAS to support a real-world application of CUAS effectiveness assessment in a classified environment. ,ability

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 8:
CUAS Legal Limitations in Each Area of Responsibility

This chapter discusses the legal constraints associated with the use of CUAS capabilities in each AOR. We define the existing legal restraints associated with RF capabilities in continent of the united states (CONUS) and OCONUS, followed by the lack of U.S. or internationally recognized policies to combat adversarial UASs with emergent CUAS capabilities. We further demonstrate the lack of USN and USMC doctrine associated with monitoring the effectiveness and suitability of CUAS employment in an AOR. We lastly provide recommendations to support the monitoring, predictive analysis, and assessment of CUAS capabilities with existing spectrum analysis tools.

8.1 Counter Unmanned Aerial Systems Employment Framework

Currently, there exists no international standard or regulation governing the acquisition and operational employment of both UAS and CUAS equities and their associated or underlying capabilities. However, as product availability proliferates throughout the commercial and contractual environments, the ability to procure acUAS and CUAS COTS and aftermarket capabilities becomes increasingly available with modifications and variances. This challenge is exacerbated by the exponential growth of the technologically inclines UAS industry, and its reactive CUAS counterpart.

As delineated in Chapter 3, UAS and CUAS capabilities, TTPs, and modifications are subject to the technological feasibility of the host nation and its subsidiary civil infrastructure. Not only is the ability to regulate UAS use in a contested and congested operational environment dependent upon the subjective rules and authorities of the nation they are operated in, the ability to adequately leverage a CUAS capability and properly exercise the elements of a proposed CUAS kill chain is also heavily reliant upon the legal infrastructure of the associated AOR and host nation. Furthermore, the inherent legal restraints of the hosting government are compounded by the U.S.'s armed forces agreements, internation-

ally recognized treaties, and international recognized standards for a region of interest. The United Nations Convention on the Law of the Sea supports the framework associated with territorial land ascribed to a country from their geographic land mass to the open oceans [168]. Country bilateral agreements address the negotiations entered in between two or more countries addressing the level of efforts for support, basing, staging of forces, and use of force in host nations [169]. These standards are also intertwined with the current rules of engagement associated with the regions' previous, current, and projected levels of hostility and endangerment towards civilians and military affiliated personnel. To understand these aforementioned elements is to better understand what means of CUAS is best leveraged to protect against UAS threats to USN and USMC installations and forward deployed elements. This chapter therefore addresses legal limitations according to the considerations in each AOR.

8.2 Overview Of CUAS Legal Implications In The Continent Of The United States

Within the CONUS region, UAS and CUAS capabilities are constrained to the rules and regulations set in place by state and federal agencies designed to protect civilian and military infrastructure. The material in Section 8.2 covers the application laws as they pertain to local U.S. laws and associated law enforcement. Per the 4th Amendment and Federal Communications Commissions, electronic surveillance and the use of electronic techniques within the U.S. that could result in unintentional EMI or jamming is prohibited for recreational use by official government personnel. Further, the employment of exercising of capabilities that could unintentionally cause EMI or jamming in the EMI may only be used by federal and state agencies and affiliated personnel after the attainment of the appropriate legal considerations [170], [171].

8.2.1 Foreign Intelligence Surveillance Act

Under the Foreign Intelligence Surveillance Act (FISA), electronic surveillance is the non-consensual gathering and attainment of electronic or wire communications from an original source by means of surveillance capabilities and technologies, where that source has the entitlement to privacy [172]. "The contents of a communication consists of any information concerning the identity of the parties, or the existence, substance, purport, or meaning of

the communication" [172]. Examples of electronic surveillance in this regard include the use of sensors and radio frequency to detect signals of interest emanating from a UAS. The first step within the CUAS kill chain is to detect active UASs within a proximity of interest pertaining to the CUAS capability and asset or assets to be protected. Detection implies the threat UAS is within the range of the CUAS sensing capabilities, and therefore within range to pose a discernible threat to the underling military infrastructure. The ability to detect can encompass one or many of the following as outlined in Table 6.1: the use of active and passive radar, radio frequency libraries, electro optical sensing, infrared sensing, and acoustic sensing.

8.2.2 Wiretap Act

In the U.S., the use of CUAS detection means such as radar to intercept electronic communications, including telemetric data, spatial and temporal information, and associated source, destination, and operator details is considered a direct violation of the Wiretap Act [173]. Often referred to as Title I of the Electronic Communication Privacy Act (ECPA) of 1986, the Wiretap Act prohibits the intentional or attempted interception and procurement of any other person and their associated equities via wire, verbal, or electronic means [173]. However, Title I "provides exceptions for operators and service providers for uses in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service and for persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the FISA of 1978" [173]. As written, section 101 of the FISA of 1978 empowers Federal, State, and other government servants the authority to exercise the use of capabilities that allow the interception of UAS communication necessary for accomplishing the detection phase of the CUAS kill chain, only after the requisite approvals.

8.2.3 Stored Communications Act

The second and third steps in the CUAS kill chain are to locate/track and classify/identify. To locate and track require the CUAS capability and operator to discern the activity of a UAS in any geographic area of interest. To classify and identify require the CUAS capability and operator to discern the UAS from the ambiguity of the operational environment and other UASs. These steps are accomplished through the successful implementation of the detection

phase, followed by the storage of the collected information for processing, discernment, and subsequent cataloging of the information for future and more expedited use. The Stored Communications Act, also referred to as Title II of the ECPA of 1986, protects against the privacy of the data and records stored by and about the commercial service providers, to include their name, serial number, model, and internet protocol address [173]. Furthermore, the Fourth Amendment of the U.S. constitution protects the rights of U.S. citizens and their private data from unreasonable searches and seizures without prior coordination and suspected probable cause. However, this is waivable under the U.S. FREEDOM Act, also referred to as the 'Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring' Act [174]. The FREEDOM Act superseded the Patriot Act in 2015, and modifies aspects of laws governing the requisition and collection of electronic communication, including the previously mentioned ECPA and FISA. The FREEDOM Act maintains the broadening of the authority for Federal and state law enforcement entities to combat adversarial use of nefarious activities through electronic surveillance on suspected U.S. persons that are affiliated with terrorist or violent extremist organizations.

8.2.4 Computer Fraud And Abuse Act

The use of cyberattack, spoofing, or directed energy are all active capabilities for a CUAS to usurp, degrade, or destroy an adversarial UAS upon detection, location, tracking, and classification. However, these means are all identified as forms of action that can induce considerable harm and erroneous consequences in the civilian and military domains and are therefore heavily guarded with legal action and ramification. The use of cyberattack to exploit and spoof a C2 RF link between the UAS and its operator could be potentially prosecuted under the Computer Fraud and Abuse Act [55]. The Computer Fraud and Abuse Act is intended to address hacking and serves as an amendment to the originally enacted Federal Computer Law. This act prohibits intentionally accessing the computer of a U.S. citizen without the proper and requisite legal oversight and authorization. However, this too is waivable with the FREEDOM Act, allowing Federal and state agencies to prosecute suspected malign individuals while in the pursuit of protecting U.S. assets, persons, and equities. Moreover, if a UAS link between the UAS and its operators is intercepted and spoofed, and that spoofing results in the commandeering of the original link, then the spoofing entity must possess a remote certificate to pilot the vehicle in accordance with

the FAA. This certification ensures the protection of all civilian and military assets either airborne or on the ground from uncertain circumstances that could arise from a UAS that has been commandeered by Federal and state authorities for the purposes of protection.

8.2.5 Directed Energy Weapon Review And Approval Process

The use of electronic attack means through emissions quantifies as directed energy, and therefore must undergo rigorous oversight and approval to meet deconfliction for civilian and military aerial operations. This process is formalized as the DEWRAP, and oversight is exercised in the Office Under the Secretary of Defense (OUSD) for installation and authority to operate. The DEWRAP instantiates the CUAS capability's range, power output, intended use, and the service component intending to operate it. It further defines the required means to ensure deconfliction with any surrounding infrastructure impacting safety of flight and transportation. The DEWRAP is contained in DOD Instruction 5000.69, and must be consistent with the DOD Directive 5134.01 for advanced research project acquisition [53]. The fifth step of the CUAS kill chain encompasses mitigation measures to either kinetically or non-kinetically neutralize the adversarial UAS platform as a threat and is subject to all the previously mentioned constraints unless otherwise deconflicted and coordinated with the federal government and law enforcement.

8.3 Overview Of CUAS Legal Implications Outside The Continent of the United States

OCONUS, the use of military capabilities and subsequent force is not as restrained as in the CONUS. Further, the use of military application, as will be presented in Sections 8.3 and 8.4 pertains to military application only. The legal discussion OCONUS for CUAS employment is primarily attributed to the UAS targets of interest, their history of proprietary employment, and their subsidiary armaments and components leveraged in varying AORss. Furthermore, UASs and their associated operators are often not considered U.S. citizens or property of the U.S. when operating and prosecuting targets OCONUS. Therefore, they are not protected by the U.S. 4th Amendment, the ECPA, or any supporting or inherent legally recognized constrictions [170]. Furthermore, the U.S. FREEDOM Act, supports the deterrent and punishment of violent extremist organizations' acts in and outside of the U.S. [174]. This act and subsequent legislation supports federal law enforcement entities in

their abilities to identify, deter, degrade, disrupt, dissuade, and prevent terrorist activities and facilitation by also encouraging U.S. and foreign law enforcement entities and financial institutions to coordinate and share information where possible. As expected, this act allows agencies and organizations such as the Drug Enforcement Agency (DEA), CIA, and National Security Agency (NSA) to coordinate and operate under mutual jurisdiction with foreign U.S. partnering countries and their associated agencies for the successful identification and prosecution of nefarious activities. Some additional purposes empowered by the legacy Patriot Act of 2001 and its successor, the FREEDOM Act, are as follows:

- To strengthen U.S. measures to prevent, detect and prosecute international money laundering and financing of terrorism;
- To subject to special scrutiny foreign jurisdictions, foreign financial institutions, and classes of international transactions or types of accounts that are susceptible to criminal abuse;
- To require all appropriate elements of the financial services industry to report potential money laundering;
- To strengthen measures to prevent use of the U.S. financial system for personal gain by corrupt foreign officials and facilitate repatriation of stolen assets to the citizens of countries to whom such assets belong. [175]

The FREEDOM Act encourages the interoperability of efforts, assets, and personnel between and within the DOD [174]. The FREEDOM Act further empowers the DOD with the requisite abilities and legal framework to track information pertaining to the purchase of hardware and software that could be used in nefarious manners [174]. This tracking, similar to the UAS DRIP requirement, can be used to support CUAS capabilities by cataloguing and incorporating findings into the associated CUAS libraries to better categorize UASs. This categorization can improve the ability to detect and classify threat UASs.

8.3.1 Rules of Engagement

In addition to the privileges afforded to the U.S. Federal government and its affiliated entities regarding the use of cyberattack and directed energy means to deter adversarial actions in the operational environment, the DOD is also governed by rules of engagement (ROE)

when operating OCONUS [176]. Per Joint Publication 1-02 'Dictionary of Military and Associated Terms', ROE are the authoritative rules and regulations issued and enforced by military authorities that demonstrate when and how U.S. forces can and will initiate or continue combatant operations with encountered adversarial forces. ROE provides commanders with the requisite tools to regulate their employment of force with the preponderance of equities under their command [176]. The inherent abilities to exercise these DOD equities are provided by subsidiary treaties, foreign policies, international norms, and rules of law. A Judge Advocate (JA) assists in this endeavor as a legal advisor to the commander to support appropriate decision making for the use of force and escalation where required. However, commanders bear ultimate responsibility for the use of force.

ROE are set in place by the Theater and/or Geographic Combatant Commander after successful coordination, deconfliction, and integration with the host nations associated within that AOR. Further, to ensure ROE are reflective of the host nations' civil and governmental authorities, U.S. embassies and consulates serve as liaisons between U.S. DOD and host nation officials. Specifically, Chiefs of Mission, Chiefs of Station, Senior Defense Officials, and Defense Attaches serve in this capacity as liaison between both parties. This is done to ensure ROE remains versatile to the environment it is applied in, understandable to the operators regardless of operational background and pedigree, and tactically attainable to ensure both operators and JAs are uniformly aware and capable of executing operational requirements and authorities within the scope of legal and ethical ramifications given the operational circumstances and current events. ROE are therein intended to fulfil the purposes of providing guidance from the U.S. President, Secretary of Defense, and subordinate Combatant Commanders to military deployed elements pertaining to the use of force. They further serve as a decision point for when an interaction between opposing forces is in a transitory position from peacetime to wartime and support associated planning.

8.3.1.1 Rules Of Engagement And CUAS

Holistically, ROE provide a framework politically in support of national security, militarily in support of the aforementioned operational planning, and legally in support of U.S. domestic and international law. Politically, ROE ensures that U.S. national strategic policies and objectives are reflective of our actions and ideals both domestically and abroad. Additionally,

it protects the image and assertion of the U.S. as a global participant for fair and equal treatment for any country's constituents. By doing so, ROE may restrict the use of certain capabilities within a host nation or AOR writ large, such as the employment of directed energy, electronic attack, or cyberattack capabilities.

The C2 specifications of the varying UAS operations indicated in Chapter 4, associated with the disparity of UAS methods of employment indicated in Chapter 5 necessitate the need for clear and concise ROE dictating the methods of CUAS to be employed to protect USN and USMC equities domestically and abroad. ROE can set, establish, or reinforce a precedent for the use of specific CUAS capabilities in an AOR. These capabilities, based on established norms, EM deconfliction, and host nation allowance could range from the use of kinetic projectiles to the employment of directed energy. ROE therein would provide the legal framework necessary to conduct succinct operations for CUAS.

8.3.2 Supplemental Rules For The Use Of Force

ROE and the associated details for the supplemental rules for the use of force (SRUF) delineate the appropriate legalities associated with military operational capabilities within an AOR and host nation [176]. Similar to ROE, SRUF apply to both civil support missions and homeland defense operations for all U.S. owned and leased territories, both ashore and abroad. Furthermore, SRUF provides the basic statements of posture and response for self-defense associated with peacetime and wartime operations in the associated areas of operations. Both ROE and RUF are set by the SecDef, and delegated to theater commanders for oversight and executions.

8.3.2.1 Supplemental Rules For The Use of Force And CUAS

SRUF serves as the associated right to use specific force as a deterrent, self-defense, and to initiate offensive [176]. SRUF arms the tactician with the legal boundaries they are to operate in for combat and non-combat operations. It further provides the appropriate tripwire steps associated with the allowance for the escalation in force during combat and non-combat operations and AORs. SRUF can therefore assist the CUAS operator with the proactive knowledge of when specific CUAS capabilities may be leveraged against a UAS threat to meet mission requirements.

8.4 CUAS Legal Implications in each Geographic Area of Responsibility

Theater commanders in conjunction with Chiefs of Mission, Chiefs of Stations, Defense Attachés, and country teams coordinate with Host Nations to ensure the adequate rule of law and military operations are executed in a manner consistent with both U.S. and host nation's policies and procedures. From this cooperation, a multinational force (MNF) ROE or a combined ROE (CROE) is either produced and executed, or the U.S. remains consistent with the existing ROE for the region [176].

Multinational ROE becomes relevant when conducting operations aboard in host nations out of U.S. forward operating bases and territories, or when the U.S. is conducting operations with Coalition partners as part of a greater MNF. MNF ROE only takes precedence however when authorized and stated by the SecDef; otherwise, U.S. ROE stands. However, the U.S. is always entitled to the inherent right of unit self-defense should any hostile intent or hostile act befall our territories or equities. Furthermore, CUAS OPORDs delegate the approval from the SecDef to theater commanders to leverage and utilize non-kinetic CUAS capabilities to deter and degrade Group 1 through 3 UASs to protect U.S. personnel and facilities. Within the CONUS, it leverages deconfliction with the FAA via OPNAV for the USN and USMC. OPNAV deconfliction provides the necessary protections against interference with critical and key civilian infrastructure.

Additionally, classified supplemental rules of engagement (SROE) further empower Theater Commanders to engage adversarial UASs in CONUS and OCONUS for the protection of U.S. equities. Such empowerment allows theater and subordinate unit commanders to leverage CUAS against Groups 1 through 3 UASs as necessary to prevent the potential harm to U.S. personnel or infrastructure, without the potential of political blowback following engagement.

With the aforementioned authorities and privileges, USN and USMC commanders are emboldened to leverage existing CUAS technologies against UASs that are non-responsive to queries, or determined to demonstrate hostile intent or action regardless of the area's designation as being peaceful, an area of armed conflict, or wartime. However, these same commanders are still confronted with the truths of our current circumstances. Depending on the AOR and corresponding host nation, certain neutralization means of existing U.S. CUAS

capabilities are not permitted to be used for fear or potential of unforeseen consequences to the surrounding civilian infrastructure.

8.4.1 Africa Command

Within AFRICOM, the U.S. maintains only one fixed presence in the country of Djibouti. Djibouti houses Naval Expeditionary Base Camp Lemonnier, established by formal agreement in 2003, located next to the Djibouti-Ambouli International Airport [177]. Camp Lemonnier houses the U.S. military's Combined Joint Task Force – Horn of Africa (CJTF-HOA), which serves as a means of deterring, degrading, and neutralizing VEO threats within the AOR, emboldening supporting countries' civilian and military infrastructures, and building partner relations through combined exercises. Further, Djibouti's location provides strategic access and influence to the Horn of Africa and Bab el Mandeb, enabling U.S. led security, regional stability, and humanitarian efforts throughout the AFRICOM and CENTCOM AORs.

8.4.1.1 Africa Command Weapons Employment in Host Nations

The Djiboutian government is supportive of the U.S.'s presence and interests, as demonstrated in the bilateral agreement between the two countries allowing for the U.S. to access Djibouti's port facilities and airport in support of U.S. civil-military operations [178]. Djibouti also houses the first overseas military base operated by China and its People's Liberation Army Navy (PLAN) [178]. In light of this, the precedence of employing electronic attack weaponry within the AFRICOM AOR and specifically in Djibouti was set by the Chinese military when the first Notice to Airmen was disseminated between April 14th 2018 to June 14th 2018 in preparation for China's directed energy weapon testing in the Djiboutian port [178].

As the presence of affluent countries increases within Djibouti, so does Djibouti's socioeconomic infrastructure and the potential for adverse collateral effects due to cyber- and electronic attack. Although Djibouti is still considered a developing country, there exist broadening civil-military infrastructure that must be considered when using active means of CUAS capabilities within the host nation. Urban sprawl and associated renovation initiatives are improving the communication and transportation infrastructures. Transportation upgrades include new railways, maritime ports, airports, and power plants [179]. Therefore,

use of active CUAS means encompassing electronic- or cyberattacks must consider adverse ramifications against the expanding Djiboutian infrastructure, as well as the potential for meeting criteria for war against adversaries that are operating in the country as well.

8.4.2 Central Command

Within CENTCOM, the U.S. maintains and operates several bases of strategic location and position to support its initiatives for freedom of navigation, continuity of seas, safety of commerce, suppression of malignant Iranian influence as well as that of its surrogates/proxies, and building relations to promote regional stability. Figure 8.1 depicts the plethora of operating locations leveraged by the U.S. within the CENTCOM AOR [180].



Figure 8.1. U.S. Naval Facilities in CENTCOM AOR. Adapted from: [180].

The U.S. houses the service elements to CENTCOM in Bahrain, Kuwait, Qatar, and the United Arab Emirates. Bahrain is host to U.S. Naval Forces Central (NAVCENT) and elements of the U.S. Marine Forces Central (MARCENT), referred to as the 5th MEB and it forward deployed Command Task Force (CTF) 51/5. Kuwait is host to elements of U.S.

Army Forces Central (ARCENT) and serves as a Joint Mail Terminal for large operations and supporting equipment entering the CENTCOM AOR. Both Qatar and the United Arab Emirates host elements of the U.S. acAFCENT between Al Udeid Air Base in Qatar and Al Dhafra Air Base in the United Arab Emirates. The U.S. maintains close diplomatic and operational ties with the aforementioned countries as part of the GCC, which serves as a socioeconomic and sociopolitical union of Arab states bordering the Arabian Gulf. The U.S.'s bilateral relation to the countries within the GCC, and it diplomatic ties to the GCC reiterate and corroborate its strategic focuses of maritime security, regional defense, non-proliferation, free trade, law enforcement against piracy and smuggling operations, energy policies, and cultural exchanges/partnerships [181].

8.4.2.1 Central Command Weapons Employment In Host Nations

There exist increased potential for unintended consequences on third party territories when exercising active RF capabilities in CENTCOM. Although the U.S. successfully collaborated with the previously mentioned countries as target audiences to the use and employment of directed energy aboard the USS PONCE between 2014 to 2017, the amphibious dock landing ship only performed directed energy engagements while operating in internationally recognized waters, 12 nautical miles outside the territory of any neighboring countries [50]. Further, the USS PONCE acknowledged operation of its LaWS only in widely publicized and heavily planned exercises, and never against actual UAS threats it encountered during choke point transits observed in Bab el Mandeb and Strait of Hormuz. Therefore, the use of directed energy in the CENTCOM theater, inside the territories of host nations has been met with uncertainty.

The use of UASs by anything other than governmental features and entities is strictly forbidden in GCC countries [182]. As such, any use of associated CUAS that leveraged active means of neutralizing a hostile UAS was considered exaggerated and necessitated the requisite program indoctrination and familiarization with host nation leadership and law enforcement, including foreign military sales. From a domestic perspective, the employment of the USS PONCE's LaWS commenced what is referred to as the DEWRAP, which is a review and approval process for a theater to operate high energy weaponry within an AOR [53]. This process is approved by the office of the SecDef, and is intended to oversee and ensure host nation civil-military equities are protected and the electronic attack

capability possessing high energy capabilities is operated in manner that prevents fratricide to host nation infrastructure. The DEWRAP further ensures host nation entities' equities are considered in the review and approval process by the associated country teams.

The legal implications and regulations required to leverage active means associated with our current and potentially future CUAS capabilities is further compounded by the complications associated with the Great Power Competition. As quoted by USCENTCOM Commander General McKenzie:

> The United States faces increasing competition in the region from Russia and China both vying for power and influence through a combination of diplomatic, military and economic means. The CENTCOM AOR is and always has been a crossroads of global interests and, historically, a prime arena for foreign powers to compete for influence for resources and for access. In 2020, Russia and China exploited an ongoing regional crisis; financial infrastructure needs; perception of declining U.S. engagement; and opportunities created by COVID-19 to advance their objectives across the Middle East and central and southern Asian nations to gain or strengthen footholds in the region. [183]

The increased presence of foreign actors and their associated doctrines and policies complicates the issue and ramifications for the misuse of electronic and cyberattack capabilities. This complication increases the likelihood of miscalculation and escalation of force against regional and foreign peers in the CENTCOM AOR and must be accounted for. To meet the growing cadre of CUAS capabilities fielded in AORs and future operational needs, there exists a necessity to have a means to conduct environmental monitoring with near real time atmospheric modeling to ensure the use of active CUAS capabilities do not interfere with the surrounding infrastructure if leveraged.

8.4.3 Europe Command

The EUCOM AOR houses major naval and marine installations and detachments in Spain, Italy, Greece, and Crete, as shown in Figure 8.2 [184].

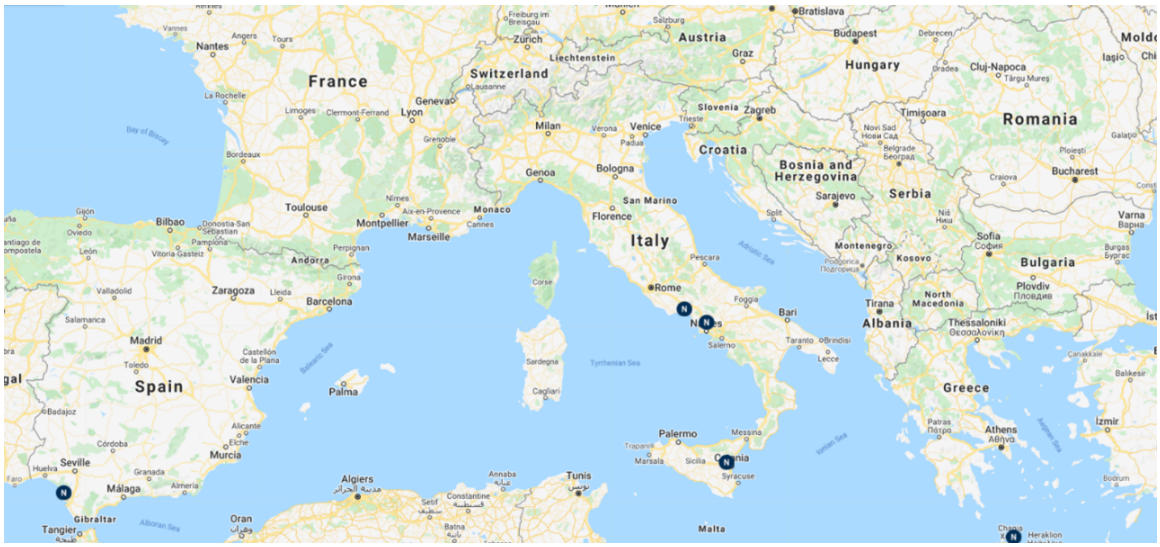


Figure 8.2. U.S. Naval Facilities in EUCOM AOR. Source: [184].

It further houses the headquarters for EUCOM, AFRICOM, and our NATO in Germany. The EUCOM AOR therein serves as an essential focal point of U.S. strategy and planning against our near peer, Russia. It further provides the requisite footprint to support our alliances and shared military resources with our European partners. The U.S.'s alliances with the countries of Spain, Greece, and Crete are dated back to the inception of the U.S. as an independent country.

8.4.3.1 Europe Command Weapons Employment In Hosts Nations

Besides our participation in NATO, security cooperation between the U.S. and the previously mentioned countries are maintained and overseen by the Mutual Defense Assistance Agreement and Agreement on Defense Cooperation [169]. This is exemplified with the U.S. strategic and operational relationship shared with Spain through its authorization of the U.S. to use designated and agreed upon facilities at existing Spanish military installations such as Naval Station Rota. In 2012 and 2015, Spain and the United States updated this agreement to allow for the housing and feeding of additional U.S. personnel and equities on Naval Station Rota and in Moron, Spain, which houses the SPMAGTF. Furthermore, Spain assisted in the previous defeat ISIS campaign in Iraq and Syria through the pledging of troops and support to coalition training [185]. Further coordination with the Mutual Defense Cooperation Agreement is delineated by the strategic location in the Eastern Mediterranean provided

by Greece and Crete, and their shared installations with the U.S. The Greek peninsula and associated islands serve as a strategic point of influence and basing for military forces operating in and out of Europe and northern Africa. The U.S. and Greek Mutual Defense Agreements allows for access and operations from Crete with the U.S.'s naval base and airfield located in Souda Bay [186].

These cooperative agreements and the mutually shared benefits from the foreign military sales (FMS) of real estate and equipment benefit the U.S. in its use of capabilities involving electronic attack and cyberattack capabilities on foreign soil and within host nation territories. The U.S. is not hindered in classification, reliability, and disclosure of CUAS weaponry in these counties, and is therefore able to cooperatively plan and deconflict the use of CUAS equipment and capabilities with host nation governments and law enforcements in a more transparent manner as compared to other AORs. However, there will always exist a threat to interference and safety of navigation with civilian infrastructures when introducing new capabilities with directed energy or offensive cyber traits. As such, sustained deconfliction and mapping of the environment must ensure between U.S. military and host nation leadership through the requisite country team affiliated personnel which shall always include the Defense Attaché Office, Attachés, Chiefs of Mission, and Chiefs of Station.

8.4.4 Pacific Command

Amidst the emergence of the Great Power Competition, the U.S. maintains a massive 'ready force' in the Asian Pacific theater in the countries of Singapore, Guam, South Korea, and Japan as shown in Figure8.3 [187].

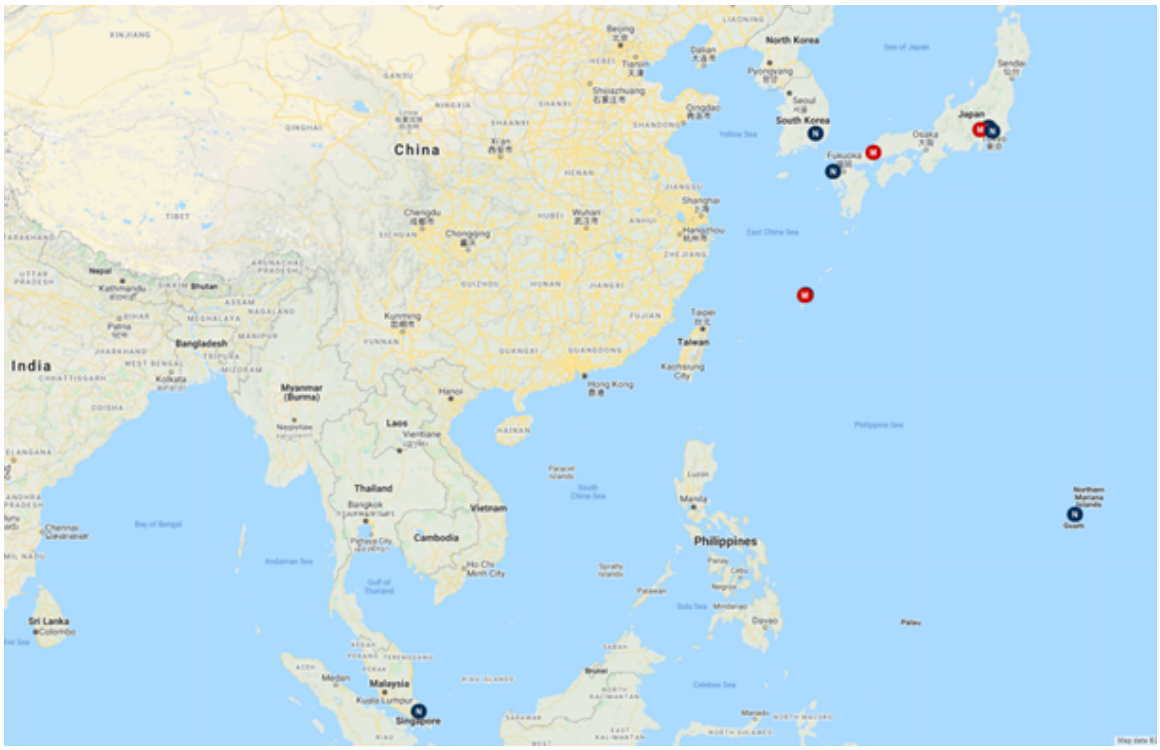


Figure 8.3. U.S. Naval Facilities in PACOM AOR. Source [187].

The presence and posture within the PACOM AOR maintains a 'fight tonight' mentality in support of its power projection, strategic deterrence, and national security policies and doctrine [137] [188]. The 'fight tonight' mentality is intended to directly address the necessity of meeting the requisite manning, equipment, and availability requirements to meet our near peers should the need for combat manifest. The vision for PACOM's readiness focuses on the Great Power Competition from a vantage point of understanding the adversary's capabilities, and therefore adjusting your own to meet the potential threat in the land, air, sea, space, and cyber domains.

8.4.4.1 Pacific Command Weapons Employment In Host Nations

The 'fight tonight' ideal is commensurate through the U.S.'s mutual defense guidelines and policies with the aforementioned countries, allowing for the sharing of resources and the basing of forward deployed Naval and Marine personnel through the region to promote domestic and regional security. Exemplary ties between the U.S. and the Asian AOR is

the alliance shared with Japan. The alliance between the U.S. and Japan in the PACOM AOR serves as the pinnacle of strategic location, influence, forward basing, and access to critical resources in the region [188]. The Alliance between the two is rooted in the shared interests and values in the region being the free flow of economic commerce in the maritime environment, support for human's rights and freedoms, and the expansion of civil liberties.

The U.S. and Japan also work together in support of regional agreements for framework encompassing the use of cyber and electronic emissions and subsequent communications. This is exemplified with the countries' cohesive approach to the information and communications technology supply chains for the use of 5G networks [189]. Such coordination supports the Supplemental ROEs for the AOR and host nation, authorizing the use of non-kinetic CUAS capabilities, to include cyber and electronic attack, inside of a host nation without the need to for deconfliction. This is delineated by the FDNF CSG and ARG operating in the PACOM AOR, who are home-ported from Japan. The CUAS policies associated with the U.S. Naval Forces Pacific Fleet and the 7th Fleet staff embarked in Yokosuka, Japan against Groups 1 through 3 UASs enable senior decision makers to take decisive actions to protect ships and shore bases against UASs that enter inside the designated vital areas pertaining to those equities.

However, such ROEs are in place for current CUAS technologies that have been deconflicted and routed through the applicable service chains of custody and command, such as OPNAV. This does not immediately satisfy the fielding of new, emerging technologies in the AOR and host nation. To meet this requirement, subsequent approval is currently required through the service administrative chain of command, which conducts the requisite deconfliction between the host nation and against U.S. standing domestic policies. Furthermore, there exists no standard to model the environment from a military situational perspective as it changes over time. Therefore a more transparent picture of what equities are at stake when cyber- and electronic attack capabilities are leveraged against a threat UAS would be beneficial.

8.4.5 North Command

The USN and USMC maintain a plethora of bases within the U.S., in CONUS for manning, training, and equipping its forward deployed forces and maintaining a ready force to meet

emerging requirements, as shown in Figure 8.4 [190].



Figure 8.4. U.S. Naval Facilities in NORTHCOM AOR. Source: [190].

As delineated in Figure 8.4, NORTHCOM's jurisdiction resides within CONUS. Therefore, there is overlap observed between local U.S. laws as well as associated SRUF in the military's application of force during military engagements on federal property. The Naval presence within the U.S. is dispersed across both the East Coast and West Coast of the U.S., the concentration of Fleet elements that necessitate a need for considering and using CUAS capabilities in support of share battle space reside amongst Florida, Georgia, Virginia, Connecticut, California, Washington, and Hawaii. These states maintain a direct and deliberate concentration maritime and ground traffic and capabilities that necessitate a need for elucidation by hobbyist, non-state actors, and state actors leveraging the previous groups as proxies and surrogates alike.

8.4.5.1 North Command Weapons Employment

Current military application is also subjected to the legal framework of FISA, ECPA, and the FREEDOM Act to identify and prosecute nefarious actors and actions. Unlike other countries OCONUS, there exist no potential or foreseeable declaration of armed conflict

in CONUS. Therefore, there exists no ROE or SROE to govern the use of electronic or cyber-attack capabilities associated with CUASs on U.S. sovereign soil. Due to this, the use of CUAS active and passive capabilities is governed by U.S. laws and regulations, with oversight by the Federal government. The U.S. has not been declared an area of armed conflict since the American Civil War. Furthermore, the persons and their associated UASs that would be prosecuted if operating in a dangerously ostentatious manner in the vicinity of armed forces' personnel and equities are more likely to be considered U.S. citizens, and therefore protected under the U.S. Constitution and its associated acts. As anticipated, the USN and USMC require authorities to leverage CUAS cyber and electronic attack capabilities in a manner to protect their personnel and equities while complying with state and federal regulations.

8.4.6 South Command

Of the several hundreds of bases maintained by the U.S. across the globe, approximately 70 of them are located in South America and the Caribbean to serve as an immediate response and presence against threats around and entering the U.S., as delineated by Figure 8.5 [191].

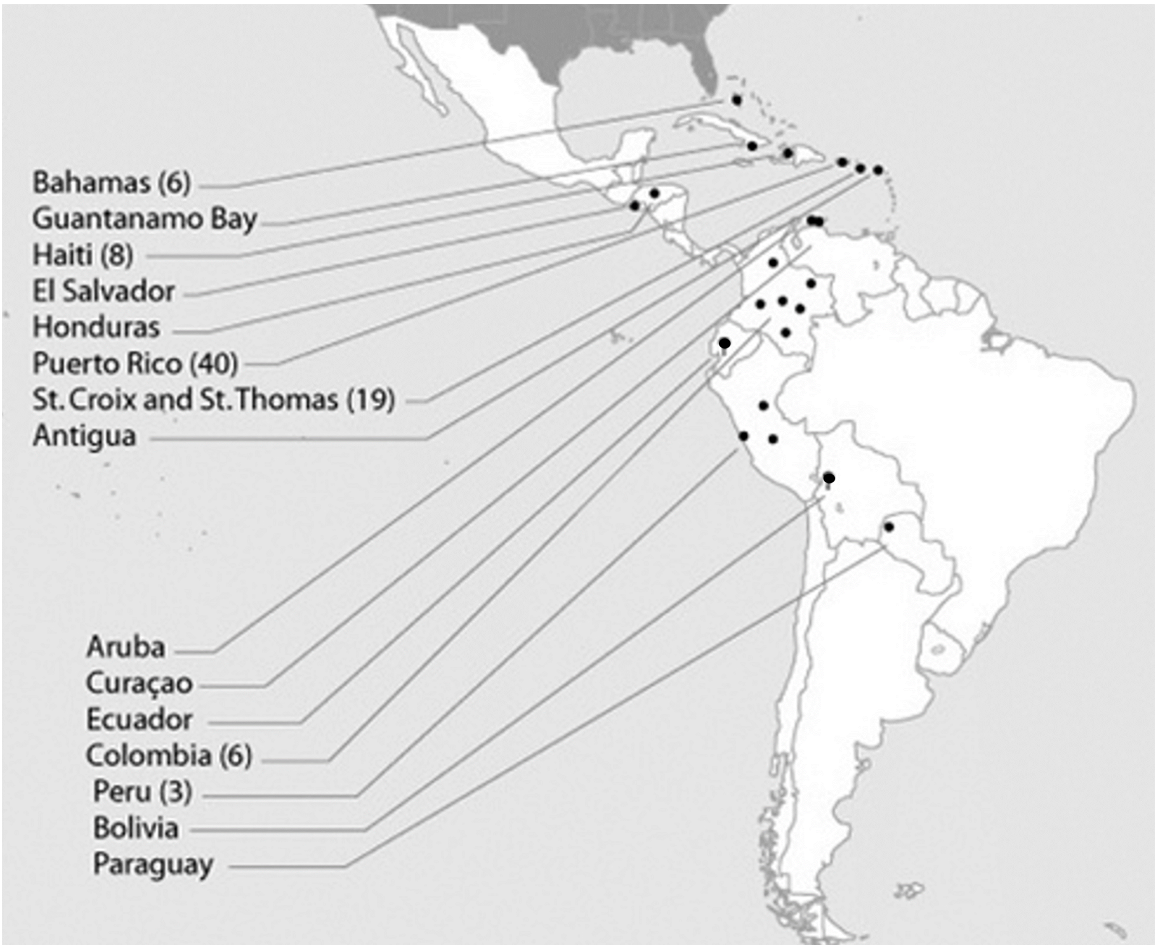


Figure 8.5. U.S. Military Facilities in SOUTHCOM AOR. Adapted from: [192].

The concentration of USN and USMC presence in South America and the Caribbean is amongst Panama, Puerto Rico, Colombia, Cuba, and Peru. These bases are under the operational purview of U.S. Southern Command, located outside of Miami, Florida. The focus of the threats in this AOR are intended to address weapons and narcotics smuggling and facilitation networks, regional and transnational criminal enterprises and networks, the encroaching presence of Iran, Russia, and China in Latin countries, humanitarian aid and disaster response, maintain freedom of navigation through the Panama Canal, and provide support to regional allies and partners. The primary countries that contribute to the aforementioned threats are Bolivia, Cuba, and Venezuela. Due to the relative closeness

of the threats posed by nefarious activities in the SOUTHCOM AOR, the United States is most easily affected by destabilizing actions undertaken in this AOR [193]. As such, these locations directly support the U.S.'s regional hegemonic endeavors and aspirations.

8.4.6.1 South Command Weapons Employment In Host Nations

Since the Spanish American War, Puerto Rico has been a U.S. territory and therefore subjected to similar laws and policies observed in the U.S. regarding the U.S. of electronic and cyberattack military capabilities to subvert UAS threats. Therefore, similar deconfliction between the USN and USMC service components and the government of Puerto Rico must ensue to use the currently available CUAS capabilities, especially due to the area's lack of designation as an area of armed conflict. Panama and the surrounding areas are, however, not U.S. territories although the U.S. temporarily controlled zones around the U.S.-built Panama Canal under former policies. Figure 8.6 shows the Panama Canal and the importance it provides to freedom of navigation to the Caribbean and SOUTHCOM AOR, connecting the Pacific Ocean to the Atlantic Ocean and dramatically improving transit time between AORs.

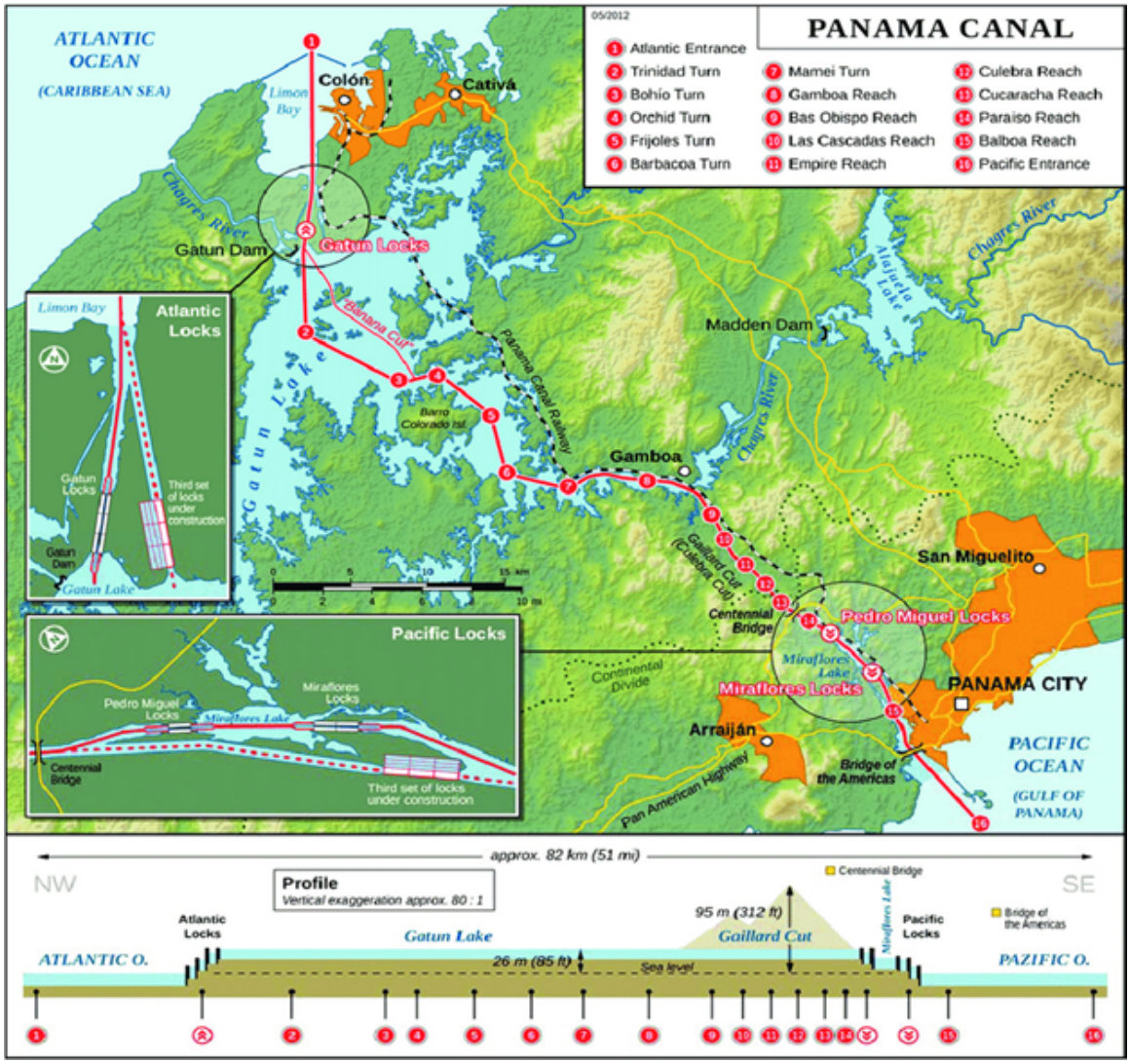


Figure 8.6. Panama Canal. Source: [194].

Panama, as anticipated, plays a strategic role with the U.S. and it's ability to assert dominance and positive influence in the AOR. Following the U.S.'s occupation and purchase of the territory surrounding the Panama Canal, it constructed the waterway as a means to support and enable freedom of navigation [195]. However, following the 1977 Torrijos-Carter Treaties between former U.S. President Jimmy Carter and former Panamanian leader Omar Torrijos Herrera, the U.S. relinquished its lease and subsequent perpetuity of occupation in the region back to the Panamanian government. As anticipated, the use of CUAS equip-

ment, primarily for the safety of naval navigation through the narrow corridor, must be deconflicted with the Panamanian government. The narrowness of this waterway presents very minute room for error, and necessitates the room for understanding the surrounding areas radio frequency patterns and modeling to prevent potential fratricide.

The U.S.'s presence in Colombia, Cuba, and Peru each represents a shared commitment to promoting regional and transnational security and democratic governance across the Western Hemisphere [196]. The U.S.'s shares a commitment with the countries of Colombia, Cuba, and Peru to identify, and prosecute members of transnational criminal and terrorist organizations whose activities pose a threat both to the host country as well as the U.S. These countries serve as a strong partner and coordinating focal point for U.S. law enforcement on domestic and foreign security issues pertaining to counterterrorism and counternarcotics for the purposes of dismantling criminal organizations [196]. Due to these host countries residing in areas that are not considered areas of armed conflict, they too are not covered under the previously mentioned ROE and SROE for using current CUAS capabilities against UAS threats that serve as an immediate, imminent threat to U.S. USN and USMC personnel and infrastructure. As expected, similar coordination must ensue between U.S. service components, the U.S. government, and host nation governments to ensure current and future capabilities are leveraged in a manner that is agreed upon by all parties involved.

8.5 CUAS Employment – Legal Framework Way Ahead

A survey of the operational environment prior to the employment of tools that ascertain the risk of adversely impacting civilian transportation, operations, and safety can contribute to the assessment of fratricide prior to operationalization. Surveys of the EM spectrum can further assess how effective a passive or active RF emissions CUAS capability will perform under the provided circumstances of weather, terrain, and surrounding infrastructure. Lastly, assessment of the EM spectrum and how an active and passive RF capability will perform can support the associated legal arguments for employing the aforesaid capabilities. Currently, neither the USN nor the USMC exercise any ability to determine the environmental effects pertaining to the real-time use of CUAS electronic and cyberattack detection, tracking, and neutralization capabilities. This is exemplified in the necessity and subsequent creation and establishment of the EM spectrum operations (EMSO), which is intended to blend the EW and electromagnetic spectrum (EMS) communities into one

community [197]. Historical applications of EW capabilities, to include CUASs, resulted in the operation of capabilities with little regard for the operational environment and underlying EM spectrum. Such operations resulted in fratricide related to EMI. Furthermore, neither service possesses a CUAS TTPs, concept of operation (CONOP), tactical memo, or standard operating procedure (SOP) that supports the standardized use of spectrum analysis capabilities to support understanding, modifying, or improving upon CUAS RF effectiveness [198]. Understanding the efficacy or inefficacy of an RF or cyber capability associated with a CUAS may support criteria associated with whether the capability should or could be leveraged. It further helps determine at what frequency, level of power, and direction a capability should be used in order to prevent or minimize the potential for fratricide against friendly forces and civilian infrastructure.

The operational environment and the associated RF spectrum's the USN and USMC operate in is neither fixed nor stagnant in nature. Civilian and military operations and daily activity is never completely routine, and operates from the advantage of having alternative courses of actions and solutions should a primary resource be restricted or obstructed. This includes the shift of frequencies for mobile communications, shift of frequencies and associated call signs for air traffic control and corresponding flights, the repositioning of assets to support improved movement of forces, and the use of alternate communications and associated crypto for maritime traffic operating in busy traffic separation schemes. All of these limited examples serve as a daily, weekly, or monthly change to the operational environment that must be considered and accounted for before employing capabilities that may either hinder of remove these methods of movement and positioning of assets from civil and military operations.

8.5.1 Current Electronic Warfare Protection Tools

The use of RF modeling and spectrum management capabilities is, however, germane to other aspects of USN and USMC sensitive compartmentalized operations for the very purposes of mitigating the potential of fratricide. The USN and USMC signals intelligence personnel leverage several capabilities that provide RF modeling, mapping, and battle damage assessments. These capabilities range in classification of use, from the unclassified Builder interactive scenario modeler, to the classified Own Force Monitoring (OFM) and AREPS. These RF modeling and prediction capabilities are managed under the DoN's

legacy Afloat Electromagnetic Spectrum Operations (AESOP) program.

8.5.1.1 Afloat Electromagnetic Spectrum Operations

AESOP serves as the DoN tool for ARG and CSG radar and communications planning and coordination to support RF spectrum interoperability for global maritime operations [199]. The intent of AESOP is to leverage previously allocated frequencies to generate optimal radar plans and operational tasking (OPTASK) order for communications that shall adhere with associated domestic and international laws, policies, treaties, and USN and USMC service components' emission policies. AESOP simplifies a complicated RF infrastructure for tactical warfighters by integrating and deconflicting RF capabilities with the surrounding operational environment they are intended to be employed in, as delineated in Figure 8.7.

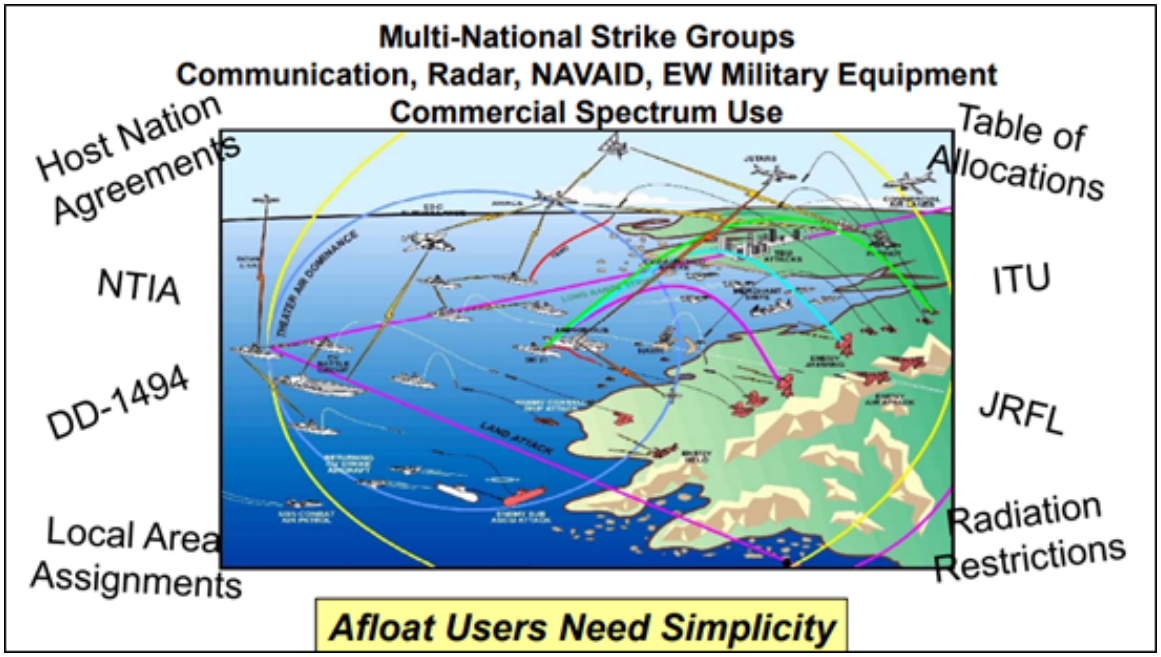


Figure 8.7. Multi-national CSG Communication, Radar, NAVAID, EW Military Equipment Commercial Spectrum Use. Source: [199].

8.5.1.2 Real-time Spectrum Operations

To support joint electromagnetic spectrum operations and in accordance with Joint Publication 3-85, AESOP was replaced by Real-Time Spectrum Operations (RTSO) in 2018, as delineated in Figure 8.8 [200].

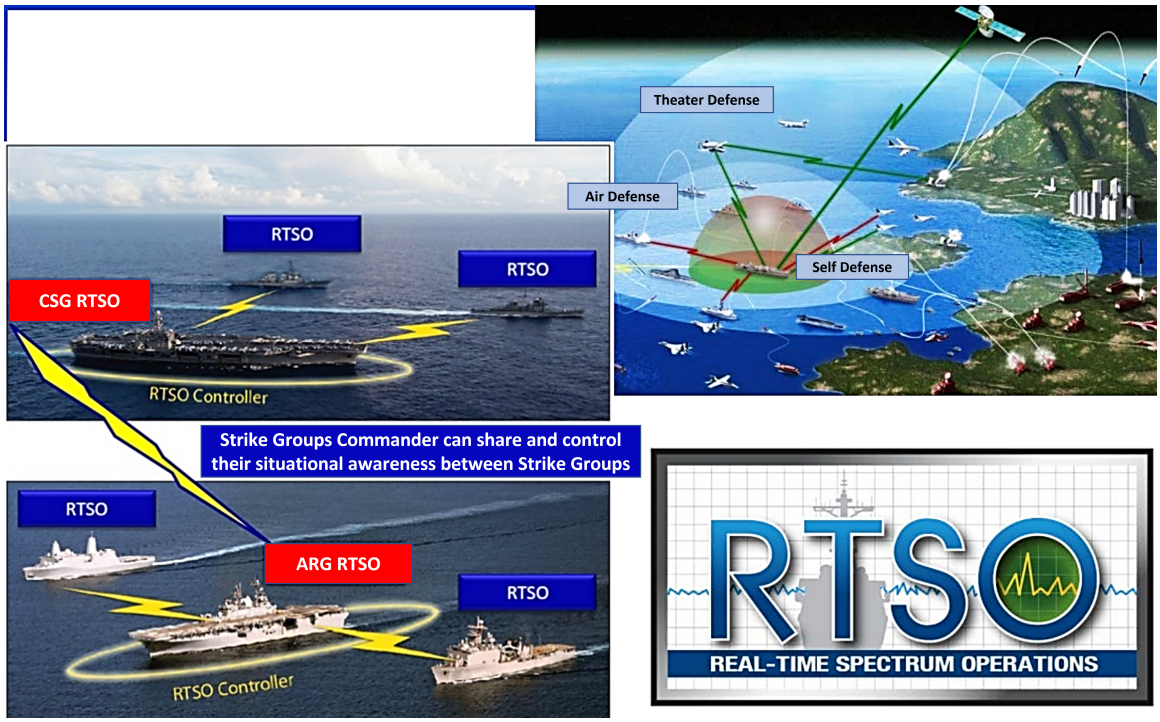


Figure 8.8. Real-time Spectrum Operations. Adapted from: [200].

RTSO supplies the same features as AESOP, still supporting the ability to promulgate OPTASK communications for tactical warfighters [201]. However, RTSO is a Windows-based USN non-program of record. Similarly, it ensures frequency compatibility and minimizes the potential for RF fratricide among radar emissions. It further allows the assignment and selection of automated circuits and frequencies and produce communications tasking for dissemination and adherence to. It is deployed on U.S. Navy, Coast Guard, and Army vessels.

Holistically, RTSO optimizes EM spectrum usage by the aforementioned means while providing real-time awareness of the operational environment and inevitable changes to the RF spectrum to the tactical decision makers and operators. This enhanced situational awareness of the RF spectrum can be leveraged to provide a premeditated response to adversarial UASs with electromagnetic and cyberattack capabilities associated with CUAS, and can further advise both military and civil decision makers on whether these capabilities will yield intended or unintended consequences following use.

8.5.1.3 Advanced Refractive Effects Prediction System

To support the enforcement of AESOP and its successor RTSO, the USN and USMC teams leverage AREPS to provide predictive analysis for their classified SIGINT capabilities [202]. AREPS serves as the successor to the legacy Integrated Refractive Effects Predictions System (IREPS). IREPS, just as its successor, was intended and provided the first capability to assess the effects of atmosphere weather against the performance of EM systems. AREPS succeeded IREPS as computing became more robust and EM propagation modeling required more advancements to account for inherent Naval system capabilities and limitation under current and future weather predictions. AREPS performs automated computation and displays the results pertaining to radar effectiveness, probability of detection of an asset, and propagation atrophy of HF, UHF, and VHF communications against the associated distance, altitude, and line of bearing from the transmitter. Similar to RTSO, AREPS leverages a Windows interface for ease of usability and operator familiarity.

AREPS uses the Advanced Propagation Model, which natively leverages the hybrid ray-optic and parabolic equation model to perform timely and accurate modeling and simulations for various sea and terrain scenarios [202]. Its calculations include, but are not limited to, the use of range-varying dielectric ground constants in support of polarization calculations and the absorption of EM energy by oxygen and water gases across a designated area of interest. These inclusions support the attainment of how far organic EM capabilities such as electronic attack may propagate from the source to a destination and the surrounding areas. AREPS natively arrives as an unclassified program with no preestablished database. As expected, users are responsible for establishing their own baselines of classified databases and network interconnectivity if required or desired. AREPS therein serves as a convenient tool to support the tactical warfighter for modeling the potential of CUAS EM emissions that are of an electronic attack definition and profile. This modeling would serve as a positive reinforcement to the preexisting rules, regulations, and policies set forth for operating current and future CUAS equipment both in CONUS and OCONUS. This modeling could be leveraged to serve as a proof-of-concept for whether CUAS capabilities should and could be used in an area of high concentration with civil and military equities. It could further support the assessment of whether CUAS capabilities could observe or yield interference as a result of fratricide.

8.5.1.4 Builder

Builder serves as a three-dimensional, interactive RF tactical decision aid currently leveraged by the USN [203]. Similar to AREPS, Builder is intended to provide the tactical warfighter an improved and comprehensive understanding of the implications associated with use of their EM capabilities. Builder accomplishes this by modeling RF propagation losses, incorporate antenna and radar cross section data as well as the effects of the surrounding environment's terrain. Builder leverages currently available National Geospatial Agency map products and Compressed Acquisition Research Center Digitized Raster Graphics and Controlled Image Base imagery and Digital Terrain Elevation Data to support interoperability and the inclusion of maximum resources to improve accuracy. Unlike AREPS, Builder does not account for atmospheric and effects impacting weather in the terrain its applied to; therefore Builder serves as a best-case tool for propagation modeling. The Builder software is unclassified as well, and therefore warrants the user to specify database and classification of subsequent drives once it is applied to a mission set. Builder serves as a cheaper alternative to solving the dilemma of modeling to support real world applications and implications associated with the use of electronic attack capabilities and potential battle damage assessment thereafter.

8.5.2 Legal Jurisdiction For Future CUAS Defeat Capabilities

As the threat evolves and advances, the counter weaponry tools must progress to meet the threat. There exists a requirement to codify the legalities and associated concept of operations for employment into an integrated cyber- and electromagnetic doctrine to support the employment of future CUAS electromagnetic and cyber capabilities. Further, there exists a necessity to update doctrine, planning, and methods of employment on a recurring basis to maintain pace with the rapidly changing operational environment. Motivation can be taken from the Army's previously released Field Manual (FM) 3-12, 'Cyberspace and Electronic Warfare Operations'. FM 3-12 provides EW and cyberspace employment guidance and direction to the Army by defining cyberspace operations and EW authorities and relationships to support Army and joint operations [204].

8.5.2.1 Codifying Advanced CUAS Tactics In Universal Doctrine

FM 3-12 captures the required tactical level decision and actions needed to support the rudimentary coordination and integration of both Army cyberspace and EW operations to support both unified land operations and joint operations in a designated AOR. Like many services, the Army too strived to converge and collate RF, cyber, and EM operations at the tactical level of warfighter to better arm tactical level commanders' and warfighters' decision making. Conversely, this allows and better informs senior decisions makers at both the operational and strategic levels of war between the Combatant Commands and their associated service elements, as well as Country Teams and host nations, with the foundational level of details needed to better support the allowance of certain capabilities and TTPs in an AOR. Further motivation can be derived by FM 3-12's distinction between electronic attack and cyberattack capabilities, and the associated authorities that govern their use. As described under the standing ROE and their supplementally classified SROE, the ability to engage an adversarial UAS through cyber or electronic attack capabilities is typically derived from a top-down authoritative process. This process involves the delegation of authority to operate from the Secretary of Defense to the DOD through executive orders (EXORDs) and ROE.

Joint forces leverage their inherent cyber and EM capabilities in non-kinetic operations in accordance with EXORDs, ROE, and other associated policies negotiated and set in place by the Secretary of Defense and Combatant Commanders. However, FM3-12 also provides a clear, distinct means of requesting approval to use new, emergent capabilities against unforeseen threats that warrant said use [204]. It is highly recommended and encouraged that a tactical unit requesting permission for the employment of a new cyber or EM capability have the network topology of the adversarial network they wish to engage, hence the necessity to leverage tools such as the DoN's Builder or AREPS to mitigate fratricide and provide battle damage assessment [204]. FM 3-12 addresses the placement of new cyber and EW capabilities in theaters of interest, based on priority of mission, location, and unit size and training. The placement of CUAS capabilities to support the high demand needs of RF deconfliction, modeling, and mapping in an area of interest is paramount to support tactical decision making [205].

8.5.2.2 Rectifying The CUAS Weapon Employment Legal Framework

The inherent defeat capabilities of CUAS equipment lie among electronic attack, cyberattack, and the mundane use of kinetic weaponry such as netting, projectiles, and small arms. We have identified and codified electronic attack as jamming or the use of directed energy to neutralize and defeat an adversarial UAS platform. We have further addressed directed energy's increased likelihood of unintended consequences to the civil-military environment it is employed in. Contrary to passive, non-directed energy methods of warfighting capabilities intended to obfuscate tactical vision aides such as smoke and camouflage, anti-optic directed energy is intended to overwhelm or burn out electronic and thermal sensors [206]. Cyberattack encompasses the use of spoofing or manipulating behavior of the adversarial UAS C2.

It is befitting of the USN and USMC to address the potential use of current and future CUAS non-kinetic and kinetic capabilities under similar constructs as addressed in other warfare areas of the DoN and Army. There uniquely exists a need to better understand the operational environment and the associated RF environment and network topology of friendly and adversarial nodes, networks, and infrastructure before leveraging non-kinetic CUAS techniques such as jamming, interference, directed energy, and cyber attack to deny, degrade, usurp, or destroy a positively identified adversarial UAS in support of a CUAS kill chain. To positively identify the surrounding civil-military and adversarial infrastructure, tools such as Builder and AREPS have proven success within the Information Warfare Community of the DoN. Such systems not only leverage current network topology based on detected emissions and the use of national technical means from classified collection agencies and networks, but they also include and address the impacts of RF propagation in the EM spectrum under weather constraints. This information serves the warfighter in two distinct areas of decision making. It provides the tactical warfighter with the understanding and risk of fratricide to the surrounding public and military services, while providing awareness of the likelihood of success should a non-kinetic technique be leveraged.

Additionally, there exists an urgent need to standardize and codify the TTPs, authorities, and review and approval process to leverage current and emerging capabilities from a cyber and EW perspective. Such inspiration can be derived from the Army's FM 3-12, which arms warfighters with the ability to determine the requisite level and use of force in an AOR to support defense in depth, force protection, and offensive operations in regards to

cyber and EW operations holistically. To be effective in CUAS operations, the USN and USMC require a combination of doctrine addressing the policies and authorities for use of emergent non-kinetic CUAS capabilities and the employment of tools to support situational awareness of the ever changing environment.

8.6 Summary

This chapter identifies the legal constraints associated with the use of weaponry yielding effects in the EMS. It further presents our assessment of the lack of synchronization across the DOD to support the deconfliction and assessment of effectiveness of CUAS capabilities in an AOR. This assessment is twofold, proving support to CUAS effectiveness under given weather, terrain, and RF propagation in an area, as well as deconfliction against fratricide from civilian and military spectrum use in an AOR. This chapter further presents options available to conduct measurement of effectiveness and deconfliction in the EMS to support host nation authorities to operate CUAS capabilities.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 9:
Conclusion and Future Work

The current threat imposed by hobbyist, non-state actors, and state actors using UASs in the operational environment has the potential to undermine USN and USMC strategic, operational, and tactical endeavors domestically and abroad. The advantage held by UAS operators is the plethora of UAS capabilities available as COTS technology. The advantage is further exacerbated by the ability to customize and modify UAS behavior and C2 to operate in different environments with varying means of communication infrastructures and specific flight profiles such as semi-autonomy, full autonomy single use, cluster use, or swarm employment. Group/cluster UASs operating with high levels of automation is an emerging threat in several of the DOD's AORs.

From Chapters 2 and 3, we assessed the ease of accessibility for Groups 1 through 3 UASs, their historic applications in nefarious manners, and their massive appeal to users as posing a significant threat to USN and USMC personnel and equities. We further find that UASs are operated in manners that are consistent with traditional air domain services to include, but not limited to ISR, C2, smuggling, information operations, and weapons delivery.

In Chapter 4, our observations delineated standard UAS C2 between the vehicle and the GCS converging at frequencies between 2.4GHz and 5.8GHz for flight and payload operations. However, the emergence of 5G delivers the potential for UASs to operate in the bands of 30GHz to 300GHz. This wide disparity in coverage for the potential use of C2 between the vehicle and the GCS or other vehicles further complicates the ability to detect, track, and neutralize UASs identified as threats.

Our analysis in Chapter 3 illustrates the varying tactics adversaries leverage under the aforesaid C2 options. These tactics vary from single use, cluster use, and swarm use. We detail in Chapter 6 the lack of effectiveness current CUAS capabilities possess against cluster and swarm UAS employment options. This is related to the inability to adequately detect and neutralize multiple, successive targets over a sustained period of time.

In Chapter 4, we assess the use of UASs as partially dependent upon the area they are operated in and therein dependent upon the area's communication infrastructure, accessibility of commercial and proprietary hardware and software, and availability of IoT communication devices. Many AORs are advancing towards institutionalized 5G communication as demonstrated in Chapter 5. At this frequency band of operation, the available CUASs leveraged by the USN and USMC are identified as ineffective due to their limitation of 5GHz. CUAS capabilities and their associated operations are currently limited to early 21st century detection techniques, such as radar, RF, EO/IR, and acoustic. In Chapter 6 we provide evidence showing the inability among the USN and USMC's currently fielded CORIAN or L-MADIS CUASs to detect and mitigate emerging technology against e.g. 5G or completely autonomous UASs.

Our research in Chapter 8 draws on the lack of legal doctrine or standardization for employing current and advanced CUAS capabilities needed to thwart emergent UAS threats, such as the use of 5G for C2. There further exists a lack of implemented spectrum analysis techniques to justify the effectiveness and legality associated with preventing or minimizing fratricide in an area of intended CUAS employment. This can be remedied with current spectrum analysis capabilities to support determining the effectiveness of CUAS RF emissions and detection. Such capabilities consist of AREPS, RTSO, OFM, and Builder. These capabilities also support the subjectivity of EMI and its potential for occurrence in an area of operation. Further, the implementation of these capabilities with CUASs can support the deconfliction and authority to operate in host nations through mission planning and assurances of limiting the potential for EMI in an area of operation.

The operational environment is saturated with both UAS and CUAS products. There remains an emergent need for the USN and USMC to conduct joint, interoperable CUAS operations against Groups 1 through 3 UAS threats. Furthermore, there now exists a requirement to support joint CUAS operations between the DOD as prescribed by the JCO. We assess current USN and USMC CUAS capabilities as only moderately effective against the UAS single and cluster methods of employment. In Chapter 7 we demonstrate the effectiveness of current USN and USMC CUAS capabilities against emergent UAS threats as inadequately effective and worsening as more UAS are operated in an area of interest. With a conservative reduction in hypothetical probability of detection and hypothetical probability of mitigation and the adjustments to the degree to which the number of simultaneous

UAS threats affects the probability of detection and mitigation of the CUAS, the model demonstrated how probability of detection and probability of mitigation would be affected which subsequently reduced the effectiveness of the CUAS against emerging UAS threats. In Chapter 6 interoperability shortfalls are identified and UAS employing different levels of collaboration for groups/clusters are discussed. One of the interoperability shortfalls is the lack of employment of common C2 standards which would enable information sharing. The Chairman of the Joint Chiefs of Staff states the need for interoperability for tactical objectives [166]. We assess CUASs should interoperate and share tactical data pertaining to the detection, tracking, and classification of the UAS in a timely and accurate manner to address the varying individual UAS threats within a group/cluster. To meet the demand of joint CUAS requirements, the USN and USMC must divest from the previous mentality of temporary solutions for a permanent problem set. Long-term, interoperable CUAS solutions, capable of performing at high rates of effectiveness against current and emergent UAS threats must remain a priority for USN and USMC CUAS agendas.

9.1 Recommendations

The following list encapsulates suggested recommendations to improve CUAS interoperability in the geopolitical environment:

- Establish a common baseline architecture to be used as the foundation for the DoN CUAS *supported by*:
  - Configuration management to management evolving software.
  - Change management to manage changes in requirements or mission shifts.
- Integrate AREPS into existing and future CUASs to provide the capability to adjust radar and RF detection and tracking techniques and to compute and display passive RF probability of detection.
- Implement CUAS capability designs that provide:
  - high probability of detection at extended ranges.
  - sensor placement accounting for threat axis and geometry of the terrain.
  - high probability of detection for a high number of simultaneous UAS targets.

9.2 Future Work

Advances in technology will continue to be adopted by emerging UAS threats and adversaries will likely increase their utilization of UASs to achieve their objectives. Therefore, future research should examine the integration of new techniques such as machine learning and other cyber capabilities into emergent CUASs to enhance detection and mitigation and support the promulgation of UAS threat libraries. Future integration efforts must also consider the level of impact to current and emergent CUAS interoperability and effectiveness. Additionally, understanding how terrain impacts UAS TTPs leveraged by adversaries may show the subsequent need for CUAS terrain-based TTPs to counter adversaries.

The threat UASs pose today are here to stay and will likely worsen in the near future. USN and USMC CUAS lines of efforts need to be closely aligned to counter the growing threat imposed by COTS UASs threat. It is necessary to establish clear requirements for current and future CUAS acquisitions to be interoperable.

Bibliography

[1] M. Jamison, "C-suas industry open house," presented at DOD C-sUAS Industry Open House, Arlington, VA, USA, Oct. 30 2020 [Online]. Available: https://govtribe.com/file/government-file/c-suas-industry-open-house-presentation-dot-pdf

[2] N. Strout, "Army selects eight counter-drone systems for the joint force," Defense News, June 26, 2020 [Online]. Available: https://www.defensenews.com/unmanned/2020/06/26/army-selects-eight-counter-drone-systems-for-the-joint-force/

[3] B. Jackson, D. Frelinger, M. Lostumbo, and R. Button. Evaluating novel threats to the homeland: unmanned aerial vehicles and cruise missiles. RAND National Defense Research Institute. Santa Monica, CA, USA, 2008 [Online]. Available: https://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG626.pdf.

[4] A. Michel. *Counter-Drone Systems*. Center for the Study of Drone at Bard College, Annadale-on-Hudson, NY, USA, 2018 [Online]. Available: https://dronecenter.bard.edu/files/2018/02/CSD-Counter-Drone-Systems-Report.pdf

[5] Office of the Secretary of Defense, "FY2009-2034 Unmanned Systems Integrated Roadmap," Washington, DC, USA, 2009 [Online]. Available: https://apps.dtic.mil/sti/citations/ADA522247

[6] S. O'Donnel, "A not-so short history of unmanned aerial vehicles (uav)," Consortiq, Jun. 10, 2020 [Online]. Available: https://consortiq.com/short-history-unmanned-aerial-vehicles-uavs/

[7] M. Benjamin and B. Ehrenreich, *Drone Warfare: Killing by Remote Control*. London, England, UK: Verso, 2013.

[8] J. Stamp, "Unmanned drones have been around since world war i," Smithsonian Magazine, February 13, 2013 [Online]. Available: https://www.smithsonianmag.com/arts-culture/unmanned-drones-have-been-around-since-world-war-i-16055939/

[9] P. Springer, *Military Robots and Drones: A Reference Handbook*. Santa Barbara, CA, USA: ABC-CLIO, 2013.

[10] N. Budanovic, "The early days of drones—unmanned aircraft from world war one and world war two," War History Online, July 13, 2017 [Online]. Available: https://www.warhistoryonline.com/military-vehicle-news/short-history-drones-part-1-m.html

[11] J. Ding and H. Mei, "Frontier progress of unmanned aerial vehicles optical wireless technologies," *Sensors*, vol. 20, no. 19, Sep. 2020 [Online]. Available: https://doi.org/10.3390/s20195476

[12] K. Pletcher, "Tokyo subway attack of 1995," Britannica, March 13, 2021 [Online]. Available: https://www.britannica.com/event/Tokyo-subway-attack-of-1995

[13] M. Gips, "A remote threat. (News and trends)," Questia, Accessed August 04, 2020 [Online]. Available: https://www.questia.com/magazine/1G1-92850644/a-remote-threat-news-and-trend

[14] E. Miasnikov, "Colombia - FARC drones discovered," *EFE News Service*, p. 25, 2002.

[15] E. Miasnikov, *Threat of Terrorism Using Unmanned Aerial Vehicles: Technical Aspects*. Moscow, Russia: Center for Arms Control, Energy and Environmental Studies Moscow Institute of Physics and Technology, 2005.

[16] The Washington Times, "Leaders reschedule summit for next week," *The Washington Times*, Mar. 10, 2004 [Online]. Available: https://www.washingtontimes.com/news/2004/mar/10/20040310-101149-4514r/

[17] D. Gormley, "Globalization and WMD Proliferation Networks: The Case of Unmanned Air Vehicles as Terrorist Weapons," *Strategic Insights*, vol. V, p. 15, Jul. 2006 [Online]. Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/a521376.pdf

[18] D. Praisler, "Counter-uav solutions for the joint force," Ph.D. dissertation, Air War College, Montgomery, AL, USA, 2017 [Online]. Available: https://apps.dtic.mil/sti/pdfs/AD1037984.pdf

[19] A. Clevenger, "Andrew Clevenger on Twitter," Twitter, October 24, 2017 [Online]. Available: https://twitter.com/andclev/status/922829571644325890

[20] Z. Haver, "Chinese drones fly near Taiwan-held island in South China Sea," Radio Free Asia, April 07, 2021 [Online]. Available: https://www.rfa.org/english/news/china/taiwan-drones-04072021180138.html

[21] D. Gettinger, "Drones operating in Syria and Iraq," The Center for the Study the Drones at Bard College, December 13, 2016 [Online]. Available: https://dronecenter.bard.edu/drones-operating-in-syria-and-iraq/

[22] T. Karygiannis, B. Eydt, G. Barber, L. Bunn, and T. Phillips, "Guidelines for securing radio frequency identification (RFID) systems," NIST, Gaithersburg, MD, USA, NIST SP 800-98, 2007 [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-98.pdf

[23] Measure, "Waypoints flights." Accessed June 24, 2021 [Online]. Available: https://www.measure.com/help/autonomous-flight-with-waypoint

[24] United States Space Force, "New civil signals," August 10, 2020 [Online]. Available: https://www.gps.gov/systems/gps/modernization/civilsignals/

[25] A. Michel and D. Gettinger, "Drones at home: drone incidents," The Center for the Study the Drones at Bard College, April 27, 2017 [Online]. Available: https://dronecenter.bard.edu/drones-at-home-drone-incidents/

[26] A. Tahir, J. Böling, M.-H. Haghbayan, H. T. Toivonen, and J. Plosila, "Swarms of unmanned aerial vehicles — a survey," *Journal of Industrial Information Integration*, vol. 16, p. 100106, 2019 [Online]. Available: https://doi.org/10.1016/j.jii.2019.100106

[27] Department of Defense, "Department of Defense announces successful micro-drone demonstration," January 9, 2017 [Online]. Available: https://www.defense.gov/Newsroom/Releases/Release/Article/1044811/department-of-defense-announces-successful-micro-drone-demonstration/

[28] Office of the Secretary of Defense, "Unmanned Systems Integrated Roadmap 2017-2042," Washington, DC, USA, 2018 [Online]. Available: https://news.usni.org/2018/08/30/pentagon-unmanned-systems-integrated-roadmap-2017-2042

[29] Office of the Secretary of Defense, "Unmanned Systems Integrated Roadmap 2005-2030," Washington, DC, USA, 2006 [Online]. Available: https://fas.org/irp/program/collect/uav_roadmap2005.pdf

[30] M. Campion, P. Ranganathan, and S. Faruque, "A review and future directions of UAV swarm communication architectures," *2018 IEEE International Conference on Electro/Information Technology (EIT)*, p. 6, 2018 [Online]. Available: https://und.edu/research/rias/_files/docs/swarm_ieee.pdf

[31] S. Romaniuk, "Military strategy and the three levels of warfare," Defence Report, November 30, 2017 [Online]. Available: https://defencereport.com/wp-content/uploads/2017/11/Romaniuk-Military-Strategy-and-the-Three-Levels-of-Warfare.pdf

[32] Department of Defense, "U.S. Department of Defense count-small unmanned aircraft systems strategy." Accessed October 11, 2020 [Online]. Available: https://media.defense.gov/2021/Jan/07/2002561080/-1/-1/1/DEPARTMENT-OF-DEFENSE-COUNTER-SMALL-UNMANNED-AIRCRAFT-SYSTEMS-STRATEGY.PDF

[33] B. Hubbard, P. Karasz, and S. Reed, "Two major Saudi oil installations hit by drone strike, and U.S. blames Iran," *The New York Times*, Sep. 15, 2019 [Online]. Available: https://www.nytimes.com/2019/09/14/world/middleeast/saudi-arabia-refineries-drone-attack.html

[34] M. D. Shear and M. S. Schmidt, "White House drone crash described as a U.S. worker's drunken lark," *The New York Times*, Jan. 15, 2015 [Online]. Available: https://www.nytimes.com/2015/01/28/us/white-house-drone.html

[35] G. Cohen, "Israel unsuccessfully tries to intercept drone that breached its airspace," *Haaretz Israel News*, Jul. 17, 2016 [Online]. Available: https://www.haaretz.com/israel-news/israel-tries-fails-to-intercept-drone-over-that-breached-its-airspace-1.5411557

[36] J. R. Hoehn and K. M. Sayler, "Department of Defense counter-unmanned aircraft systems," Washington, DC, USA, CRS Report No. IF11426 v1, 2020 [Online]. Available: https://crsreports.congress.gov/product/pdf/IF/IF11426/1

[37] The Economist, "Home-made drones now threaten conventional armed forces," February 10, 2018 [Online]. Available: https://www.economist.com/science-and-technology/2018/02/08/home-made-drones-now-threaten-conventional-armed-forces

[38] J. Stringfellow, "Aegis - the shield of the fleet," Lockheed Martin 2021 [Online]. Available: https://www.lockheedmartin.com/en-us/products/aegis-combat-system.html

[39] R. Pickrell, "China deploys drones to spy on the South China Sea like never before," Business Insider, September 11, 2019 [Online]. Available: https://www.businessinsider.com/chinese-is-deploying-drones-to-spy-on-south-china-sea-2019-9

[40] Center for Strategic and International Studies, "Is China at the forefront of drone technology?" May 29, 2018 [Online]. Available: https://chinapower.csis.org/china-drones-unmanned-technology/

[41] N. Turak, "How Saudi Arabia failed to protect itself from drone and missile attacks despite billions spent on defense systems," CNBC, September 19, 2019 [Online].

Available: https://www.cnbc.com/2019/09/19/how-saudi-arabia-failed-to-protect-itself-from-drones-missile-attacks.html

[42] J. Judson, "House panel wants cheaper Patriot missile," Defense News, June 05, 2019 [Online]. Available: https://www.defensenews.com/land/2019/06/05/house-panel-wants-cheaper-patriot-missile/

[43] D. Hawkins, ""A U.S. 'ally' fired a $3 million Patriot missile at a $200 drone. Spoiler: the missile won."," *The Washington Post*, Mar. 13, 2017 [Online]. Available: https://www.washingtonpost.com/news/morning-mix/wp/2017/03/17/a-u-s-ally-fired-a-3-million-patriot-missile-at-a-200-drone-spoiler-the-missile-won/

[44] Acumen Research and Consulting, "Anti-drone market size worth around US$ 4.43 billion by 2026," Globe Newswire , January 28, 2020 [Online]. Available: http://www.globenewswire.com/news-release/2020/01/28/1976029/0/en/Anti-Drone-Market-Size-Worth-Around-US-4-43-Billion-by-2026.html

[45] G. C. Birch, J. C. Griffin, and M. K. Erdman, "UAS detection, classification, and neutralization: market survey 2015," Sandia National Laboratories, Albuquerque, NM, USA, SAND 2015-6365, 2015 [Online]. Available: http://www.osti.gov/servlets/purl/1222445/

[46] J. Whitney, "Counter UAS technology report," Intelligent Aerospace, December 12, 2019 [Online]. Available: https://www.intelligent-aerospace.com/unmanned/article/14073687/counter-uas-technology-report

[47] National Urban Security Technology Laboratory, "Counter-unmanned aircraft systems technology guide," Department of Homeland Security, February 28, 2020 [Online]. Available: https://www.dhs.gov/sites/default/files/publications/c-uas-tech-guide_final_28feb2020.pdf.

[48] Precision Hawk, "Beyond the edge: how advanced drones, sensors, and flight operations are redefining the limits of remote sensing." Accessed June 24, 2021 [Online]. Available: https://www.precisionhawk.com/sensors/advanced-sensors-and-data-collection/thermal

[49] Internet Engineering Task Force, "Drone remote ID protocol (DRIP)," Datatracker, September 12, 2020 [Online]. Available: https://datatracker.ietf.org/wg/drip/about/

[50] S. LaGrone, "U.S. Navy allowed to use Persian Gulf laser for defense," USNI News, December 10, 2014 [Online]. Available: https://news.usni.org/2014/12/10/u-s-navy-allowed-use-persian-gulf-laser-defense

[51] M. Kaufmann and J. R. Vacca, *Computer and Information Security Handbook*, 3rd ed. Manhattan, KS: Elsevier Inc, 2017.

[52] 911 Security, “Drone communication - data link.” Accessed July 12, 2021 [Online]. Available: https://www.911security.com/learn/airspace-security/drone-fundamentals/drone-communication-data-link

[53] *DOD Joint Services Weapon and Laser System Safety Review Processes*, DOD Instruction 5000.69, Department of Defense, Washington, DC, 2017.

[54] National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, Sec. 1602. 2017 [Online]. Available: https://www.congress.gov/bill/115th-congress/house-bill/2810

[55] Cornell Law School, “18 U.S. Code § 1030 - Fraud and Related Activity in Connection With Computers,” Legal Information Institute, Accessed August 31, 2021 [Online]. Available: https://www.law.cornell.edu/uscode/text/18/1030

[56] Office of the Federal Register, “Electronic code of federal regulations (eCFR).” Accessed September 28, 2020 [Online]. Available: https://www.ecfr.gov/

[57] G. Balamurugan, J. Valarmathi, and V. P. S. Naidu, “Survey on UAV navigation in GPS denied environments,” in *2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)*, 2016, pp. 198–204.

[58] M. C. Horowitz and M. Fuhrmann, “Droning on: explaining the proliferation of unmanned aerial vehicles,” Social Science Research Network, Rochester, NY, USA, SSRN Scholarly Paper ID 2514339, 2015 [Online]. Available: https://papers.ssrn.com/abstract=2514339

[59] J. Nicas and C. Murphy, “Who builds the world’s most popular drones? ,” *Wall Street Journal*, Nov. 10, 2014 [Online]. Available: https://online.wsj.com/articles/who-builds-the-worlds-most-popular-drones-1415645659

[60] Drone Flyers, “2013 vs. 2017 - how much camera drone tech do you get for your money? ,” July 25, 2017 [Online]. Available: https://www.droneflyers.com/2013-vs-2017-much-camera-drone-tech-get-money/

[61] C. Shu, “EHANG, maker of ghost drone, raises $10M Series A led by GGV Capital,” Tech Crunch, December 30, 2014 [Online]. Available: https://social.techcrunch.com/2014/12/30/ehang-seriesa/

[62] National Intelligence Council, “Nonstate actors: impact on international relations and implications for the united states,” August 23, 2007 [Online]. Available: https://www.dni.gov/files/documents/nonstate_actors_2007.pdf

[63] J. Binnie, "Iranian media identifies Ababil-3 UAV," IHS Jane's Defence Weekly, Accessed December 16, 2020 [Online]. Available: http://www.janes.com/article/40484/iranian-media-identifies-ababil-3-uav.

[64] K. Sayler, "A world of proliferated drones: a technology primer," Center for New American Security, June 30, 2015 [Online]. Available: http://drones.cnas.org/wp-content/uploads/2016/03/CNAS-World-of-Drones_052115.pdf

[65] Y. Dreazen, "The Next Arab-Israeli War Will Be Fought with Drones," *The New Republic*, Mar. 26, 2014 [Online]. Available: https://newrepublic.com/article/117087/next-arab-israeli-war-will-be-fought-drones

[66] Israel Aerospace Industries, "Heron TP MALE unmanned aerial system (UAS)," December 18, 2020 [Online]. Available: https://www.iai.co.il/p/heron-tp

[67] T. Craig, "Pakistan says it will deploy its own armed drone against terrorists," *The Washington Post*, Mar. 13, 2015 [Online]. Available: https://www.washingtonpost.com/world/pakistan-says-it-will-deploy-its-own-armed-drone-against-terrorists/2015/03/13/ac0a9008-c98d-11e4-bea5-b893e7ac3fb3_story.html

[68] United States European Command Public Affairs, "Senate Armed Services Committee hearing on United States European Command and United States Transportation Command defense authorization request for fiscal year 2021," February 26, 2020 [Online]. Available: https://www.eucom.mil/transcript/40285/senate-armed-services-committee-hearing-on-un

[69] J. Garamone, "Northcom commander calls for 21st century tools to defeat current threats," DOD News, March 11, 2020 [Online]. Available: https://www.defense.gov/Explore/News/Article/Article/2109462/northcom-commander-calls-for-21st-century-tools-to-defeat-current-threats/

[70] Dronefly, "Anatomy of a drone infographic," July 14, 2020 [Online]. Available: https://www.dronefly.com/the-anatomy-of-a-drone

[71] W. James, "How far can a 2.4 GHz drone go?" Best Quadcopter, June 12, 2020 [Online]. Available: https://www.best-quadcopter.com/buying-guide/2020/06/how-far-can-a-2-4-ghz-drone-go/

[72] SATEL, "Radio connection distance and RF setup," August 23, 2020 [Online]. Available: https://www.satel.com/wp-content/uploads/2019/08/FAQ-0041_Radio-connection-distance-and-RF-setup_v.1.0.pdf

[73] M. Woodley, "Bluetooth specification version 5.0," Bluetooth SIG, Inc., August 21, 2021 [Online]. Available: https://www.bluetooth.com/bluetooth-resources/bluetooth-5-go-faster-go-further/

[74] D. Kelley, "Is bluetooth security good enough for your most sensitive corporate communications?" Security Intelligence, December 12, 2016 [Online]. Available: https://securityintelligence.com/is-bluetooth-security-good-enough-for-your-most-sensitive-corporate-communications/

[75] I. Arghire, "BLURtooth vulnerability can allow bluetooth MITM attacks," Security Week, September 10, 2020 [Online]. Available: https://www.securityweek.com/blurtooth-vulnerability-can-allow-bluetooth-mitm-attacks

[76] P. Cope, J. Campbell, and T. Hayajneh, "An investigation of bluetooth security vulnerabilities," *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 1–7, Jan. 2017 [Online]. Available: https://doi.org/10.1109/CCWC.2017.7868416

[77] Drones UAV Report, "Guide to significantly boost your drone range," April 15, 2020 [Online]. Available: https://dronesuavreport.com/2019/04/15/guide-to-significantly-boost-your-drone-range/

[78] ElectronicNotes, "Wifi standards: IEEE 802.11," April 19, 2021 [Online]. Available: https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/standards.php

[79] L. Davoli, E. Pagliari, and G. Ferrari, "Hybrid LoRa-IEEE 802.11s opportunistic mesh networking for flexible UAV swarming," *Drones*, vol. 5, no. 2, p. 26, June 2021. Available: https://doi.org/10.3390/drones5020026

[80] C. He and J. Mitchell, "Security analysis and improvements for IEEE 802.11i," in *Network and Distributed System Security Symposium (NDSS)*, 2005 [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/2017/09/Security-Analysis-and-Improvements-for-IEEE-802.11i-Changhua-He.pdf

[81] J. R. Vacca, *Network and System Security*, 2nd ed. Manhattan, KS, USA: Science Direct, 2014 [Online]. Available: https://doi.org/10.1016/C2011-0-08779-3

[82] S. Mandal, K. Maheta, V. Kumar, and M. S. Prasad, "Control of UAV using GSM technology," in *Proceedings of the International Conference on Modern Research in Aerospace Engineering*, Singapore, 2018, pp. 77–85.

[83] L. Sundqvist, "Cellular controlled drone experiment: Evaluation of network requirements," M. Sci. thesis, Dept. of Communications and Networking, Aalto University School of Engineering, Espoo, Finland, Nov. 2005.

[84] C. Sbeglia, "Four 5G drone demonstrations and trials," RCR Wireless News, September 22, 2020 [Online]. Available: https://www.rcrwireless.com/20200922/carriers/four-5g-drone-demonstrations-and-trials

[85] P. Choudhari, V. Kaul, and S. K. Narayankhedkar, "An enhanced encryption algorithm for 4G networks," *International journal of engineering research and technology*, vol. 3, no. 6, 2014. Available: https://www.ijert.org/research/an-enhanced-encryption-algorithm-for-4g-networks-IJERTV3IS061214.pdf

[86] M. Hadded, "Does 5G create new cybersecurity risks?" Electronics 360, March 17, 2021 [Online]. Available: https://electronics360.globalspec.com/article/16468/does-5g-create-new-cybersecurity-risks

[87] Unmanned Systems Technology. "Satellite Receivers & SATCOM". Accessed March 11, 2021 [Online]. Available: https://www.unmannedsystemstechnology.com/category/supplier-directory/data-communications/satellite-receivers-satcom/

[88] M. Chen, U. Challita, W. Saad, C. Yin, and M. Debbah, "Artificial neural networks-based machine learning for wireless networks: A tutorial," *IEEE Communications Surveys Tutorials*, vol. 21, no. 4, pp. 3039–3071, Jul. 2019 [Online]. Available: https://doi.org/10.1109/COMST.2019.2926625

[89] J.-P. Yaacoub, H. Noura, O. Salman, and A. Chehab, "Security analysis of drones systems: Attacks, limitations, and recommendations," *Internet of Things*, vol. 11, p. 100218, May 2020 [Online]. Available: https://doi.org/10.1016/j.iot.2020.100218

[90] Honeywell International Inc. "Small UAV SATCOM". Accessed July 15, 2021 [Online]. Available: https://aerospace.honeywell.com/content/dam/aerobt/en/documents/landing-pages/brochures/N61-2386-000-000_UAV_SATCOM-bro.pdf

[91] M. Monnik, "Hacking the DJI phantom 3 drone," DroneSec, August 16, 2021 [Online]. Available: https://dronesec.com/blogs/articles/hacking-the-dji-phantom-3-drone

[92] Da-Jiang Innovations, "Datalink 3." Accessed August 16, 2021 [Online]. Available: https://www.dji.com/datalink-3

[93] L. Bigazzi, M. Basso, E. Boni, G. Innocenti, and M. Pieraccini, "A multilevel architecture for autonomous UAVs," *Drones*, vol. 5, no. 3, p. 55, Jun. 2021 [Online]. Available: https://doi.org/10.3390/drones5030055

[94] E. Nettleton, S. Thrun, H. Durrant-Whyte, and S. Sukkarieh, "Decentralised SLAM with low-bandwidth communication for teams of vehicles," in *Field and Service Robotics: Recent Advances in Research and Applications* (Springer Tracts in Advanced Robotics), S. Yuta, H. Asama, E. Prassler, T. Tsubouchi, and S. Thrun, Eds. Berlin, Germany: Springer Berlin Heidelberg, 2006, pp. 179–188.

[95] J. Barnard, "Small UAV command, control and communication issues," in *2007 IET Seminar on Communicating with UAV's*, 2007 [Online]. Available: https://ieeexplore.ieee.org/document/4450038

[96] Da-Jiang Innovations, "DJITelloPy API Reference." Accessed August 16, 2021 [Online]. Available: https://djitellopy.readthedocs.io/en/latest/tello/

[97] D. Baldwin, "Tello drone programming with Python," DroneBlocks, Accessed August 16, 2021 [Online]. Available: https://learn.droneblocks.io/p/tello-drone-programming-with-python

[98] D. B. Larter, "Jim Mattis' 'dynamic force employment' concept just got real for the US Navy," Defense News, July 16, 2018 [Online]. Available: https://www.defensenews.com/naval/2018/07/16/jim-mattis-dynamic-force-employment-just-got-real-for-the-us-navy/

[99] United States Africa Command, "What we do." Accessed February 3, 2021 [Online]. Available: https://www.africom.mil/what-we-do

[100] Military Bases, "US military bases in Djibouti." Accessed July 21, 2021 [Online]. Available: https://militarybases.com/overseas/djibouti/

[101] F. A. Gebreab, "Getting connected: Competition and diffusion in African mobile telecommunications markets," working paper, World Bank, Washington D.C., USA, 2002 [Online]. Available: https://documents1.worldbank.org/curated/en/399831468741917899/104504322_20041117162008/additional/multi0page.pdf

[102] G. Mortimer, "Denel Dynamics touts South African UAV expertise," sUAS News, March 7, 2012 [Online]. Available: https://www.suasnews.com/2012/03/denel-dynamics-touts-south-african-uav-expertise/

[103] Denel Dynamics, "Welcome to Denel Dynamics." Accessed July 21, 2021 [Online]. Available: http://www.deneldynamics.co.za/

[104] P. Bergen, M. Salyk-Virk, and D. Sterman, "World of drones," New America, July 30, 2020 [Online]. Available: http://newamerica.org/international-security/reports/world-drones/

[105] Q. Velluet, "Africa's drone industry is taking off," The Africa Report, January 12, 2021. Available: https://www.theafricareport.com/58486/africas-drone-industry-is-taking-off/

[106] K. Okeleke and S. Suardi, "2020 the mobile economy sub-saharan Africa," GSMA, September 30, 2020 [Online]. Available: https://www.gsma.com/mobileeconomy/sub-saharan-africa/

[107] United States Central Command, "CENTCOM priorities." Accessed April 4, 2021 [Online]. Available: https://www.centcom.mil/ABOUT-US/COMMAND-PRIORITIES/

[108] S. D. Rosbo, H. Lancaster, and K. Wansink, "2019 global fixed broadband - analyses, statistics and regional overviews," Budde Communications, Sydney, Australia, 16th edition, 2019 [Online]. Available: https://www.budde.com.au/Research/2019-Global-Fixed-Broadband-Analyses-Statistics-and-Regional-Overviews

[109] Budde Communications, "The middle east relies heavily on mobile infrastructure during 2020," GlobeNewswire, July 20, 2020 [Online]. Available: https://www.globenewswire.com/news-release/2020/07/20/2064406/0/en/The-Middle-East-relies-heavily-on-mobile-infrastructure-during-2020.html

[110] AP Consulting, "Middle East articles - telecommunications in the Middle East." Accessed April 15, 2021 [Online]. Available: http://www.mideastlaw.com/article_telecommunications_in_the_middle_east.html

[111] D. D. Luce, "Iranian-backed Houthi rebels in Yemen ramp up drone, missile attacks on Saudi Arabia," NBC News March 12, 2021 [Online]. Available: https://www.nbcnews.com/news/world/iranian-backed-houthi-rebels-yemen-ramp-drone-missile-attacks-saudi-n1260488

[112] M. S. Schmidt and E. Schmitt, "Pentagon confronts a new threat from ISIS: Exploding drones," *The New York Times*, Oct. 10, 2016 [Online]. Available: https://www.nytimes.com/2016/10/12/world/middleeast/iraq-drones-isis.html

[113] Center for Strategic and International Studies, "Hay'at Tahrir al-Sham (HTS)." Accessed July 13, 2021 [Online]. Available: https://www.csis.org/programs/transnational-threats-project/past-projects/terrorism-backgrounders/hayat-tahrir-al-sham

[114] Haaretz, "Russia: Drones used in Syria base attacks indicate 'outside assistance'," January 11, 2018 [Online]. Available: https://www.haaretz.com/middle-east-news/syria/russia-drones-used-in-syria-base-attacks-indicate-outside-assistance-1.5730232

[115] Statista, "Leading telecommunications brands in the Middle East in 2020, by brand value," August 28, 2020 [Online]. Available: https://www.statista.com/statistics/971969/middle-east-leading-telecom-brands-by-value/

[116] United Nations Office on Drugs and Crime. The use of the Internet for terrorist purposes. United Nations. New York City, NY, USA, 2012 [Online]. Available: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

[117] R. Blackwill and S. Sestanovich, "Conflict in Ukraine," Council on Foreign Relations, July 22, 2021 [Online]. Available: https://microsites-live-backend.cfr.org/global-conflict-tracker/conflict/conflict-ukraine

[118] United States European Command, "Commander's priorities." Accessed April 15, 2021 [Online]. Available: https://www.eucom.mil/organization/commanders-priorities

[119] C. Barnard, "Improve U.S. maritime posture in Europe through strategic realignment," Center for International Maritime Security, January 27, 2021 [Online]. Available: https://cimsec.org/improve-u-s-maritime-posture-in-europe-through-strategic-realignment/

[120] United States European Command, "Organization." Accessed July 27, 2021 [Online]. Available: https://www.eucom.mil/organization

[121] United States Naval Forces Europe-Africa/United States 6th Fleet, "Ctf-65." Accessed July 23, 2021 [Online]. Available: https://www.c6f.navy.mil/About-Us/Our-Task-Forces/CTF-65/

[122] Morgan Stanley, "European telcos build for speed," November 7, 2019 [Online]. Available: https://www.morganstanley.com/ideas/europe-telcos-5G-wireless-infastructure

[123] A. Patil, D. Tewar, and R. Humbare, "Europe 5G infrastructure outlook - 2027," Allied Market Research, August 19, 2020 [Online]. Available: https://www.alliedmarketresearch.com/europe-5g-infrastructure-market

[124] K. Johnson, "Why is China buying up Europe's ports?" Foreign Policy, February 02, 2018 [Online]. Available: https://foreignpolicy.com/2018/02/02/why-is-china-buying-up-europes-ports/

[125] European Commission, "Trade: policy: countries and regions: China." Accessed April 19, 2021 [Online]. Available: https://ec.europa.eu/trade/policy/countries-and-regions/countries/china/

[126] Mordor Intelligence, "Europe small UAV market - growth, trends, COVID-19 impact, and forecasts (2021-2026)." Accessed April 19, 2021 [Online]. Available: https://www.mordorintelligence.com/industry-reports/europe-small-uav-market-industry

[127] C. Palestini, "Countering drones: looking for the silver bullet," NATO Review, Decemeber 16, 2020 [Online]. Available: https://www.nato.int/docu/review/articles/2020/12/16/countering-drones-looking-for-the-silver-bullet/index.html

[128] N. Martin, "Drones could be used in terror attacks, EU Security Chief fears," Deutsche Welle, March 08, 2019 [Online]. Available: https://www.dw.com/en/drones-could-be-used-in-terror-attacks-eu-security-chief-fears/a-49876427

[129] S. Sprenger, "European Union's defense arm urges work on common counter-drone weapon," Defense New, November 30, 2020 [Online]. Available: https://www.defensenews.com/global/europe/2020/11/30/european-unions-defense-arm-urges-work-on-common-counter-drone-weapon/

[130] Eurostat, "Being young in Europe today - digital world." Accessed May 20, 2021 [Online]. Available: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Being_young_in_Europe_today_-_digital_world

[131] Connection Cafe, "Dissecting the U.S. telecommunications infrastructure," April 20, 2018 [Online]. Available: https://www.connectioncafe.com/dissecting-the-u-s-telecommunications-infrastructure/

[132] Cyber and Infrastructure Security Agency, "Communications sector." Accessed April 20, 2021 [Online]. Available: https://www.cisa.gov/communications-sector

[133] Mordor Intelligence, "North america small UAV market - growth, trends and forecast (2021-2026)." Accessed July 23, 2021 [Online]. Available: https://www.mordorintelligence.com/industry-reports/north-america-small-uav-market-industry

[134] Market Data Forecast, "North America agricultural drones market," April 23, 2021 [Online]. Available: https://www.marketdataforecast.com/market-reports/na-agricultural-drones-market

[135] A. Solodov, A. Williams, S. Al Hanaei, and B. Goddard, "Analyzing the threat of unmanned aerial vehicles (UAV) to nuclear facilities," *Security Journal*, vol. 31, no. 1, pp. 305–324, Feb. 2018 [Online]. Available: https://doi.org/10.1057/s41284-017-0102-5

[136] R. J. Bunker, "Terrorist and insurgent unmanned aerial vehicles: Use, potentials, and military implications," U.S. Army War College, Strategic Studies Institute, Carlisle Barracks, PA, USA, ADA623134, 2015 [Online]. Available: hhttps://apps.dtic.mil/sti/pdfs/ADA623134.pdf

[137] United States Indo-Pacific Command, "About United States Indo-Pacific command." Accessed April 19, 2021 [Online]. Available: https://www.pacom.mil/About-USINDOPACOM/

[138] A. W. Dowd, "NATO's Pacific plans," The American Legion, February 17, 2021 [Online]. Available: https://www.legion.org/landingzone/251823/natos-pacific-plans

[139] S. Millward, "Asia's mobile and broadband internet speeds, in one infographic," Tech in Asia, November 2, 2016 [Online]. Available: https://www.techinasia.com/asia-internet-speeds-mobile-broadband

[140] V. Arianti and M. Taufiqurrohman, "Weaponized drones: The next terrorist modus operandi in Southeast Asia?" The Diplomat, April 12, 2021 [Online]. Available: https://thediplomat.com/2021/03/weaponized-drones-the-next-terrorist-modus-operandi-in-southeast-asia/

[141] D. Makichuk, "China experiencing a drone 'revolution' in agriculture," Asia Times, October 26, 2020 [Online]. Available: https://asiatimes.com/2020/10/china-experiencing-a-drone-revolution-in-agriculture/

[142] R. K. Nichols, H. Mumm, W. Lonstein, C. Carter, and J. Hood, *Chinese Drones in Spratly Islands, and Chinese Threats to USA forces in Pacific*, 2nd ed. Manhattan, KS, USA: New Prairie Press, 2007, pp. 390–414.

[143] A. Rodgers, "Rise of the machines," United States Indo-Pacific Command, February 25, 2020 [Online]. Available: https://www.pacom.mil/Media/News/News-Article-View/Article/2093652/rise-of-the-machines/

[144] H. I. Sutton, "China builds surveillance network in South China Sea," Forbes, August 5, 2020 [Online]. Available: https://www.forbes.com/sites/hisutton/2020/08/05/china-builds-surveillance-network-in-international-waters-of-south-china-sea/?sh=61c5c9a674f3

[145] B. Speegle and K. O'Keefe, "China exploits fleet of U.S. satellites to strengthen police and military power," *The Wall Street Journal*, Apr. 23, 2019 [Online]. Available: https://www.wsj.com/articles/china-exploits-fleet-of-u-s-satellites-to-strengthen-police-and-military-power-11556031771

[146] C. T. Lopez, "Southcom Can Use More ISR Capacity, Security Cooperation," Department of Defense, April 15, 2021 [Online]. Available: https://www.defense.gov/Explore/News/Article/Article/2574990/southcom-can-use-more-isr-capacity-security-cooperation/

[147] United States Southern Command, "SOUTHCOM components & units." Accessed April 20, 2021 [Online]. Available: https://www.southcom.mil/About/SOUTHCOM-Components-and-Units/

[148] C. S. Faller, "Statement of Admiral Craig S. Faller Commander, United States Southern Command before the 117th Congress Senate Armed Services Committee March 16, 2021," Senate Armed Service Committee, March 16, 2021 [Online]. Available: https://www.armed-services.senate.gov/imo/media/doc/Faller_03-16-21.pdf

[149] R. L. Katz and A. Dichter, "Decentralizing telecommunications in Latin America," Strategy+Business, April 20, 2021 [Online]. Available: https://www.strategy-business.com/article/12811?gko=4a44c

[150] E. R.Guzmán and B. Jaramillo, "The future of telecommunications service in Latin America: What are the challenges? what are some proposed solutions? prominent telecommunications attorney, Eduardo Guzman, explains." Latin America Legal, blog, August 8, 2018 [Online]. Available: https://www.lexology.com/library/detail.aspx?g=3e2f557a-2b29-4f63-b391-70a48d84d814

[151] M. Cawley, "Drone Use in Latin America: Dangers and Opportunities," InSight Crime, March 27, 2017 [Online]. Available: https://insightcrime.org/news/analysis/drone-use-in-latin-america-dangers-and-opportunities/

[152] A. Michel. *Counter-Drone Systems*. Center for the Study of Drone at Bard College, Annadale-on-Hudson, NY, USA, 2019 [Online]. Available: https://dronecenter.bard.edu/projects/counter-drone-systems-project/counter-drone-systems-2nd-edition/

[153] R. O'Rourke, "Navy lasers, railgun, and gun-launched guided projectile: Background and issues for congress," Congressional Research Service, Washington D.C., USA, R44175, 2020 [Online]. Available: https://crsreports.congress.gov/product/pdf/R/R44175

[154] Marine Corps System Command, "Ground-based air defense." Accessed August 19, 2020 [Online]. Available: https://www.marcorsyscom.marines.mil/PEOs/-PEO-LS/PM-GBAD/

[155] J. R. Hoehn and K. M. Sayler, "Department of Defense counter-unmanned aircraft systems," Congressional Research Service, February 12, 2020 [Online]. Available: https://assets.documentcloud.org/documents/6776412/Department-of-Defense-Counter-Unmanned-Aircraft.pdf

[156] R. Nichols, J. Ryan, H. Mumm, W. Lonstein, C. Carter, and J. Hood, *Counter Unmanned Aircraft Systems Technologies and Operations*. Salina, KS, USa: R. K. Nichols, 2020.

[157] RADA USA, "Multi-Mission Hemispheric Radar (MHR)," RADA Technologies LLC, November 30, 2019 [Online]. Available: https://radausa.com/products/mhr

[158] W. L. Patterson, "Advanced Refractive Effects Prediction System (AREPS)," in *2007 IEEE Radar Conference*, 2007, pp. 891–895.

[159] W. L. Patterson, "Advanced Refractive Effects Prediction System," Defense Technical Information Center, Fort Belvoir, VA, USA, ADA434242, 2001 [Online].

[160] K. Hale, "Expanding the use of time/frequency difference of arrival geolocation in the department of defense technology," Ph.D. dissertation, Pardee RAND Graduate School, Santa Monica, CA, USA, 2012 [Online]. Available: https://www.rand.org/content/dam/rand/pubs/rgs_dissertations/2012/RAND_RGSD308.pdf

[161] 5G Americas, "Advanced Antenna Systems For 5G," 5G Americas Inc, Bellevue, WA, USA, 2019 [Online]. Available: https://www.5gamericas.org/advanced-antenna-systems-for-5g/

[162] GSMA, "5G Spectrum: GSMA Public Policy Position," GSMA Association, November 2018 [Online]. Available: https://www.gsma.com/spectrum/resources/5g-spectrum-positions/

[163] CFRS, "RFeye Node 100-40." Accessed June 15, 2021 [Online]. Available: https://www.crfs.com/product/receivers/rfeye-node-100-40/

[164] Ascent Vision Technologies, "CM262 4-Configuration Gyro-Stabilized System," October 2020 [Online]. Available: https://www.caci.com/sites/default/files/2020-10/cm262_cm262_datasheet_3-2-0_1.pdf

[165] R. Nichols, J. Ryan, H. Mumm, W. Lonstein, and J. H. C. Carter, *Unmanned Aircraft Systems in the Cyber Domain*, 2nd ed. Manhattan, KS, USA: New Prairie Press, 2019.

[166] *Rationalization, Standardization, and Interoperability (RSI) Activities*, "CJCSI 2700.01G," Chairman of the Joint Chiefs of Staff, Washington, DC, USA, 2019.

[167] B. S. Blanchard and W. J. Fabrycky, *Systems Engineering and Analysis*, 5th ed. New York City, NY, USA: Pearson, 2011.

[168] International Union for Conservation of Nature, "UNCLOS." Accessed September 1, 2021 [Online]. Available: https://www.iucn.org/theme/marine-and-polar/our-work/international-ocean-governance/unclos

[169] United States Department of State, "U.S. Bilateral Relations Fact Sheets." Accessed July 7, 2021 [Online]. Available: https://www.state.gov/u-s-bilateral-relations-fact-sheets/

[170] Cornell Law School, "Fourth Amendment," Legal Information Institute, Accessed August 26, 2021 [Online]. Available: https://www.law.cornell.edu/constitution/fourth_amendment

[171] Federal Communications Commission, "Jammer Enforcement," April 30, 2020 [Online]. Available: https://www.fcc.gov/general/jammer-enforcement

[172] Cornell Law School, “Electronic Surveillance,” Legal Information Institute, Accessed January 2, 2021. Available: https://www.law.cornell.edu/wex/electronic_surveillance

[173] Department of Justice, “Electronic Communications Privacy Act of 1986,” Office of Justice Programs, Accessed January 2, 2021 [Online]. Available: https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285

[174] B. Duignan, “USA PATRIOT Act,” Britannica, October 24, 2001 [Online]. Available: https://www.britannica.com/topic/USA-PATRIOT-Act

[175] Office of the Director of National Intelligence, “USA Patriot Act,” January 4, 2021 [Online]. Available: https://www.dni.gov/index.php/who-we-are/organizations/ise/ise-archive/ise-additional-resources/2116-usa-patriot-act

[176] *Operational Law Handbook, 2015*, CJCSI 3121.01B, Chairman of The Joint Chiefs of Staff, Washington, DC, USA, 2005 [Online]. Available: https://www.loc.gov/rr/frd/Military_Law/pdf/OLH_2015_Ch5.pdf

[177] United States Department of State, “U.S. Relations With Djibouti.” Accessed February 9, 2021 [Online]. Available: https://www.state.gov/u-s-relations-with-djibouti/

[178] K. Atherton, “Who’s testing a laser in Djibouti?” C4ISRNET, April 27, 2018 [Online]. Available: https://www.c4isrnet.com/electronic-warfare/2018/04/27/whos-testing-a-laser-in-djibouti/

[179] Oxford Business Group, “Infrastructure development across Djibouti boosts construction,” February 10, 2021 [Online]. Available: https://oxfordbusinessgroup.com/overview/building-blocks-countrywide-infrastructure-development-expands-construction-activities

[180] GeoBasis-DE/BKG, “U.S. military facilities in the Middle East region,” Google My Maps, Accessed February 10, 2021 [Online]. Available: https://www.google.com/maps/d/viewer?mid=12AO9A22Cjkv3pG_tyiIx468a8WpqTaJU

[181] United States Department of State, “U.S. relations with United Arab Emirates.” Accessed February 10, 2021 [Online]. Available: https://www.state.gov/u-s-relations-with-united-arab-emirates/

[182] P. Butterworth-Hayes, “Middle East UAV market "to reach USD3.95 Billion by 2025" - new Report,” Unmanned Airspace, February 19, 2021 [Online]. Available: https://www.unmannedairspace.info/latest-news-and-information/middle-east-uav-market-to-reach-usd3-95-billion-by-2025-new-report/

[183] J. Garamone, "Great power competition adds to challenges in Middle East," DOD News, February 9, 2021 [Online]. Available: https://www.defense.gov/Explore/News/Article/Article/2498114/great-power-competition-adds-to-challenges-in-middle-east/

[184] Today's Military, "Bases around the world - EUCOM." Accessed February 15, 2021 [Online]. Available: https://www.todaysmilitary.com/ways-to-serve/bases-around-world

[185] United States Department of State, "U.S. relations with Spain," January 13, 2020 [Online]. Available: https://www.state.gov/u-s-relations-with-spain/

[186] United States Department of State, "U.S. relations with Greece," August 12, 2021 [Online]. Available: https://www.state.gov/u-s-relations-with-greece/

[187] Today's Military, "Bases around the world - PACOM." Accessed February 17, 2021 [Online]. Available: https://www.todaysmilitary.com/ways-to-serve/bases-around-world

[188] C. T. Lopez, "People, policy, performance readiness mean U.S. prepared to fight," DOD News, October 15, 2020 [Online]. Available: https://www.defense.gov/Explore/News/Article/Article/2383064/people-policy-performance-readiness-mean-us-prepared-to-fight/

[189] United States Department of State, "U.S. relations with Japan," January 21, 2020 [Online]. Available: https://www.state.gov/u-s-relations-with-japan/

[190] Today's Military, "Bases around the world - NORTHCOM." Accessed February 2, 2021 [Online]. Available: https://www.todaysmilitary.com/ways-to-serve/bases-around-world

[191] K. C. Johnson, "History 30.8: Nov. 10 & 12," Word Press, July 2009 [Online]. Available: https://kc-johnson.com/history-30-8-nov-10-12/

[192] Emergency, "US military expanding presence in Colombia: A threat to South America?" Open Source Intelligence on the Emergency of Globalization, November 16, 2009 [Online]. Available: http://mrgnc.blogspot.com/2009/11/us-military-expanding-presence-in.html

[193] R. C. Fernández, "U.S. military presence in Latin America & the Caribbean," Granma, August 15, 2018 [Online]. Available: http://en.granma.cu/mundo/2018-08-15/us-military-presence-in-latin-america-the-caribbean

[194] A. B. Berrocal and J. P. de la Flor, "General map of the Panama Canal," Research Gate, February 21, 2021 [Online]. Available: https://www.researchgate.net/figure/General-map-of-the-Panama-Canal-and-its-enlargement-Below-longitudinal-cut-of-the_fig1_319400464

[195] United States Department of State, "U.S. relations with Panama," June 10, 2019 [Online]. Available: https://www.state.gov/u-s-relations-with-panama/

[196] United States Department of State, "U.S. relations with Colombia," July 19, 2021 [Online]. Available: https://www.state.gov/u-s-relations-with-colombia/

[197] C. T. Lopez, "New spectrum strategy reveals DOD's plan to master airwaves," DOD News November 3, 2020 [Online]. Available: https://www.defense.gov/Explore/News/Article/Article/2404027/new-spectrum-strategy-reveals-dods-plan-to-master-airwaves/

[198] Board on Army Science and Technology, "Counter-Unmanned Aircraft System (CUAS) Capability for Battalion-and-Below Operations," The National Academics Press, Washington, DC, USA, Tech. Rep., 2018 [Online]. Available: https://www.nationalacademies.org/our-work/counter-unmanned-aircraft-system-cuas-capability-for-battalion-and-below-operations

[199] M. Neel, "Afloat Electromagnetic Spectrum Operations Program (AESOP) spectrum management challenges for the 21st century," Naval Surface Warfare Center, Electromagnetic & Sensor Systems Dept., Dahlgren, VA, USA, March 3, 2010 [Online]. Available: https://apps.dtic.mil/sti/pdfs/ADA519589.pdf

[200] Naval Surface Warfare Center Dahlgren Division, "Real Time Spectrum Operations." Accessed June 8, 2021 [Online]. Available: https://www.secnav.navy.mil/innovation/Documents/2017/06/RTSO.pdf

[201] *Joint Electromagnetic Spectrum Operations*, Joint Publication 3-85, Department of Defense, Washington, DC, USA, 2020 [Online]. Available: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_85.pdf

[202] W. L. Patterson, "Advanced Refractive Effects Prediction System (AREPS)," in *2007 IEEE Radar Conference*. Waltham, MA, USA: IEEE, Apr. 2007, pp. 891–895, iSSN: 1097-5659. Available: http://ieeexplore.ieee.org/document/4250431/

[203] United States Naval Research Laboratory, "Interactive scenario builder," Office of Naval Research, March 1, 2021 [Online]. Available: https://builder.nrl.navy.mil/login

[204] *Cyberspace and Electronic Warfare Operations*, Field Manual 3-12, Headquarters, Department of the Army, Washington, DC, USA, 2017 [Online]. Available: https://rdl.train.army.mil/catalog-ws/view/100.ATSC/12BAB5E3-1C00-4DB8-B324-2AA7C6F6F420-1492095745021/fm3_12.pdf

[205] M. Pomerleau, "Army releases new cyber, EW field manual," C4ISRNET, April 21, 2017 [Online]. Available: https://www.c4isrnet.com/c2-comms/2017/04/21/army-releases-new-cyber-ew-field-manual/

[206] J. H. McCall Jr., "Blinded by the light: International law and the legality of anti-optic laser weapons," *Cornell International Law Journal*, vol. 30, no. 1, pp. 1–43, Jan. 1997 [Online]. Available: https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=1394&context=cilj

Initial Distribution List

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California