Winter 2-1-2020

Counter Unmanned Aircraft Systems Technologies and Operations

Randall K. Nichols
Kansas State University - Polytechnic Campus, profrknichols@ksu.edu

Hans C. Mumm
hans.mumm@gmail.com

Wayne D. Lonstein
wayne@vft-solutions.com

Julie J.C.H Ryan
julieryan@julieryan.com

Candice Carter
candicemcarter11@gmail.com

Authors
Randall K. Nichols, Hans C. Mumm, Wayne D. Lonstein, Julie J.C.H Ryan, Candice Carter, and John-Paul Hood

Counter Unmanned Aircraft Systems Technologies and Operations

R. K. NICHOLS, J.J.C.H. RYAN, H.C. MUMM, CANDICE CARTER, W.D. LONSTEIN, AND J.P. HOOD

R. K NICHOLS
SALINA, KANSAS

This book was produced with Pressbooks (https://pressbooks.com) and rendered with Prince.

Contents

Part II. SECTION 2: C-UAS Technologies and Processes

Part III. SECTION 3: Counter C-UAS

Part IV. SECTION 4: Legal and Administrative Issues

Books also by Professor Randall K. Nichols

R.K. Nichols, J.J.C.H. Ryan, H.C. Mumm, C. Carter, W.D. Lonstein, J.P. Hood, (2019) *Unmanned Aircraft Systems in the Cyber Domain Protecting USA's Advanced Air Assets*, 2nd Ed. 26 July 2019, Copyright 2019-2025, All Rights Reserved, Manhattan: New Prairie Press (NPP). ISBN:978-1-944548-15-5. https://newprairiepress.org/ebooks/27

R.K. Nichols, J.J.C.H. Ryan, H.C. Mumm, C. Carter, W.D. Lonstein. (2018) *Unmanned Aircraft Systems* (UAS) *in the Cyber Domain: Protecting* USA's *Advanced Air Assets*, 14 September 2018, Copyright 2018-2025, All Rights Reserved, Manhattan: New Prairie Press (NPP). ISBN:978-1-944548-14-8. https://newprairiepress.org/ebooks/21

R.K. Nichols, & P. Lekkas, (2002) *Wireless Security: Models, Threats, Solutions*. New York: McGraw-Hill. ISBN-13: 978-0071380386

R.K. Nichols, D.J. Ryan, & J.J.C.H. Ryan (2000) *Defending Your Digital Assets Against Hackers, Crackers, Spies and Thieves*. New York: McGraw-Hill. ISBN-13: 978-0072122854

R.K. Nichols, (1998) the ICSA *Guide to Cryptography*. New York: McGraw-Hill. ISBN-13: 978-0079137593

R.K. Nichols, (1996) *Classical Cryptography Course Volume II*. Laguna Hills, California: Aegean Park Press. [Originally distributed under Nom-de Guerre, LANAKI] ISBN-13: 0-89412-264-9

R.K. Nichols, (1995) *Classical Cryptography Course Volume I*. Laguna Hills, California: Aegean Park Press. [Originally distributed under Nom-de Guerre, LANAKI] ISBN-13: 0-89412-263-0

R.K. Nichols, (1991) The *Corporate Aluminum Model*, Texas A & M University- Kingsville Press, Kingsville, TX. MAI:#2902, T378.24 N5184C

Dedications

From: Professor Randall K. Nichols

I dedicate this book to three groups: **All USA serving and retired military personnel,** US Coast Guard and federal and state law enforcement and **to our fallen comrades** for keeping our country safe; to my Angel wife of 36 years, Montine, and children Robin, Kent, Phillip (US Army), Diana (US Army), and Michelle who have lived with a Dragon and survived; and finally, to all my students (over 50 years) who are securing our blessed United States from terrorism.

From: Dr. Hans C. Mumm

I dedicate this work to my students and colleagues and all those innovators; those dreamers that race against time as they create a future that is ever changing and evolving in ways that we cannot even imagine today. Your dedication to the field of autonomous systems will bring about positive change to the world landscape and humankind.

From: Wayne D. Lonstein

I dedicate this work to my wife and best friend Julie, my sons Ethan, Ari and Sam as well as my extended family and co-workers and my co-authors from whom I have learned so much. To all those brave souls who have made the ultimate sacrifice serving this nation, as well as those who have, are or will serve in our armed forces, police, fire and other emergency functions and their families who silently sacrifice. May our work in some way help you perform your duties more effectively and safely and through your service may the world becomes a more peaceful and harmonious place for all.

From: Dr. Julie J. C. H. Ryan

I dedicate this work to my husband Dan and to my students, who have taught me so very, very much.

From: Candice Carter:

I dedicate this work to an exceptional leader, mentor, and master of Bushido; Professor Randall Nichols. His commitment to training dragons to be successful in asymmetric warfare and in life is unprecedented. I am honored to be a lifetime dragoness trained by the master of Nito Ichi Ryu Ni To.

From: CPT John-Paul Hood:

I dedicate this work to my loving and supportive wife Katie, my two daughters Evelyn and Gwendelyn as well as my extended family whom continue to support me through this journey. Thank you for your love, encouragement and presence in my life.

Disclaimers

Information contained in this work has been obtained by the authors from sources believed to be accurate and reliable. However, neither New Prairie Press, R. K. Nichols (publisher), the U.S Army, U.S. Air Force, U.S. Navy, the Department of Defense, Kansas State University, nor any of its authors guarantees the accuracy or completeness of the information published herein and neither any of the above mentioned parties nor its authors shall be responsible for any errors, omissions, or damages arising out of use of this information.

This work examines *inter alia* technical, legal and ethical dimensions of behavior regarding electronic warfare, cybersecurity, directed energy, acoustical countermeasures and Counter Unmanned Aircraft Systems (C-UAS). It is not intended to turn intelligence analysts, counter terrorism, information technology, engineers, forensics investigators, drone operator / pilots or any related professionals into lawyers. Many of the topics discussed will be concerned with the law and legal implications of certain behaviors. Every effort is made to provide accurate and complete information. However, at no time will legal advice be offered. This work is published with the understanding that the authors are supplying information but are not attempting to render professional services. Any reader requiring legal advice, should seek services of a lawyer authorized to practice in the appropriate jurisdiction. All scenarios discussed in this work are hypothetical in nature and not to be taken or construed to be actual occurrences.

The authors, publishers and associated institutions specifically represent that all reasonable steps have been taken to assure all information contained herein is from the public domain and to the greatest extent possible no information of a confidential or classified nature is set forth herein. Additionally, this misuse, re-engineering, retransmission or republication of any content, information or concept contained herein shall not be permitted unless express written permission is granted by the authors, publishers and associated institutions. Additionally, any use of the aforesaid information by any party or intentionally disseminated to any third party or parties for any illegal or improper purpose is expressly forbidden.

Foreword by Joel Anderson OVPR and Development Director

Foreword to Counter Unmanned Aircraft Systems
by
Joel D. Anderson, Colonel USMC (Ret);
Development Director Office of Research
Development/Office of the Vice President for Research Kansas
State University

I am pleased and honored to recommend ***Counter Unmanned Aircraft Systems Technologies and Operations*** for your use as both an educational text and practical reference for the student and practitioner alike.

Within the text you will find a logical and data rich foundation for current, emerging and yet unforeseen applications, considerations/ approaches and practices relevant to the ever-unfolding world of unmanned autonomous systems. The evolution of work found in both the First and Second Editions of **Unmanned Aircraft Systems in the Cyber Domain: Protecting USA's Advanced Air Assets** (Nichols & et.al, 2019) and now this sister textbook covering ***Counter Unmanned Aircraft Systems Technologies and Operations*** (C-UAS) underscores one profound yet enduring theme:

Technology is changing the landscape at a rapid if not exponential rate. The ability to respond and mitigate known and unknown challenges remains an integral factor in our education, understanding and collective ability to remain relevant.

In that context, the authors have striven to provide a valuable understanding of the “as-is” environment while endeavoring to maintain an enduring framework of practices and insight necessary to respond to the unfolding “to-be” environment of the future. I think you will find this sister edition, as with the previous two, of immense value and insight. In it, you will find its organization into sections on:

- CUAS operations as a Concept,
- Technologies and Processes,
- Counter C-UAS, and
- Legal and Administrative Issues to be logically and informatively laid out.

Within the respective sections and nested chapters, the authors lay the foundation for logical and enduring insights. Insights beneficial to our collective ability to learn, assess, understand and respond with relevance–now and into the future. The chapters of the text provide a framework of intuitive understanding of both related technology/material solutions and important/enduring approaches necessary for conceptual planning, response and legal considerations. I am confident that the nature of this text will remain a directional beacon over time providing a holistic, realistic and tangible framework in understanding and addressing current and long-term needs.

My involvement with “drones” began in the mid-1980s when the Pioneer Unmanned Aerial Vehicle (UAV) was delivered to Camp Pendleton, California. Shortly afterwards, my unit was asked to support an operationally relevant environment test of a system called the Pointer UAV, then a small Styrofoam system thrown by hand and carrying a small video sensor. The intent was to assess the utility of a system that could be used for close in reconnaissance; to see what was on the “other side of the hill.” As a technical solution, these “systems” were not necessarily new but the maturity of drone technology then, created an environment where operationally, they would become an integral part of military framework across what is now referred to as multi-domain operations. The emergence of unmanned systems technology created a number of dilemmas for planning, employment, airspace coordination and de-confliction. The widespread use of unmanned systems today are just an expanded manifestation of those considerations only a much wider scale. Then, as now, their introduction was not without controversy, nor challenges with integrating them into a complex technical framework that is non-trivial at the local, regional, national and international levels.

A challenge, then as now, is that technology development just may be the easy thing. It is the nature and impact of emergent often times disruptive technology that presents challenges in response. The response factor coupled with time latency in understanding intended and unintended consequences arguably presents a lagging approach and relatively long lead time in putting context to necessary considerations and approaches. I believe that the authors of this text get in front of the “boom” of technology by supporting a comprehensive and integrated approach to factors and considerations far too often ignored.

As we look forward, Pillar II of the current National Security Strategy (NSS) discusses the importance of leadership in “Research, Technology, Invention and Innovation.” Undoubtedly, UAS will remain part of that innovation ecosystem well into the future. Globally, we are witnessing rapid technical change and use of these systems in a myriad of context that also influence an increasingly complex top to bottom security environment. Nested within the NSS our National Defense Strategy (NDS) calls for agility in responding to both the technical and security challenges in our future by integrating and adapting at “The Speed of Relevance.”

This context is important on three levels.

1. First. Platform development and use has become pervasive as a major economic technology powerhouse globally. Unmanned aerial systems are in fact becoming ubiquitous.

2. Secondly. Because technology has matured to a point where unmanned systems have become a fully integrated reality of commercial use and applications within the National Air Space, they must be addressed holistically.

3. Finally. We are experiencing introduction of newer technologies daily. Their usage will continue to challenge our understanding of the materials and manufacturing space and our collective ability to respond to change. Counter UAS will be a critical enabler as we move forward.

On the latter point, this sister edition provides exceptional insight and practical understanding into a technology domain that is experiencing development at break-neck speed, disruptive use across an expansive application domain, and yes, even unanticipated implications in their development, usage, employment and ramifications therein.

Today, the challenges, gaps and opportunities of assessing platforms, sensors, communications, information technology, cyber and use cases for surveillance and reconnaissance require a foundation for legal and ethical insight, knowledge and best practices.

The value of this sister edition is that it provides a long term and enduring foundation and fundamental framework of insights, best practices and considerations for "**Counter Unmanned Aircraft Systems Technologies and Operations"** that can and will serve the reader well.

Joel D. Anderson
Colonel USMC (Ret)
Development Director
Office of Research Development (ORD)
Office of the Vice President for Research
Kansas State University

References

Nichols, R., & et.al. (2019). *Unmanned Aircraft Systems in the Cyber Domain: Protecting* USA's *Advanced Air Assets* . Manhattan, KS: New Prairie Press #27.

Preface

As the quarter-century mark in the 21st Century nears, new aviation-related equipment has come to the forefront, both to help us and to haunt us. (Coutu, 2020) This is particularly the case with unmanned aerial vehicles (UAVs).[1] These vehicles have grown in popularity and accessible to everyone. Of different shapes and sizes, they are widely available for purchase at relatively low prices. They have moved from the backyard recreation status to important tools for the military, intelligence agencies, and corporate organizations. New practical applications such as military equipment and weaponry are announced on a regular basis – globally. (Coutu, 2020) Every country seems to be announcing steps forward in this burgeoning field.

In our successful 2nd edition of *Unmanned Aircraft Systems in the Cyber Domain: Protecting USA's Advanced Air Assets* (Nichols, et al., 2019), the authors addressed three factors influencing UAS phenomena. First, unmanned aircraft technology has seen an economic explosion in production, sales, testing, specialized designs, and friendly / hostile usages of deployed UAS / UAVs / Drones. There is a huge global growing market and entrepreneurs know it. Small UAS companies have been reproducing like rabbits. Only the FAA has been a stumbling block trying to balance UAS safe integration into the National Airspace against hundreds of thousands of new recreational and commercial operators testing their meddle in the skies. FAA's best efforts surround its decision to register UAS and provide a process for Part 107 Certification. (Nichols, et al., 2019) Certification[2] brings sanity and education into a chaotic public market in the US.

Second, ***hostile use of UAS is on the forefront of DoD defense and offensive planners***. They are especially concerned with SWARM behavior. Movies like "*Angel has Fallen*," where drones in a SWARM use facial recognition technology to kill USSS agents protecting

POTUS, have built the lore of UAS and brought the problem forefront to DHS. The author presented at several international C-UAS conferences which were attended by commercial, educational and military organizations for the purpose of hardening USA air assets against hostile drone activities. These were serious conversations and workshops – many of them – behind closed doors and interacting with military brass. (Nichols, et al., 2019)

Third, UAS technology was exploding. Everyday our team reads / discusses new UAS developments in navigation, weapons, surveillance, data transfer, fuel cells, stealth, weight distribution, tactics, GPS / GNSS elements, SCADA protections, privacy invasions, terrorist uses, specialized software, and security protocols. (Nichols, et al., 2019) Our team has followed / tracked joint ventures between military and corporate entities and specialized labs to build UAS countermeasures. The number of professional C-UAS conferences around the world are significant. This is a growing field like INFOSEC was a predictable offshoot to cybercrime.

As authors, we felt compelled to address at least the edge of some of the new C-UAS developments. It was clear that we would be lucky if we could cover a few of – the more interesting and priority technology updates – all in the UNCLASSIFIED and OPEN sphere.

Counter Unmanned Aircraft Systems: Technologies and Operations is the companion textbook to our 2nd edition. The civilian market is interesting and entrepreneurial, but the military and intelligence markets are of concern because the US does NOT lead the pack in C-UAS technologies. China does. China continues to execute its UAS proliferation along the New Silk Road Sea / Land routes (NSRL). It has maintained a 7% growth in military spending each year to support its buildup. (Nichols, et al., 2019) [Chapter 21]. They continue to innovate and have recently improved a solution for UAS flight endurance issues with the development of advanced hydrogen fuel cell. (Nichols, et al., 2019) Reed and Trubetskoy presented a terrifying map of countries in the Middle East with armed drones and their manufacturing origin. Guess who? China. (A.B. Tabriski & Justin, 2018, December)

Our C-UAS textbook has as its primary mission to educate and train resources who will enter the UAS / C-UAS field and trust it will act as a call to arms for military and DHS planners.

Step up the U.S. defense game (spending) or teach your children to learn Chinese.[3] If you have been asleep at the wheel for a while, you might want to look into *WeChat*, a super social media app designed by Tencent, a Chinese tech company. You can do everything on your phone. Everything. It has 850 million users. The Chinese government uses it to keep an eye on all its citizens, censor public posts , chats and banned words, alert police to potential riot conditions or just unacceptable group gatherings. It is used to create a "social credit score" to impose restrictions on those citizens that have breached some "trust." (Deutsche Welle, 2017) *Trust* is defined by the Chinese government. What's the connection? China uses surveillance drones to augment this people control strategy for not only its own citizens but those they have military or economic agreements with along the NSRL from the South China Seas, Asia, Europe, and Africa [the newest testing playground for UAS / C-UAS technologies for several nations.] (Nichols, et al., 2019)

Here is the condensed outline of topics in our sister textbook:

SECTION 1: Counter-UAS (C-UAS) Operations as a Concept

Chapter 1: The Role of Information Technologies (Automated decisions, Artificial Intelligence (Weak and Strong), Communications, Networking, Remote Sensing)]

Chapter 2: Understanding C-UAS Purpose and Process

Chapter 3: Developing a C-UAS Strategy, Goals, Options, Target Analysis, Process Selection, Operational Metrics, Approaches to Countering UAS Activities (First Principles)

Chapter 4: Planning for Resiliency and Robustness Expecting pushback, When Secrecy is Needed, How to Shield Operations

SECTION 2: C-UAS Technologies and Processes

Chapter 5: Surveillance and Reconnaissance

Chapter 6: C-UAS Evolving Methods of Interdiction

Chapter 7: UAS Area / Airspace Denial

Chapter 8: Emerging Interdiction Technologies

Chapter 9: Non- Kinetic: Military Avionics, EW, CW, DE, SCADA Defenses

SECTION 3: Counter C-UAS

Chapter 10:When the Other Side Fights Back – Cyberwarfare, Direct Energy Weapons, Acoustics, Integrating C-UAS into Planning

Chapter 11: Thinking Like the Enemy: Seams in the Zone

SECTION 4: Legal and Administrative Issues

Chapter 12: C-UAS Regulation, Legislation & Litigation from A Global Perspective

SECTION 1 Enumerates the concepts of Counter Unmanned Aircraft Systems. It is concerned with the role of information technology, the Strategy, Goals, Options, Target Analysis, Process Selection, Operational Metrics, and Approaches to Countering UAS Activities.

SECTION 2 looks at the C-UAS technologies and processes. To wit: Surveillance and Reconnaissance; Evolving Methods of Interdiction; UAS Area / Airspace Denial; Emerging Interdiction Technologies; and Non- Kinetic: Military Avionics, EW, CW, DE, SCADA Defenses.

SECTION 3 broaches the sensitive subject of Counter C-UAS and current research into Cyberwarfare, Direct Energy Weapons, Acoustic / IFF defenses; Integrating C-UAS into Planning and Thinking Like the Enemy.

SECTION 4 puts our work into a global legal framework: C-UAS Regulation, Legislation & Litigations.

We trust our newest book will enrich our students' and reader's understanding of the purview of this wonderful technology we call C-UAS.

Best

Randall K Nichols
Professor of Practice
Director, Unmanned Aircraft Systems –
Cybersecurity Certificate Program
Managing Editor / Author
Kansas State University Polytechnic Campus &
Professor Emeritus – Cybersecurity, Utica College

LinkedIn Profile:
http://linkedin.com/in/randall-nichols-dtm-2222a691
Illi nunquam cedunt.
"We Never Yield"

References

A.B. Tabriski & Justin, B. (2018, December). *Armed Drones in the Middle East Proliferation and Norms in the Region.* Westminister, UK: Royal United Services Institute.

Coutu, P. (2020). *Global Megatrends and Aviation – The Path to Future-Wise Organizations.* Quebec: ASI Institute.

Deutsche Welle. (2017, March 31). *Hello, Big Brother: How China controls its citizens through social media.* Retrieved from amp.dw.com: amp.dw.com /science

FAA. (2020, January 29). *FAA Aerospace Forecast FY 2018-2038.* Retrieved from faa.gov: www.faa.gov/data_research/aviation/aerospace_forecasts/media/FY2018-2038_faa_aerospace_forecast.pdf

Nichols, R. K. (2008). *Cyber Counterintelligence & Sensitive Compartmented Information Facility (SCIF) Needs – Talking Points;* Utica College, Chair Cybersecurity. Utica New York: Private Memo to R. Bruce McBride. Retrieved September 5, 2008

Nichols, R., Ryan, J., Mumm, H., Lonstein, W., Carter, C., & & Hood,

J. (2019). *Unmanned Aircraft Systems in the Cyber Domain: Protecting* USA's *Advanced Air Assets, 2nd Edition.* Manhattan, KS: New Prairie Press.

US-CERT. (2015, August 27). *Computer Forensics.* Retrieved from US-CERT: https://www.us-cert.gov/sites/default/files/publications/forensics.pdf

[1] Also known as "Drones" and in our textbook, the more general term is UAS, for unmanned aircraft system. The term C-UAS refers to the counter -UAS, for countermeasures applied to protect against maleficent use.

[2] By late 2018, the FAA had issued over 73,000 Remote Pilot Certifications. (FAA, 2020) This shows how attractive and useful in the civilian sector this type of vehicle is and why it is so popular. Practical civilian applications include package delivery, law enforcement, surveying, electrical line repair, crop dusting, home / business security, construction supervision, mountain rescue, surveillance, and many more. (Coutu, 2020)

[3] Amazon sells a fine beginner's course in Mandarin Chinese. Entitled: *Living Language Mandarin Chinese, Complete Edition: Beginner through advanced course, including* 3 *coursebooks,* 9 *audio* CDs, *Chinese character guide, and free online learning* Audio CD *– Unabridged*, October 18, 2011 See: https://www.amazon.com/Living-Language-Mandarin-Chinese-Complete/dp/0307478610/ref=sr_1_5?crid=3ATY71J5226P1&keywords=mandarin+chinese+for+beginners&qid=1580320321&sprefix=Mandarin+%2Caps%2C176&sr=8-5

Acknowledgements

Books such as this are the products of contributions by many people, not just the musings of the authors. ***Counter Unmanned Aircraft Systems Technologies and Operations*** has benefited from the review of numerous experts in the field, who gave generously of their time and expertise. In addition to named subject matter experts, this book was reviewed by sources in the two federal agencies who must remain anonymous and by export /procedural committee's at KSU. Their contributions were especially helpful in not releasing protected information, classified or deemed exportable categories. We will name only a few and clearly miss some special friends whose contributions were noteworthy. For this we apologize in advance and beg your forgiveness.

There are many people we would like to shout out a special thank you for your guidance, continued support and experience from Kansas State University / Kansas State University Polytechnic (KSU / KSUP): Dr. Richard Myers, President KSU; Dr. Kurt C. Barnhart, Associate Dean of Research and Executive Director of the UAS Research Laboratory KSUP; Dr. Alysia Starkey, Dean & CEO of KSUP; Dr. Terri Gaeddert, Director of Academics, School of Integrated Studies (SIS) KSUP; Dr. Donald V. Bergen, prior Director of Graduate Studies KSUP; Fred Guzek, Professor and current Director of Graduate Studies KSUP; Dr. Kurt Caraway, Executive Director UAS, Dr. Michael Most. (Retired) UAS Department Chair, Dr. Mark J. Jackson, Professor, SIS KSUP; Dr. Saeed Khan, Professor, SIS KSUP; Dr. Tom Haritos, ARG, Associate Director of Research and UAS Research Program Manager; Dr. Siny Joseph, ARG, and Associate Professor of Economics; Dr. M.J. Pritchard, Sr. Davis Scientist; Professor Raju Dandu; Dr. Katherine Jones, KSUP Research and Library; Rachel Miles, Assistant Professor, Hale Library KSU; Lisa Shappee, Director, KSUP Library; Beth Drescher, Grant Specialist KSUP; Charlene Simser, Professor and Coordinator of Electronic

Publishing at New Prairie Press and Pressbooks,[my mentor in the publishing gig] Chad Bailey, Instructor SIS KSUP, Professor Troy Harding; Aris Theocharis, our terrific editor; and especially Joel Anderson, KSU OVPR and Research Director. Joel wrote our foreword for this book and we stand proud and honored.

We had some wonderful outside SMEs to bounce ideas off and get our heads straight. They include Dr. Donald Rebovich, Professor Emeritus and SME in Fraud and Identity Theft; Professor of Practice and Cybersecurity Director, Joe Giordano, Utica College; Professor Harold B. Massey, Executive Director of UAS Drone Port and UAS Pilot and Dr Amit K Maitra, Chairman and Founder of Borders and Beyond, Inc; and Joel Coulter, President, Mobile Sciences Consortium, LLC.

Next comes our writing team: Dr Julie J. C. H. Ryan, CEO, Wyndrose Technical Group, is hands down the best subject matter expert (SME) in the Information Security field. Dr. Hans C. Mumm is an expert in leadership and UAS weapons – a lethal combination. Dr. Wayne C. Lonstein, Esq., a previous Dragon (Nichols' student) has gained recognition (licenses and certifications) in both law and cybersecurity as well as heads up his own legal firm. Professor Candice C. Carter, a Dragoness who is the creator of a cybersecurity program at Wilmington University and travels globally closing specialized cybersecurity breaches in major corporations. Capt. John Paul Hood, US Army, (our military adviser and previous Dragon) joined us to help us understand the intricacies of military C-UAS (non-classified) applications. Professor Nichols is managing editor / author / co-author of eight prior books and developer of six Masters and Certificate programs in Cybersecurity at Utica College and KSUP with five decades of experience.

Finally, Montine Nichols deserves a commendation for her help on the final drafts and copy edit work for our book (and living with a real Dragon). Several KSUP UAS pilot – students helped with the "student view," and made valid suggestions for improvement, Randall Mai, Research Technologist for KSU; Jeremy Shay, RET USAF, Fabrication Production Manager, Spirit AeroSystems; Vincent

Salerno, Senior Airman in Kansas Air National Guard, John Boesen, (our handwriting expert); Diana K. Nichols, UAS Pilot; Josh Jacobs, Jorge Silva, Sr. UAS Safety Engineer, and Jordan McDonald. Special thanks go out to Kira C. Miller who professionally developed (more like "nailed") our cover art.

The team especially thanks Assistant Professor Ryan W. Otto, Scholarly Communication Librarian, for his super help with the NPP final efforts!

Randall K Nichols
Professor of Practice
Director, Unmanned Aircraft Systems (UAS) – Cybersecurity Graduate Certificate Program
Managing Editor / Author
Kansas State University Polytechnic Campus &
Professor Emeritus – Cybersecurity, Utica College

List of Contributors

Professor Randall K. Nichols, (Managing Editor* / Author)

Randall K. Nichols is Professor of Practice in Unmanned Aircraft Systems (UAS) – Cybersecurity at Kansas State University Polytechnic (KSUP) in Salina, Kansas. Nichols serves as Director, graduate UAS- Cybersecurity Certificate program at KSUP. Nichols is internationally respected, with 50 years of experience in leadership roles in cryptography, counterintelligence, INFOSEC, and sensitive computer applications. Throughout his career, Nichols has published nine best-selling textbooks. Nichols has provided counsel to the United States government and is certified as a federal subject matter expert (SME) in both cryptography and computer forensics. His most recent work involves creating master and certificate graduate – level programs for KSU and Utica College. To wit:

- Author/ Developer: MPT/ MS / Certificate in Unmanned Aerial Systems (UAS) -Cybersecurity
- Author/ Developer: BS Unmanned Aerial Systems (UAS) -Cybersecurity
- Retired Chair and Program Developer: MS – Cybersecurity –Intelligence and Forensics
- Retired Chair and Program Director: BS – Cybersecurity and Information Assurance

- Co-Author / Developer: MPS – Risk Assessment and Cybersecurity Policy
- Author / Developer: MS Cyber Surveillance and Warfare

Previously, Nichols was COO of INFOSEC Technologies, LLC, a consulting firm specializing in Counter-Terrorism, Counter-Espionage, and Information Security Countermeasures to support its 1700 commercial, educational and U.S. government clients.

Nichols served as CEO of COMSEC Solutions, a Cryptographic / Anti-virus / Biometrics Countermeasures Company, which was acquired by a public company in 2000. He served as Vice President of Cryptography and Director of Research of the acquiring firm.

Nichols served as Technology Director of Cryptography and Biometrics for the International Computer Security Association (ICSA), President, and Vice President of the American Cryptogram Association (ACA).

Areas of Expertise / Research Interests

- Counterterrorism / Counter- Intelligence /Counterespionage / Computer Security
- Countermeasures Asymmetric Warfare and Attack / Defense Scenarios against National Critical Infrastructure
- Computer Forensics and Cryptography SME & Federal Expert Witness (Federal Criminal Cases: Treason / Espionage)
- Risk Assessment / Threat Analysis / Vulnerabilities Analysis / Countermeasures
- Cybersecurity / Surveillance Technologies: Aerial, Infrared, Visual, Ultraviolet, Radio, Radar & Sonar
- SCADA – Advanced Cyber-weapons Creation / Deployment / Deployment / Defense
- UAS- Integrating Unmanned Aircraft Systems into National Airspace System
- Designing Acoustic Countermeasures against hostile -actor UAS SWARMS & developing dual purpose IFF sound libraries.

Contact Prof. Randall K Nichols at 717-329-9836 or profrknichols@ksu.edu.

*Direct all inquiries about this book to Prof. Randall K. Nichols at profrknichols@ksu.edu

Dr. Hans C. Mumm (Co-Author)

Dr. Hans C. Mumm holds a Doctor of Management with a concentration in Homeland Security from Colorado Technical University (CTU) and an MS in Strategic Intelligence from American Military University (AMU). He gained notoriety during Operation Iraqi Freedom as the officer in charge of the "Iraqi Regime Playing Cards; CENTCOM'S Top 55 Most Wanted List" which was touted by the Defense Intelligence Agency (DIA) as one the most successful Information Operations (IO) in the history of Defense Intelligence Agency (DIA). Dr. Mumm is the former Division Chief for Cyber Security at the Office of The Director of National Intelligence (ODNI) programming and executing a budget of over $140 M. Dr. Mumm has earned twenty-three personal military ribbons/medals including six military unit medals/citations, and two Directors Awards, from the DIA. In 2016 he was awarded the People of Distinction Humanitarian Award as well as being granted a US Patent and Trademark for How to Harmonize the Speed of Innovation and Change with the Human Spirit's Need for Leadership. In 2005, Dr. Mumm was recognized as one of the "Ten Outstanding Young Americans," and in 2003 he was awarded the National Defense PAC "American Patriot Ingenuity Award" for his service during "Operation Iraqi Freedom."

He co-authored an international best-selling book titled "Lightning Growth" which is a follow up to his best-selling book in 2015 titled “Applying Complexity Leadership Theory to Drone Airspace Integration.”

He is a published researcher in both the scientific and social science arenas and has won grants and contracts to further test and evaluate his original research. He has notable experience in research and systems engineering which includes contracts for UAV research and the creation of an advanced multiple fuel system which operated the world’s first and only helicopter that can fly on five separate fuels without engine modifications. His research extends into emerging and disruptive technology for offensive and defensive missions supporting US and coalition operations. His UAV and robotics expertise has focused on determining the specific uses, exceptions, and allowances for robotics operations; including studying the unintended consequences, future use, and misuse of such technologies. Dr. Mumm’s presentations and publications support his research into autonomous systems in the virtual and physical worlds. Additionally, he serves as an adjunct professor at California University of Pennsylvania (CALU) instructing Homeland Security courses in the Criminal Justice Department.

Contact Information: Dr. Hans C. Mumm, 703-303-1752, hans@hansmumm.com. www.HansMumm.com

Wayne D. Lonstein, Esq. CISSP (Co-Author)

Wayne Lonstein holds a Bachelor of Arts Degree in Political Science from Wilkes University, a Bachelor of Science Degree in Cyber Forensics and Information Security from Syracuse University – Utica Collage, A Master of Science Degree in Homeland Security with a concentration in Information Security from The Pennsylvania

State University and a Juris Doctor Degree from Pace University School of Law. Additionally he holds a CISSP Certification from The Pennsylvania State University. He is a member of the state bars of New York, New Jersey, Massachusetts an Pennsylvania as well as being admitted to over 30 United States District Court Bars, The Court of Veterans Appeals, United States Tax Court and the bar of the United States Court of Appeals of the 2nd, 3rd and 5th Circuits.

In addition Mr. Lonstein has practiced law nationally since 1987 in the area of technology, intellectual property, sports and entertainment and has litigated over 2000 cases. He is also a member of the New York State Magistrates Association and has served as a Magistrate Judge in the Town of Wawarsing, New York since 1989.

He a member of Signal law PC, the Co- Founder and CEO VFT Solutions is a member of the Forbes Technology Council and has authored numerous articles including: "Why Industry and Government Leaders Need to Realize Vulnerabilities of the Cloud"

Published on June 16, 2017 on LinkedIn; 'Identifying The Lone Wolf Using Technology," on LinkedIn, Published on July 3, 2015; "Are Social Media Companies Using ToS And Safe Harbor To Profit From Infringement, Crime And Terror?," Forbes.com, April 28, 2017; "Weaponizing Social Media: New Technology Brings New Threat," Forbes.com, July 7, 2017; 'Pay No Attention To That Man Behind The Curtain': Technology vs. Transparency," Forbes.com, October 17, 2017; and "Drone Technology: The Good, The Bad And The Horrible," Forbes.com, January 10, 2018.

Julie J.C.H. Ryan, D.Sc. (Co-Author)

Julie J.C.H. Ryan, D.Sc., is the CEO of Wyndrose Technical Group, having retired from academia in 2017. Her last position in academia was Professor of Cybersecurity and Information Assurance from the U.S. National Defense University. Prior to that, she was tenured faculty at the George Washington University and a visiting scholar at the National Institute for Standards and Technology (NIST).

Dr. Ryan came to academia from a career in industry that began when she completed military service. Upon graduating from the U.S. Air Force Academy, Dr. Ryan served as a Signals Intelligence Officer in the Air Force, and then as a Military Intelligence Officer with the Defense Intelligence Agency. Upon leaving government service, she worked in a variety of positions, including systems engineer, consultant, and senior staff scientist with companies including Sterling Software, Booz Allen & Hamilton, Welkin Associates, and TRW/ESL supporting a variety of projects and clients.

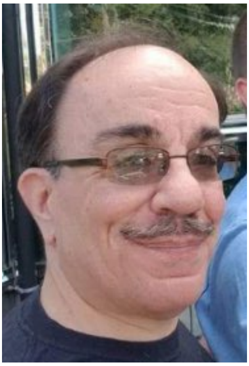
She is the author /co-author of several books, including *Defending Your Digital Assets Against Hackers, Crackers, Spies, and Thieves* (McGraw Hill 2000), and a Fellow of the American Academy of Forensic Sciences (AAFS). At Wyndrose Technical Group, she focuses on futures forecasting and strategic planning with an eye on technology surprise and disruption.

Candice Carter (Co-Author)

Ms. Candice Carter is a cybersecurity expert with over 15 years of hands-on experience in the areas of counter-terrorism, counterintelligence and criminal cyber investigations. She conducts Classified/Unclassified briefings in the areas of Terrorism Cyber

Capabilities using Social Media and Counter-terrorism for the Intelligence Community (IC). Ms. Carter conducts research and constructs Asymmetric Warfare and Attack / Defense Scenarios against National Critical Infrastructure. She is the Team Lead and for NASA Aeronautics Research Institute for *Transformative Vertical Flight* (TVF) *Commercial Intra-City On-Demand* VTOL group. Ms. Carter is an invited speaker for key organizations including BSides London and (ISC)2 Security Congress. She is an Assistant Professor/ Chair MSc Cybersecurity program at the Wilmington University. Ms. Carter holds a MSc Cybersecurity Forensics and Intelligence from Utica College, Utica , NY and a PMT Cybersecurity UAS (expected 2019) from Kansas State University.

Aris Theocharis (Co-Editor)



Aris has 30+ years of IT experience and earned a BS in Cybersecurity from Utica College, Utica, NY while working full time. He has provided editing skills for Professor Nichols for 10 years now. His approach is all encompassing, as opposed to strict grammar rules. Reading ease, topic flow, clarity, and being succinct are the focus.

Kurt Barnhart, Ph.D. (Foreword To 1st Edition)

Dr. Barnhart is Professor and currently the Associate Dean of Research at Kansas State University Salina. In addition, he established and serves as the executive director of the Applied Aviation Research Center. He oversees the Unmanned Aerial Systems program office. Dr. Barnhart previously served as the Head of the Aviation Department at Kansas State University.

Dr. Barnhart is a member of the graduate faculty at K-State. He is eminently qualified with: 1) a commercial pilot certificate with instrument, multi-engine, seaplane and glider ratings; 2) a certified flight instructor with instrument and multi-engine ratings; 3) an airframe and power plant certificate with inspection authorization.

Dr Barnhart's educational pedigree is outstanding: an A.S. in Aviation Maintenance Technology from Vincennes University, a B.S. in aviation administration from Purdue University, an MBAA from Embry-Riddle Aeronautical University, and a Ph.D. in educational administration from Indiana State University.

Dr. Barnhart's Research agenda is focused in aviation psychology and Human Factors as well as the integration of Unmanned Aircraft Systems into the National Airspace System. His industry experience includes work as a R&D inspector with Rolls Royce Engine Company where he worked on the RQ-4 Unmanned Reconnaissance Aircraft development program, as well as serving as an aircraft systems instructor for American Trans-Air airlines. Formerly, Dr. Barnhart was an Associate Professor and Acting Department Chair of the Aerospace Technology at Indiana State University where he was responsible for teaching flight and upper division administrative classes. Courses taught include Aviation Risk Analysis, Citation II

Ground School, King Air 200 Flight, Air Navigation, Air Transportation, Instrument Ground School and many others.

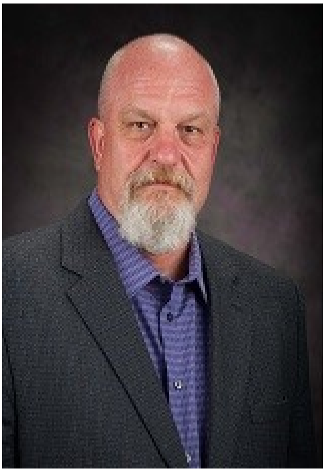
CPT John-Paul Hood USA (Co-Author)

CPT John-Paul Hood is a researcher focused on the development of future counter unmanned aircraft technologies, theories and best practices for both government and civilian applications. CPT Hood has commanded in the US Army Field Artillery with a background specializing in the coordination and delivery of conventional / smart munitions as well as achieving desired battlefield effects through the integration of lethal and non-lethal assets. CPT Hood holds a BS in Geospatial Information Systems from the United States Military Academy, West Point NY and a Professional Masters in Technology UAS (expected 2019) from Kansas State University.

Dr. Alysia Starkey (CEO & Dean Kansas State University Polytechnic; 2nd Ed. Foreword)

Dr. Starkey is a Professor and currently serves as the CEO and Dean for the Kansas State University Polytechnic Campus. As Dean, she oversees the College of Technology and Aviation academic programs and campus research centers. Dr. Starkey holds an A.A.

in Social Work from Colby Community College, a B.S. in Psychology from Fort Hays State University, a M.L.S. from University of North Texas, and a Ph.D. in Curriculum and Instruction from Kansas State University. Joining Kansas State Polytechnic in June 2002 as a technical services/automation coordinator and assistant professor, Starkey was promoted to library director and associate professor in 2007, and to assistant dean of continuous improvement and distance education in 2010. She was named associate dean of academics and promoted to full professor in 2014. She gained the additional duties of interim CEO and Dean in June 2018 and continues in that capacity today.



Joel D. Anderson Colonel USMC (Ret), OVPR and Research Director (C-UAS Foreword)

Mr. Anderson has more than 30 years experience in military, industry and academia. He currently serves as Development Director for Kansas State University within the Office of Research Development (ORD). Prior to joining KSU, he served as a Technical Director, Innovation Evangelist, and Senior Subject Matter Expert for ManTech International in support of HQMC Intelligence Department and its Tactical Exploitation of National Capabilities (TENCAP) office and Technology and Innovation Directorate; and as the Director for Mosaic ATM, Inc.'s Autonomous Systems Group. Between 1984-2010, he served in the United States Marine Corps where he rose in rank from Private to Colonel. During his career, he served as an (0231) intelligence analyst while enlisted where he was meritoriously promoted to Corporal, and as an officer he held military occupational designations as an (0202) Marine Air Ground Task Force Intelligence Officer, (0240) Imagery Officer, (0540) Space Operations Officer, and (8058) Acquisition Professional earning DAIWIA Level III Certification as Program Manager and member of the acquisition community while PM-Marine Intelligence Systems for the Marine Corps Systems Command. He held command positions as a Surveillance and Target Acquisition Platoon Commander, Commander of the 2nd Force Imagery Interpretation Unit (FIIU) and was Commanding Officer Company E. Marine Security Guard Battalion (Department of State). He served as the Marine Corps Senior Departmental Requirements Officer (DRO) and as the Imagery and Collections Section Head while serving with the Marine Corps Intelligence Activity; as the Branch Head for HQMC Intelligence Departments Imagery and Geo-spatial Plans and Policy Branch, and concluded his career as a Strategic Intelligence Planner for the Office of the Under Secretary of Defense for Intelligence (OUSD-I) and as the Chief of Staff for Secretary Gates Intelligence, Surveillance and Reconnaissance Task Force (ISRTF). He has served at every operational level of the Marine Corps from Battalion, Regiment, Division, Wing, MEU and MEF; within the Marine Corps supporting establishment, HQMC and on the OUSD-I staff. Mr. Anderson has spent a career supporting efforts to address the complexities of the intelligence community and inter-agency information management, decision making, talent acquisition, educational and operational environments.

His personal awards include the Defense Superior Service Medal;

Bronze Star; Meritorious Service Medal with four gold stars in lieu of 5th award; Navy and Marine Corps Commendation Medal; Navy and Marine Corps Achievement Medal; Joint Meritorious Unit Citation; Meritorious Unit Citation; Navy Unit Citation; Marine Corps Expeditionary Medal; National Defense Medal with one device in lieu of second award; Armed Forces Expeditionary Medal; Southwest Asia Service Medal with three stars in lieu of additional awards; Global War on Terrorism Service Medal; Sea Service Deployment Ribbon with three stars in lieu of additional awards; Overseas Deployment Ribbon with one device; Marine Security Guard Ribbon; Kuwaiti Liberation Medal (Saudi Arabia); Kuwaiti Liberation Medal (Kuwait).

Abbreviations and Acronyms

Abbreviations: Acronyms [Rev 66A]

The following terms are common to the UAS industry, general literature or conferences on UAS/UAV/Drone systems.

A2 / AD	Anti-access / Area Denial
A /Aref	Amplitudes of source and reference points, see Eq-20-6,7
AA	Anti-aircraft / Adaptive Antennas
AAA	Anti-aircraft artillery
AAIB	Air Accidents Investigation Board
AAM	Air-to-air missile
AAV	Autonomous air vehicle
ABI	Aviation Block Infrastructure
A/C	Aircraft
ACAS	Airborne collision avoidance system / Assistant Chief of the Air Staff
ACL	Agent communication language / Autonomous control levels
ACOUSTIC	Detects drones by recognizing unique sounds produced by their motors
ACRP	Airport Cooperative Research Project
ACS	Airbome (defense) control station (system)
ACTD	Advanced Concept Technology Demonstration
AD	Air Defense / Ansar Dine terrorist group
A/D	Attack / Defense Scenario Analysis
ADAC	Automated Dynamic Airspace Controller
ADC	Air data computer
ADF	Automatic direction finder/finding
ADMS	Air defense missile (radar) system
ADS	Air Defense System (USA)

ADS-B	Automatic Dependent Surveillance – Broadcast systems
ADT	Air Data Terminal
AESA	Active electronically scanned array
AEW	Airbome early warning
AF	Adaptive Filtering
AFCS	Automatic flight control system
AFRICOM	US Africa Command
AGL	Above ground level
AGM	Air- to- surface missile
AGARD	Advisory Group for Aerospace Research and Development (NATO)
AGM-65	Maverick (USA) is an air-to-surface missile (AGM) designed for close air support. It is the most widely produced precision-guided missile in the Western world, and is effective against a wide range of tactical targets, including armor, air defenses, ships, ground transportation and fuel storage facilities.
AHA	Autopilot Hardware Attack
AHD	Analog high definition
AHRS	Attitude and heading reference system
AI	Artificial intelligence
AIAA	American Institute of Aeronautics and Aerospace
AIC	Aeronautical Information Circular
AIP	Aeronautical Information Publication
AIS	Automated Identification System for Collision Avoidance
AJ	Anti-Jam
ALB	Air Land Battle
ALERT	Advanced Low-observable Embedded Reconnaissance Targeting system.
AM	Amplitude Modulation / al-Mourabitoun terrorist group
AMB	Agile Multi-Beam
AMRAAM	Advanced Medium-Range Air-to-Air Missile
ANSP	Air Navigation Service Provider

ANO	Air Navigation Order (UK)
AO	Area of Operations
AoA	Angle of Attack
APEC	Asia Pacific Economic Cooperation
APG	Asia-Pacific Gateway
APKWS	Advanced precision kill weapon system
AQ	Al-Qaida Terrorist Group – “the Base”
AOA	Aircraft operating authority
AQIM	al-Qaeda in the Islamic Maghreb
Ar	Receive antenna effective area, m2
AR	Aspect ratio
AR drone	AR stands for “Augmented Reality” in AR *drone*. AR *Drone* can perform tasks like object recognition and following, gesture following.
ARM	Anti-Radiation Munitions
ARS	Airborne Remote Sensing
ARW	Anti-radiation weapons
AS	Airborne Sensing Systems
ASB	Advisory Service Bulletin / Air Sea Battle
ASEA	Active electronically scanned arrays
ASEAN	Association of Southeastern Asian Nations
ASL	Airborne Systems Laboratory
ASMS	Automated Separation Management System
ASTM	American Society of Testing and Materials (ASTM)
ASTER	Agency for Science, Technology and Research
ASuW	Anti-surface unit warfare
ASW	Anti-submarine warfare
AT	Aerial target
ATC	Air Traffic Control
ATHENA	Lockheed Martin Advanced Test High Energy Asset
ATM	Air Traffic Management
ATR	Automatic Target Recognition
ATS	Air Traffic Service
AUDS	Anti-UAV Defense System
AUV	Autonomous Underwater Vehicle

Avionics Aviation electronics in manned or unmanned aircraft

AUVSI Association for Unmanned Vehicle Systems International

AV Air Vehicle

AWSAS All Weather Sense and Avoid System

B IF equivalent bandwidth, Hz

BAMS Broad Area maritime surveillance

Backhauling Intermediate links between core network or internet backbone and small subnets at the edge of the network

Bandwidth Defined as the Range within a band of wavelengths, frequencies or energy.

Think of it as a range of radio frequencies occupied by a modulated carrier wave, assigned to a service over which a device can operate. Bandwidth is also a capacity for data transfer of electrical communications system.

BDA Battle Damage assessment

BER Bit error rate

BLOS Beyond line-of-sight

BNF Bind and Fly – with custom transmitter

BRI Belt and Road Initiative

BR&T Boeing Research and Technology

BSR Bilinear Signal Representation

BSs Base Stations

BVR Beyond visual range

c Speed of light ~ (3 x 108 m/s) [186,000 miles per sec] in vacuum named after Celeritas the Latin word for speed or velocity

c speed of sound (344 m/s) in air

C Combined methods of CR

C2 / C2W Command and control / Command and Control Warfare

C3I Command, control, communications and Intelligence

C4 Command, control, communications and computers

C4I	Command, control, communications and computers, intelligence
C4ISR	Command, control, communications, computers, intelligence, surveillance & reconnaissance
C4ISTAR	Command, control, communications, computers, intelligence, surveillance, target acquisition and reconnaissance
CA	Collision Avoidance / Clear Acquisition (GPS) / *Cyber Assault (aka Cy*A)
CAA	Control Acquisition cyber attack
CAS	Close Air Support / Common situational awareness
CASA	Civil Aviation Safety Authority
CASIC	China Aerospace Science and Industry Corporation
C of A	Certificate of Airworthiness
CAP	Civil Air Publication
CAT	Collision Avoidance Threshold
CC / CyC	Cyber Crime
CCCI/II	Classical Cryptography Course Volume I/II (Nichols R. K., Classical Cryptography Course Volume I / II, 1996)
CCE	Cyber Counter Espionage
CCI	Command control interface / *Cyber Counterintelligence*
CCS	Cyber Counter Sabotage
CCT	Cyber Counter Terrorism
CC-UAS	Counter-Counter Unmanned Aircraft Systems
CD	Conflict Detection
CDL	Common data link
CDMA	code division multiple access
CDR	Collision detection and resolution systems (automated SAA in UAS)
CEA	Cyber electromagnetic activities (Cyber, EW, Spectrum warfare)
CETC	Chinese Electronics Technology Group
CF	Computer Forensics
CFTA	Continental Free Trade Area

CFT	Certificate of flight trials / Cross-functional teams
CHIMERA	Counter-electronic HPM Extended range base air defense
CI / CyI	Cyber Infiltration
CIA	Confidentiality, Integrity, Availability / Central Intelligence Agency
CIAD	Cyber- Multi-layered Integrated Air Defense Systems
CIED	Computer improvised explosive device
CIN	Common Information Network
CIR	Color Infrared – artificial standard where NIR bands shifted so that humans can see the infrared reflectance
CLE	Airport code for Cleveland
C/N	Carrier to Noise ratio in HAPS, => C/ N0
CM / CyM	C*ountermeasure* / Cyber Manipulation
CN3	Communications / navigation network node
CNI	Critical National Infrastructure
CNKI	China-North Korea-Iran technical weapons cooperation agreements
CNO	Chief Naval Operations
CNPC	Control and non-payload links
COA	Certificate of Waiver or Authorization
COB	Chief of the Boat
COMINT	Communications intelligence
COMJAM	Communications Jamming
COMSEC	Communications Security
CONOP(S)	Concepts of Operations
CONUS	Continental United States
COS	Continued Operational Safety
COTS	Commercial off-the-shelf
CPA	Closest Point of Approach
CPA Spoof	CPA spoof involves faking a possible collision with a target ship
CPL	Commercial pilot’s license

CPNI	Center for Protection of National Infrastructure (UK)
CPRC	Communist Party of the Republic of China
CR	Conflict Resolution / Close range / Cyber Raid (aka CyR)
CRH	Coaxial rotor helicopter
CRX	Received Signal Power, watts
CS	Control station
CSDP	Common Security and Defense Policy missions (EU)
CSR	Compact Surveillance Radar
CSfC	Commercial Solutions for Classified Program
CSIRO	Commonwealth Scientific and Industrial Research Organization
CT	Counter Terrorism / Counter Terrorism Mission
CTOL	Conventional take-off and landing
C-UAS	Counter Unmanned Aircraft Systems (defenses / countermeasures)
CUAS	CSIRO Unmanned Aircraft Systems
CV	Collision Volume
CW / CyW	Cyber Warfare
D	distance from transmitter in Range equation (Adamy D. -0., 2015)
DA	Danger area

Danger Close

Definition www.benning.army.mil/infantry/magazine/issues/2013/May-June/Myer.html Nov 14, 2013 – 1) danger close is included in the "method-of-engagement" line of a call-for-fire request to indicate that friendly forces are close to the target. … Danger close is a term that is exclusive from risk estimate distance (RED) although the RED for 0.1 percent PI is used to define danger close for aircraft delivery. Pi = Probability of incapacitation. 2) Definition of "danger close" (US DoD) In close air support, artillery, mortar, and naval gunfire support fires, it is the term included in the method of engagement segment of a call for fire which indicates that friendly forces are within close proximity of the target.

DARO	Defense Airborne Reconnaissance Office
DARPA	Defense Advanced Research Projects Agency
DAS	Detection by Acoustical Signature
dB	decibels
DC	Direct Current
DCPA	Distance between vessels approaching CPA
DDD	Dull, dangerous, and dirty
DDOS	Distributed Denial of Service cyber attack
DE	Directed Energy
DEF CON	DEF CON is the world's longest running and largest underground hacking conference.
DE / EP	Directed energy / Electromagnetic pulse
DEW	Directed energy weapons
DF	Direction finding
DFCS	Digital Flight Control System
DHS	Department of Homeland Security
DIME	Diplomatic, information, military and economy
DIRCM	Directed Infrared Countermeasures
DIY	Do-it-yourself (amateur built drones or modified racing drones)
D j	Jammer location – to-target receiver location distance, in km, FM 34-40-7
DJ	Data Jamming / Drone Jammer
DJI	Popular and functional Chinese made drone series: Mavic, Phantom, Ryze, Matrix, Spark, Enterprise, Inspire, Tello {However, banned by USA Army} (Newman, 2017)
DL	Downlink in HAPS
DLA	Date last accessed (usually a web reference)
DLI	Data Link interface
DNA	Deoxyribonucleic acid
DoD	Department of Defense
DOF	Degrees of Freedom
DOS	Denial of Service cyber attack

DPM	Direct power management / Dynamic Power Management
DPRK	Democratic People’s Republic of Korea
D-R-O-N-E	FAA Guidance: Direct, Report, Observe, Notice &Execute
DSA	Detect, sense and avoid / Dynamic Sense-and-Act
DSS	Decision Support System
DSSS	Direct sequence spread spectrum
D t	Enemy transmitter location -to- target receiver location, in km, FM 34-40-7
DT	Directional transmission / Department of Transport (UK)
DTDMA	Distributed Time Division Multiple Access (DTDMA) network radio system
DTED	Digital terrain evaluation data
DTF	Drug Task Force
DTH	Direct-To-Home
DTI	Direct Track & Identify
DTRA	Defense Threat Reduction Agency
DUO	Designated UAS operator
EA	Electronic Attack
EARSC	European Association of Remote Sensing Companies
EAS	Equivalent airspeed
EAU	East Africa union comprising of Israel and six East African states, Kenya, Ethiopia, Tanzania, Uganda, Rwanda and South Sudan
(Eb / No)	Thermal noise power spectral density ratio
ECCM / EP	Electronic counter-countermeasures / Electronic Protection
ECM	Electronic countermeasures
ECR	Electronic combat reconnaissance
EDC	Estimated Date of Completion
EDEW	Effects of Directed Energy Weapons
EEZP	Exclusive economic Zone protection
EHS	Enhanced surveillance

EIRP	Effective isotopic radiated power
Electrolaser	Electroshock weapon that is also a DEW. Uses lasers to form electrically conductive laser-induced plasma charge
ELINT	Electronic Intelligence
ELT	Emergency locator transmitter
ECM	Electromagnetic compatibility
EM	Electromagnetic
EMC	Electromagnetic compatibility
EME	Electromagnetic environment
EMI	Electromagnetic interference
EMO	Electromagnetic operations
EMP	Electromagnetic pulse
EMR	Electromagnetic Radiation
EMS	Electromagnetic Spectrum
EMSVIS	Electromagnetic Spectrum Visible Light
EMW	Electromagnetic Waves
EO	Electro-optical (sensing) / Earth Observation
EOTS	Electro-optical targeting system
ERPJ	Effective radiated power of the jammer, in dBm
ERPS	Effective radiated power of the desired signal transmitter, in dBm
ESM / ES	Electronic support measures / Electronic warfare support / Earth station & ESM Electronic Signal Monitoring
EU	European Union
EUNAVFOR	European Union Naval Force's anti-piracy naval mission
EUTM	Somalia Military training mission in Somalia
EVTOL	Electric Vertical Take-off and Landing
EW	Electronic warfare, see 9-15 & footnotes
F	Field theory methods of CR
F	F*undamental frequency* is defined as the lowest frequency of a periodic waveform
f	Frequency, cycles / second RRE)
Fo	Resonant frequency of string, Hz see Eq. 20-5

F Frequency in MHz, FM 34-40-7

FAA Federal Aviation Administration

FACE Future Airborne Capability Environment

FAR False Alarm Rates

FBL Fly-by-Light, a type of flight-control system where input command signals are sent to the actuators through the medium of optical-fiber …

FBW Fly-by-wire

FCC Federal Communications Commission

FCS Flight control systems / Flight Control Station

FDF Frequency Domain Filtering

FDM frequency division multiplexing

FHSS Frequency hopping spread spectrum

FIR Far Infrared (25-40) to (200-350) um

FIRES definition (US DoD – JP 3-0) the use of weapon systems to create a specific lethal or nonlethal effect on a target.

FL Flight Level

FLIR Forward-looking infrared

Fly-by-Wire Predetermine flight mission path based on GPS coordinates

FMS Flexible manufacturing system

Follow-Me UAS autopilot automatically follows operator

Fom HAPS Figure of merit in upload /download link

FoV Field of view

FFOV Forward Field of View

FRAGO Fragmentary Order – to send timely changes of existing orders to a subordinate

FPV First Person View – live streaming video used in racing drones

FPGA Field programmable gate array

FS Fixed service

FSS Fixed satellite service

FW Fixed wing

G Geometric methods of CR

G5S	G5 Sahel (G5S) Joint Force, has membership of five states; Burkina Faso, Mali, Mauritania, Niger, and Chad
GAO	General Accounting Office USA
gAR	Receiving Antenna Gain as a Factor
GBU	Guided Bomb Unit
GCHQ	Government Communications Headquarters (Britain)
GCS	Ground control station
GDPR	European Union's (EU) General Data Protection Regulation
GDT	Ground data terminal
GEO	Geostationary Earth orbit satellite
GeoFence	A geo-fence is a virtual perimeter for a real-world geographic area
GLOW	Gross lift-off weight for a missile / rocket
GNSS	Global Navigation Satellite System
GLONASS	Global Satellite Navigational System
GPS	Global Positioning System / Geo Fencing
GPS/INS	Use of GPS satellite signals to correct or calibrate a solution from an inertial navigation system (INS). The method is applicable for any GNSS/INS system.
GPSSPOOF	Hack of GPS system affecting UAS commands
GPWS	Ground proximity warning system
G R	The receiving antenna gain in the direction of the desired signal transmitter, dBi
G RJ	Receiving antenna gain in the direction of the jammer, in dBi
GS	Ground segment of HAPs
GSE	Ground support equipment
GSHM	Ground Station Handover Method
GSM	Global System for Mobile Communications
GT	Game Theory methods of CR
G/T	Ratio of the receive antenna gain to system noise temperature

(G /Ts) dB	Represents the figure of merit of the HAPS receiver, in dB
GT	Gain of the transmit antenna, dB
GTA	Ground -to -Air Defense
Hard damage	DEW complete vaporization of a target
Harmonic	Frequency, which is an integer multiple of the fundamental frequency
H	Elevation of the jammer location above sea level, feet, FM 34-40-7
HAE	High altitude endurance
HALE	High altitude – long endurance
HAPS	High Altitude Platforms (generally for wireless communications enhancements)
HAPS UAVs	UAVs dedicated to HAPS service (example to communicate via CNPC links)
HEAT	High-explosive anti-tank warhead
HELWS	High energy laser weapon system
HITL	Human in-the-loop
HMI	Human machine interface
HO	Home Office (UK)
HPA	High power amplifier
HPL	High powered laser weapon
HPM	High powered microwave defense
H t	Elevation of enemy transmitter location above sea level, in feet, FM 34-40-7
HUD	Heads-up display
HUMINT	Human intelligence (spy's)
HVT	High value target (generally, for assassination)
I	Sound intensity, W x m-2 [Source strength S / 4πr2] (Uni-wuppertal, 2019)
IA	*Information Assurance* / Intentional cyber warfare attack
I-actors	Intentional Cyber Actors
IADS	Multi-layered integrated air defense systems
IAI	Israeli Aerospace Industries

IAS	Indicated airspeed
ICAO	International Civil Aviation Organization
I.C.B.C	International Center for Boundary Cooperation (China)
ICBM	Intercontinental Ballistic Missiles
ICGs	Information centers of gravity
ICS	Internet Connection Sharing
ID	Information Dominance / Inspection and Identification
IEDs	Improvised Explosive Devices
IEEE	Institute of Electrical and Electronics Engineers
IEWS	Intelligence, electronic warfare and sensors
IFF	Identification, friend or foe
IFR	Instrument flight rules
I&I	Interchangeability and Interoperability
IIT	Intentional Insider Threats
Imaging Sensors	ARS sensors that build images
IL	Intensity level of sound measured, dB, Eq. 20-2
IMINT	Imagery intelligence
IMM	Interacting-multiple-models tracker
IMU	Inertial Measurement Unit
INS	Inertial navigation system
IMU	Inertial Measurement Unit
INFOSEC	*Information Security*
IO	Information Operations, see Figure 9-11 & footnotes
IOC	Intergovernmental Oceanographic Commission
IOR	India Ocean Region
IoT	Internet of things
IIoT	Industrial Internet of things
IPL	Insitu Pacific Limited
IR	Infrared Sensors
IRST	Infrared search and tracking
IS	Information Superiority
ISIS	*Islamic State of Iraq and al Sham* (ISIS)

ISR	Intelligence, Reconnaissance and Surveillance UAS Platform
ISTAR	Intelligence, surveillance, target acquisition and reconnaissance
IT	Information Technology
ITU	International Telecommunications Union – Standards Organization
ITU-R	International Telecommunications Union – Radio Sector
IW	Information Warfare
JAGM	Joint-Air-to-Ground Missile
JAUS	Joint architecture for UAS
JDAM	Joint direct attack munitions
JFO	Joint fires observer
JP	Joint Publication – followed by military identifier
JDAM	Joint Direct Attack Munition
JNIM	Jama'at Nusrat al-Islam wal-Muslimin
JOAC	Joint Operational Access Concept
JOPES	Joint Operation and Planning System / Execution System
JP	Joint Publication
J / S	= the ratio of the jammer power to the desired signal power at the input to the receiver being jammed in dB
JTAC	Joint Terminal Attack Controller;
JTIDS	Joint Tactical Information Distribution System (JTIDS) is an L band DTDMA
K	Boltzmann's constant (Noise component, RRE) (1.38 x 10 -23 J/K), Kelvin
K	2 for jamming frequency modulated receivers (jamming tuner accuracy), FM 34-40-7
KAMIKAZI	Means "Divine Wind," Tactic best known for Japanese suicide A/C attacks on Allied Capital Vessels in WWII. UAS TEAMS or SWARMS could be directed in the same way.
KE	Kinetic energy
KEW	Kinetic energy weapons

KM Katiba Macina Groups

L λ / 2 in Eq. 20-5

LAANC Low Altitude Authorization and Notification Capability

LASER "A laser is a device that emits light through a process of optical amplification based on the stimulated emission of electromagnetic radiation. The term "laser" originated as an acronym for "light amplification by stimulated emission of radiation". A laser differs from other sources of light in that it emits light coherently, spatially and temporally. Spatial coherence allows a laser to be focused to a tight spot, enabling applications such as laser cutting and lithography. Spatial coherence also allows a laser beam to stay narrow over great distances (collimation), enabling applications such as laser pointers. Lasers can also have high temporal coherence, which allows them to emit light with a very narrow spectrum, i.e., they can emit a single color of light. Temporal coherence can be used to produce pulses of light as short as a femtosecond. Used: for military and law enforcement devices for marking targets and measuring range and speed." (Wiki-L, 2018)

Laser JDAM Laser Joint Direct Attack Munition – dumb bombs, all weather precision –guided munitions. Guided by an integrated inertial guidance system.

Laser rangefinder Scope to assist targeting of munitions. Countermeasure: laser-absorbing paint

LGWs Laser-guided weapons

Latency Processing difference between time interval signal is transmitted and signal is received

LCDR Lieutenant Commander

L/D Lift to drag ratio

LDCM Low Duty cycle methods

LEO Low Earth Orbit Satellite

LGB Laser-guided bomb, a guided bomb that uses semi-active laser guidance to strike a designated target with greater accuracy than an unguided one

LGTF	Liptako-Gourma task force (LGTF) established by Burkina Faso, Mali, and Niger to secure their shared border region
LIDAR	Light (Imaging) Detection and Ranging
LFS	Free- Space Loss as a Factor
LIPC	laser-induced plasma channel
LJ	Propagation loss from jammer to receiver, in dBi
LMADIS	Light Marine Air Defense Integrated System (family of C-UAS systems)
LMM	Lightweight Multi-role Missile (by Thales)
LOS	Line-of-sight / Loss of Signal / Loss of Separation
LOSAS	Low cost Scout UAV Acoustic System
LPA	Log periodic array
LPI	Low Probability of Intercept
LR	Long range
LRA	Long range artillery
LRAD	Long Range Acoustic Device (Weapon) (Yunmonk Son, 2015)
LRCS	Low radar cross section
LRE	Launch and recovery element
LRF	Laser rangefinder
LS	Losses existing in the system (lumped together), dB (RRE)
LS	The propagation loss from the desired signal transmitter, in dBm
LSDB	Laser Small Diameter Bomb
LST	Laser spot trackers
LTA	Lighter than Air (airship) /Low noise amplifier
LTE /LTE+	Long Term Evolution – refers to mobile telecommunications coverage
LWIR	Long wave Infrared (sensor or camera)
M	Mass in Eq. 20-5
MA	Multi-agent methods of CR
MAD	Magnetic anomaly detection
MADIS	Marine Air Defense Integrated System
MAE	Medium-altitude endurance

MAGTF	Marine air-ground task force
MALDRONE	Malware injected into critical SAA for UAS
MALE	Medium-altitude, long endurance UAS
MALE-T	Medium altitude long endurance – tactical UAS
MAME	Medium altitude, medium endurance.
MASINT	Measurement and Signal Intelligence
MATS	Mobile Aircraft Tracking System
M-AUDS	Mobile Anti-UAV Defense System
MAV	Micro-air vehicle
Maverick	AGM -65 (USA) Missile
MCE	Mission control element
MCM	Mine countermeasures
MCU	Master Control Unit
MDR	Missed Detection Rates
MEB	Marine expeditionary brigade (14,500 marines and sailors);
MEMS	Micro-electromechanical systems
MEO	Medium Earth Orbit satellite
MFD	Multi Function display
MGTOW	Maximum gross takeoff weight
MHT	Multiple-hypotheses-testing
MIM	Man in the Middle cyber attack
MINUSMA	Multidimensional Integrated Stabilization Mission in Mali
MIR	Mid Infrared 5 to (25-40) um
MIT	Massachusetts Institute of Technology
MLRS	Multi launch rocket systems
MLU	Mid-life upgrade
MMI	Man-machine interface
MORS	Military Operations Research Society
MPA	Maritime patrol aircraft
MPI	Message-passing interface
MPO	Mission payload operator
MR	Medium range
MRE	Medium-range endurance

MS Mobile service

MSL / AGL MSL altitudes are measured from a standard datum, which is roughly equal to the average altitude of the ocean. So, an aircraft traveling 5,000 feet directly above a mountain that's 3,000 feet tall would have an altitude of 5,000 feet Above Ground Level (AGL) and 8,000 feet MSL.

MSR Maritime Silk Road (China)

MTCR missile Technology Control Regime

MTI Moving target indication

MTOM Maximum take-off mass

Modulation Signal Modulation is the process of varying one or more properties of a periodic waveform, called the *carrier signal*, with a modulating signal that typically contains information to be transmitted

MORS Military Operations Research Society

MTOW Maximum takeoff weight of an aircraft at which the pilot can attempt to take off, due to structural or other limits.

MTS Multi Spectral Targeting System

MTTR Multitarget tracking radar/Mean time to repair

MUAV Mini-UAV or maritime UAV

MUJAO Movement for Unity and Jihad in West Africa

MUM Manned-unmanned teaming

MW Microwave

MWIR Midwave Infrared

MW microwave towers

N Available Noise power, watts for HAPS

N Terrain and ground conductivity factor, FM 34-40-7

5 = very rough terrain with poor ground conductivity

4 = moderately rough terrain with fair to good ground conductivity

3 = Farmland terrain with good ground conductivity

2 = Level terrain with good ground conductivity[1]

The elevation of the jammer location and the enemy transmitter location does not include the height of the antenna above the ground or the length of the antenna. It is the location deviation above sea level.

NAC	Network Access Control
NACA	National Advisory Committee on Aeronautics
NAS	National Airspace (USA)
NASAMS II	National Advanced Surface to Air Missile System
NATO	North Atlantic Treaty Organization
NAV	Nano-air vehicle / NAV data message for GPS systems
NBC	Nuclear, biological and chemical warfare
NCO	Network-centric operations
NCW	Network Centric Warfare
NDRC	National Development and Reform Commission (China)
NEC	Network enabled capability
NGO	Non-Governmental Organization
NIEM	National Information Exchange Model
NIR	near Infrared
NLOS	Non-line-of-sight
NM	Nautical Miles
NMAC	A NMAC is defined as an incident associated with the operation of an aircraft in which a possibility of collision occurs as a result of proximity of less than 500 feet to another aircraft, or a report is received from a pilot or a flight crewmember stating that a collision hazard existed between two or more aircraft.
NMLA	the National Movement for Liberation of Azawad (Tuareg Rebellion)
NO	Numerical Optimization methods of CR
NOLO	No onboard live operator (USN)
NOTAM	Notice to airmen
NPD	Near Peer Doctrine
NPS	National Park Service
NSA	National Security Agency (US)
NSRL	New Silk Road Sea / Land routes (Chinese)

NTIA	National Telecommunications and Information Administration
NTSB	National Transportation Safety Board
NTT	Non-Threat Traffic
NULLO	Not using live operator (USAF)
O	Other methods of CR
OEM	Original Equipment Manufacture
OIO	Offensive Information Operations
OLOS	Out-of-the-line-of-sight
OODA	Decision Loop: Observe, Orient, Decide, Act
OPA	Optionally piloted aircraft
OPAV	Optionally piloted air vehicle
OPSEC	Operations Security
OSI	Open systems interconnection
OTH	Over- the- horizon
P	Isotropic source of an electromagnetic pulse of peak power, Mw
PANCAS	Passive Acoustic Non-Cooperative Collision Alert System
PB	Particle Beams, Particle beams are large numbers of atomic or subatomic particles moving at relativistic velocities.
PCAS	Persistent close air support
PCS	Personal Communication Services
PEIRP	Transmitter's effective isotropic radiated power, watts
PFMS	Predictive Flight Management System
PEMSIA	Partnership in Environmental Management of the Seas of East Asia
PGB	Precision guided bomb
PGM	Precision guided missile
PHOTINT	Photographic intelligence (usually sky – ground)
PHX	Airport code for Phoenix
PI	Probability of Incapacitation
PII	Personal Identifiable Information

PIM	Position of intended movements/Previously intended movements
PIT	Proximity Intruder Traffic
P j	Minimum amount of jammer power output required, in watts, FM 34-40-7
PL	Power level, dB, Eq. 20-1
PLA	Chinese People's Liberation Army
PLAN	Peoples Liberation Army Navy (China)
PLC	Programmable Logic Controllers
PMIAA	Permissions Management: Identification, Authentication and Authorization
PNF	Plug and Fly with custom transmitter, receiver, battery and charger
PO	Psychological Operations
POS	Position and Orientation System
POV	Point of View
PPP	Precise Point Positioning
PPS	Precise positioning service (GPS)
PRC	Peoples Republic of China (China)
Primum Non Nocere – First Do No Harm (Latin)	
PSD	Power Spectral Density
PREACT	*Partnership for Regional East Africa Counterterrorism* (PREACT)
PRF	Pulse repetition frequency codes
PRM	Precision Runway Monitor
PSH	Plan-symmetric helicopter
PSR	Primary Surveillance Radar
P t	Power output of the enemy drone, in watts, FM 34-40-7
PW /PSYWAR	Psychological Warfare
PWO	Principal Warfare officer
P(Y)	Precise Signal (GPS)
QOS	Quality of Service in HAPs
QUAS	QUT UAS
QUT	Queensland University of Technology

R	1 /Tb is the bit rate (b/s) in link equation
R4	Energy density received at detected target range, R, nm
RA	Resolution Advisory
RAC	Range air controller
RADAR	Radio Detection and Ranging
RADINT	Radar intelligence
RAM	Radar absorbing materials
RAS	Radar absorbing structure
RAST	Recovery, assist, and traverse
RB	Rule-based methods (Conflict Resolution)
RBW	Red- breasted Woodpecker
RCE	Remote Code Execution
RCO	Remote-control operator
RCS	Radar cross-section
RCTA	Surf Radio Technical Commission for Aeronautics
RED	Risk Estimate Distance
RES	Radio electronic systems
RF	Radio Frequency
RGB	Red Green Blue for VIS camera
RGT	Remote ground terminal
Rician PDF	Rician probability density function
RIMPAC	Rim of the Pacific Exercise – Maritime
RL	Ramp launched
RMS	Reconnaissance management system /Root-mean-square
RN	Ryan-Nichols Qualitative Risk Assessment Equations 17-2, 17-3
RNRA	Ryan – Nichols Attack / Defense Scenario Risk Assessment for Cyber cases
ROA	Remotely operated aircraft
ROC	Republic of China (Taiwan) / Regional Operations Center (USA)
RPA	Remotely piloted aircraft
RPH	Remotely piloted helicopter

RPV	Remotely piloted vehicle
RR	Radio regulations
RRE	Radar Range Equation
RSA	RSA (Rivest–Shamir–Adelman) -authors of early public –key cryptographic system
RSTA	Reconnaissance, surveillance and target acquisition
RTA	Dubai Roads and Transport Authority
RTF	Off- the- shelf, Ready -to -Fly
RTK	Real Time Kinematic
RTS	Remote tracking station/Request to send/Release to service
RTU	Remote Terminal Unit
RUAV	Relay UAV
RWR	Radar warning receiver
S	Intensity at surface of sphere
SA	Situational Awareness
SAA	Sense and Avoid &
SAA	*Sense and Act Systems*; replaces *See and Avoid function* of a human pilot
SAASM	Selective Availability Anti-Spoofing Module
SAE	Society of Automotive Engineers
SAM	Surface to Air Missile
SAMPLE	Survivable autonomous mobile platform, long-endurance
SAP	Systems Applications and Products also the name of a company
SAR	Synthetic aperture radar / Search and rescue- especially using helicopters
SAS	Safety Assurance System
SATCOM	Satellite communications
SCADA	Supervisory Control and Data Acquisition systems
SCHEMA	Security Incident Identification
SCIF	Sensitive Compartmented Information Facility
SCS	Shipboard control system (or station) / Stereo Camera System / South China Sea

SE Synthetic environment

SEA Airport code for Seattle

SEAD Suppression of Enemy Air Defenses

SECDEF Secretary of Defense

Shadowing Airframe shadowing – UAV- Ground signal degradation during maneuver

SEZ Special economic zones

SHM Simple harmonic motion – represented by sign wave

SHORAD Short Range Air Defense systems

SIGINT Signals Intelligence

Signature UAS detection by acoustic, optical, thermal and radio /radar

SJM Salafi-Jihad Movement

SKASaC Seeking airborne surveillance and control

SKYNET Fictional artificial intelligence system that becomes self-aware

SLAMRAAM Surface launched AMRAAM

SM Separation Management

SMC Single moving camera

SME Subject matter expert

SMR Single main rotor

S/N S / N = is one pulse received signal to noise ratio, dB; Signal to Noise ratio at HAPS receiver

SOA Static Obstacle – Avoidance system

Soft damage DEW disruption to a UAS computer

SPL Sound pressure level, dB = 20 Log p / po [measured pressures to reference pressure] see Eq. 20-3,4; 6-7

SPS Standard position service (GPS)

Spoofing A Cyber-weapon attack that generates false signals to replace valid ones

Spot sensors ARS sensors that measure single locations without image library.

SQL SQL Injection – common malevolent code injection technique

SR Short range

SRBM	Short range ballistic missile, ex SCUD missile
SRL	Systems readiness level
SSA	Static Sense-and -Act
SSBN	Ballistic missile submarine force
SSP	Smart Skies Project
SSR	Secondary Surveillance Radar
SST	Self – Separation Threshold
STANAG 4856	Standard interfaces of UAV Control System for NATO UAV
STK	Satellite toolkit
STOL	Short take-off and landing
sUAS	Small Unmanned Aircraft System
SUAVE	Small UAV engine
SWARM	High level, dangerous collaboration of UAS, UUV, or unmanned boats
SWAT	Special Weapons and Tactics (police / paramilitary)
SWAP	Size, weight and power
SWIR	Shortwave infrared, 1400-3000 nm, 1.4 -3.0 um wavelength range
SZ	**Safety Zone** is defined as the horizontal and vertical separation criteria which form a cylindrical airspace volume around the UAS. In figure 3-2 that volume is defined by 1000 ft radius and 200 ft height. It is assumed that initially the UAS is in the center with 100 ft above and below the A/C.
T	In Range equation & environment, strength of a received signal, function of square or fourth power of distance, d, from transmitter (Adamy D. -0., 2015)
T	Time, sec (RRE)
T	Tension in Eq.20-5
TA	Traffic Advisory
TAC	Target air controller
TACAN	Tactical air navigation
TAR	Antenna noise temperature, Kelvin
TAS	True airspeed
TBO	Time between overhauls

TC Type certificate

TCAS Traffic alert and collision avoidance system

TCPA Time to reach Closest Point of Approach

Te Effective input noise temperature, Kelvin,

TEAM (UAS) High level, dangerous collaboration of UAS, UUV, or unmanned boats; differs from SWARM in that it has a UAS Team Leader, (TL) where SWARM does not. TL directs the UAS team and is the primary counter UAS target to disrupt.

TETRA Terrestrial Trunked Radio for terrestrial terminals / services

Thermobaric Metal augmented charge

THOR Tactical high-power operational responder

TIR Thermal infrared = 8000 – 15000 nm, 8 -15 um

TL Team Leader

TO take-off

Tort A tort is an act or omission that gives rise to injury or harm to another and amounts to a civil wrong for which courts impose liability.

TP Trajectory Prediction

TRANSCOM U.S. Transportation Command networks

TRL Technology readiness level

TS Measured noise temperature, Kelvin units above absolute zero

TSTCP Trans-Sahara Counterterrorism Partnership. TSCTP partners include Algeria, Burkina Faso, Cameroon, Chad, Mali, Mauritania, Morocco, Niger, Nigeria, Senegal, and Tunisia.

TT & C Telemetry, tracking and command

TUAV Tactical UAV

UA Unmanned Aircraft (non-cooperative and potential intruder)

U-Actors Unintentional Cyber Actors

UAE United Arab Emirates

UAM Urban Air Mobility (vehicle)

UAPO Unmanned Aircraft Program Office

UAS Unmanned aircraft system

UASCdr	Unmanned aircraft system commander
UASIPP	UAS Integration Pilot Program
UAS-p	UAS pilot
UAV	Unmanned aerial vehicle
UAV-p	UAV pilot
UBR	Uplink bit rate, Mb/s
UCAR	Unmanned combat armed rotorcraft
UCARS	UAV common automated recovery system
UCAV	Unmanned combat air vehicle
UCWA / UA	Unintentional cyber warfare attack
UGCS	Unmanned Ground Control Station
UGS	Unmanned ground-based station
UGV	Unmanned ground vehicle
UHF	Ultra High Frequency, 300 MHz – 3 GHz
UIT	Unintentional Insider Threats
UK	United Kingdom
UL	Upload link
UMTS	Universal Mobile Telecommunications System
U.N.	United Nations
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNICEF	United Nations Children's Fund
USD	Unmanned surveillance drone
UTM	Unmanned Traffic Management
UTV	Unmanned target vehicle
UUV	Unmanned underwater vehicle
UUNs / DUNSs	Urgent / deliberate universal needs statements
V	Visible
VFR	Visual flight rules
VIKI	Virtual Interactive Kinetic Intelligence
VLA	Very light aircraft
VLJ	Very Light Jet
VLAR	Vertical launch and recovery
VLOS	Visual Line of Sight
VMC	Visual Meteorological Conditions

VNIR	Visible light and near infrared 400 – 1400 nm, 0.4 – 1.4 um wavelength range
Voloport	Landing site for Volcopter
VTOL	Vertical take-off and landing
VTUAV	Vertical take-off UAV
WEF	World Economic Forum
WEZ	Weapon Engagement Zone
WMD	Weapons of Mass Destruction
WRC	World Radio Conference Standards Organization
XO	Executive Officer of Naval vessel
ZIGBEE or KILLERBEE	Sniffing / penetration tools specific to UAS

Greek Symbols

λ	Wavelength in Hz, c / f where c= speed of light 344 m/s and f = frequency, Hz.
Σ	Radar Cross Sectional Area, m2

Sources plus Bibliography below: (Nichols R. K., 2019)

Austin, R, (2010) *Unmanned Aircraft Systems*: UAVS *Design, Development and Deployment*, West Sussex, UK: Wiley, [Condensed with additions from eleven-page "Units and Abbreviations Table." Pp. ix-xxix] Additional sources generated from / specific to Chapter development / discussion. A few definitions taken from Wikipedia.

Cyber terminology from: Nichols, R. K. (Sept. 5, 2008) *Cyber Counterintelligence & Sensitive Compartmented Information Facility (SCIF) Needs – Talking Points & (Randall K. Nichols J. J., 2018) & (Nichols R. K., Hardening US Unmanned Systems Against Enemy Counter Measures, 2019) & (Randall K. Nichols D. , Chapter 20 Acoustic CM & IFF Libraries* V SWARMS *Rev* 1 05142019, 2018) *& (Randall K. Nichols and Lekkas*, 2002)*& (*NIST, *September* 2012)

Alford, L. D., Jr., USAF, Lt. Col. (2000) Cyber Warfare: Protecting

Military Systems *Acquisition Review Quarterly*, spring 2000, V.7, No. 2, P, 105, (Nielsen, 2012)

Nichols, Randall K.; Mumm, Hans C.; Lonstein, Wayne D.; Ryan, Julie J.C.H.; Carter, Candice; and Hood, John-Paul, "Unmanned Aircraft Systems in the Cyber Domain" (2019). *NPP eBooks*. 27. https://newprairiepress.org/ebooks/27

Http://Www.Dtic.Mil/Dtic/Tr/Fulltext/U2/A487951.Pdf

Appendix 1: Standard Acoustic Principal Physical Properties **(Entokey, 2019)**

and **(Gelfand S. A., 2009)**

A majority of the technical abbreviations come from (Nichols, et al., Unmanned Aircraft Systems in the Cyber Domain, 2019)

Bibliography

49 U.S. Code §40103, 49 U.S. Code §40103 Sovereignty and use of airspace (U.S. Code July 5, 1994).

Abramson, E. (2016). *Ethical Dilemmas in the Age of AI*. Retrieved from Abramson, E. – knowmail.me/blog: https://www.knowmail.me/blog/ethical-dilemmas-age-ai/

Adamy, D. -0. (2015). *EW 104 EW against a New Generation of Threats*. Boston: Artech House.

Adamy, D. (2001). *EW 101 A First Course in Electronic Warfare*. Boston, MA: Artech House.

Adamy, D. (2001). *EW 101 A First Course in Electronic Warfare*. Boston: Artech House.

Adamy, D. (2004). *EW 102 A Second Course in Electronic Warfare*. Boston: Artech House.

Adamy, D. (2009). *EW 103 Tactical Battlefield Communications Electronic Warfare*. Boston: Artech House.

Adamy, D.-9. (1998, Jan). Lesson 4: the basic link for all EW functions. (electronic warfare)(EW Reference & Source Guide). *Journal of Electronic Defense, Jan 1998 Issue*.

Administrator. (2015, June 15). *Standing Wave and Fundamental*

Frequency. Retrieved from Electronics Hub: https://www.electronicshub.org/?s=fundamental+frequency

Administrator. (2019, May 17). *Harmonic Frequencies.* Retrieved from electronicshub.org: https://www.electronicshub.org/harmonic-frequencies/

Alejandro Aragon-Zavala, J. L.-R.-P. (2008). *High-Altitude Platforms for Wireless Communications.* Chichester, West Sussex, UK: John Wiley & Sons.

Alford, L. (2000). Cyber Warfare: Protecting Military Systems. *Acquisition Review Quarterly.*

Anon. (2019). *Saudi Arabia grants citizenship to robot Sophia.* Retrieved from dw: Saudi Arabia grants cihttps://www.dw.com/en/saudi-arabia-grants-citizenship-to-robot-sophia/a-41150856

Asimov, I. (1950). "*Runaround*". *I, Robot (The Isaac Asimov Collection ed.).* New York City: Doubleday.

Atherton, K. D. (2019). Can the Pentagon sell Silicon Valley on AI as ethical war? . *C4ISRNET.*

Austin, R. (2010). "*Design for Stealth*", *Unmanned Aircraft Systems* UAVS *Design Development and Deployment.* New York: John Wiley and Sons.

Brown, E. F. (Dec 2008). Airborne Communication Networks for Small Unmanned Aircraft Systems. *Proc. IEEE*, *vol* 96, *no* 12, pp. 2008-17.

Burch, D. (2015). *RADAR for Mariners.* New York: McGraw-Hill.

Cameron, J. &. (Director). (1991). *Terminator 2: Judgement Day* [Motion Picture].

Chapman, A. (2019, May 31). *GPS Spoofing.* Retrieved from Tufts University – Tech Notes 2017: https://sites.tufts.edu/eeseniordesignhandbook/files/2017/05/Red_Chapman.pdf

Cornell University Legal Information Institute. (2019, June 5). *But-for test.* Retrieved from law.cornell.edu: https://www.law.cornell.edu/wex/but-for_test

Cornell University Legal Information Institute. (2019, June 5). *Intervening Cause.* Retrieved from law.cornell.edu: https://www.law.cornell.edu/wex/intervening_cause

Cornell University Legal Information Institute. (2019, June 5). *Personal Jurisdiction.* Retrieved from law.cornell.edu: https://www.law.cornell.edu/wex/personal_jurisdiction

D, G. a. (2010). *Broadband Communications via High Altitude Platforms.* New York City, NY: John Wiley & Sons.

Daniel-Cornel TĂNĂ, S. (2018). The Impact of the Development of Maritime Autonomous Systems on the Ethics of Naval Conflicts. *Annals: Series on Military Sciences*(2), 118-130.

Deloitte Center for Government Insights analysis. (2018, June 18). *The future of regulation. Principles for regulating emerging technologies.* Retrieved from Deloitte Insights: https://www2.deloitte.com/insights/us/en/industry/public-sector/future-of-regulation/regulating-emerging-technology.html

Dewey, D. (2017, July 14). *Drone crashes into LDS temple in Utah; raises questions of airspace rules.* Retrieved from eastidahonews.com: https://www.eastidahonews.com/2017/07/drone-crashes-lds-temple-utah-raises-questions-airspace-rules/

Diversity of citizenship; amount in controversy; costs, 28 U.S. Code §1332 (United States Congress June 25, 1948).

DJI. (2019, June 5). *DJI Enterprise.* Retrieved from Enterprise DJI.com: https://enterprise.dji.com/civil-protection

DLSR Pros. (2019, June 3). *Best Drones* (UAVs) *for Firefighting in* 2019. Retrieved from dlsrpros.com: https://www.dslrpros.com/dslrpros-blog/best-drones-firefighting-2019/

DoD. (2018). *Dictionary of Military Terms.* Retrieved from JCS.Mil: http://www.jcs.mil/doctrine/dod_dictionary/

DoD. (2018). *Joint Publication (JP) 3-01 Countering Air and Missile Threats.* Washington, DC: DoD.

DoD-02. (2018). *Information Operations (IO) in the United States.* Retrieved from JP 3-13 : http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf

DoD-03. (2015). *Unmanned Systems Roadmap 2013 to 2038.* Retrieved from DTIC: http://www.dtic.mil/dtic/tr/fulltext/u2/a592015.pdf

Drones, Q. S. (2017, July 11). *quadcopters-have-hit-the-sound-barrier/.* Retrieved from quadstardrones.com: https://quadstardrones.com/2017/07/11/quadcopters-have-hit-the-sound-barrier/

EARSC. (2015). A Taxonomy for the EO Services Market: enhancing perception and performance of the EO service industry. *EARSC Issue* 2.

Entokey, a. G. (2019, May 16). *entokey.com/acoustics-and-sound-measurement/*. Retrieved from entokey.com/acoustics-and-sound-measurement/: https://entokey.com/acoustics-and-sound-measurement/

ESA-ESTEC Contract 162372/02/NL/US. (September 2005). STRATOS: *Stratospheric Platforms a definition study for* ESA *Platform, Final Report*, 1-34. ESA-ESTEC .

European Union. (2019, May 2019). *About the regulation and data protection.* Retrieved from ec.europa.eu: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

Federal Question, 28 U.S. Code §1331 (United States Congress June 25, 1948).

FEMA. (2013). *Lessons Learned from the Boston Marathon Bombings: Preparing for and Responding to the Attack.* Retrieved from www.fema.gov: http://www.fema.gov/media-library-data/20130726-1923-25045-1176/lessons_learned_from_t

Filippo Santoni de, S. &. (2018). Meaningful Human Control over Autonomous Systems: A Philosophical Account. *Frontiers in Robotics and* AI. doi:10.3389/frobt.2018.00015

Fleetwood, J. (2017). Public Health, Ethics, and Autonomous Vehicles. *American Journal of Public Health*, 107(4), 632-537.

Fortuna, C. (2017, 12 02). *Autonomous Driving Levels* 0–5 + *Implications.* Retrieved from cleantechnica.com: https://cleantechnica.com/2017/12/02/autonomous-driving-levels-0-5-implications/

Gelfand. (2004). "*Physical Concepts*", *Hearing an Introduction to Psychological and Physiological* Acoustics, *4th ed.* New York City.

Gelfand, S. A. (2009). *Essentials of Audiology, 3rd Edition*. Stuttgart, DE: Thieme.

Giordano, N. (2009). *College Physics: Reasoning and Relationships*. New York City, NY: Cengage Learning. pp. 421–424.

Guardbaum, S. (1994). The Nature of Preemption. *Cornell Law Review*, 767, 771.

Harris Aerial. (2019, June 5). *Carrier HX8 Sprayer Drone*. Retrieved from harrisaerial.com: https://www.harrisaerial.com/carrier-hx8-sprayer/

Heinman, C. (2019). *Hearing Loss Tests Patrient D v-105*. Carlisle, PA: Brown Optical Hearing Aid Service.

Henderson, T. (2017). The Doppler Effect – Lesson 3, Waves. *Physics tutorial. The Physics Classroom*. Retrieved from Henderson, Tom (2017). "The Doppler Effect – Lesson 3, Waves". Physics tutorial. The Physics Classroom. Retrieved September 4, 2017.: Henderson, Tom (2017). "The Doppler Effect – Lesson 3, Waves". Physics tutorial. The Physics Classroom. Retrieved September 4, 2017.

Hern, A. (2017, 1 12). *Give robots 'personhood' status, EU committee argues*. Retrieved from The Guardian: www.theguardian.com/technology/2017/jan/12/give-robots-personhood-status-eu-committee-argues

Hubbard, R. K. (1998). *Boater's Bowditch*. Camden, MA: International Marine.

Ibrahim, A. (2019). *Optimization Methods for User Admissions and Radio Resource Allocation for Multicasting over High Altitude Platforms* . Memorial University of Newfoundland , Canada: River Publications.

IEEE . (2017). The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems Announces New Standards Projects. *Telecom Standards*, 27(11), pp. 4-5. .

Jesus Gonzalo, D. L. (2018, March 15). On the Capabilities and Limitations of High Altitude Pseudo-Satellites. *Progress In Aerospace Sciences*, 37-56. doi:https://doi.org/10.1016/j.paerosci.2018.03.006

Johnson, O. &. (2012). *Ethics: Selections from Classic and Contemporary Writers*. Boston, MA: Cengage Learning.

Jones, T. (2017). *International Commercial Drone Regulation and Drone Delivery Services*. Santa Monica: The Rand Corporation.

Kanowitz, S. (2019, 05 15). *Toward the deployment of ethical AI*. Retrieved from Government Computer News. : Kanowitz, S. (2019). Toward the dephttps://gcn.com/articles/2019/05/15/ethical-ai-idc.aspx?s=gcntech_200519

Kirk, J. (2015, August 5). *sounds-can-knock-drones-sky*. Retrieved from www.computerworld.com.au/article/581231: https://www.computerworld.com.au/article/581231/sounds-can-knock-drones-sky/

Knight, W. (2018). Nine charts that really bring home just how fast AI is growing. *MIT Technology Review* .

Legal Information Institute – Cornell University. (2019, May 31). *Strict Liability* . Retrieved from Legal Information Institute: https://www.law.cornell.edu/wex/strict_liability

LRAD. (2019, May 189). *LRAD 450XL Datasheet*. Retrieved from LRADX: http://www.lradx.com/wp-context/uploads/2015/05/LRAD_datasheet_450XL.pdf

MacGregor, D. S. (2018). *Colorado Causes of Action: Elements, Defenses, Remedies, and Forms*. Denver: Bradford Publishing Co. .

Macnamara, T. M. (2010). *Introduction to Antenna Placement & Installation*. New York City, NY : John Wiley & Sons.

Mahon, J. (2012). *Classical Natural Law Theory St. Thomas Aquinas (1227-1274) – the "Angelic Doctor" Lecture*. Retrieved from Mahon, J. (2012). Classical Natural Law Theory St. Thomas Aquinas (1227-1274) – the Philosophy of Law. : Mahon, J. (2012). Classical Natural Law Theory St. Thomas Aquinas (1227-http://home.wlu.edu/~mahonj/PhilLawLecture1NatLaw.htm

Marbury v. Madison, 5 U.S. 137 (United States Supreme Court February 23, 1803).

Matolak, R. S. (April 2015). Initial Results for Airframe Shadowing in L-band and C-band Air -Ground Channels. *Proc. Integrated Commun,, Navigation, and Surveillance Conf*, (pp. pp. 1-8).

McCullogh v. Maryland, 17 U.S. 316 (United States Supreme Court March 6, 1819).

Merriam-Webster. (2019, May 17). Merriam-Webster Online Dictionary.

Merriam-Webster, Inc. (2019). *Definition of Ethics.* online: Merriam-Webster, Inc. Retrieved from Definition of Ethics. (2019a). Online: Merriam-Webster, Incorporated.: Definition of Ethics. (2019a). Online: Merriam-Webster, Incorporated.

Middleton, C. (2018). *SAP launches ethical A.I. guidelines, expert advisory panel.* Retrieved from internetofbusiness.com: Middleton, C. (2018). SAP launches ethical A.I. guidelines, expert advisory panel. Retrieved from https://internetofbusiness.com/sap-publishes-ethical-guidelines-for-a-i-forms-expert-advisory-panel/

Misselhorn, C. (2018). Artificial Morality. Concepts, Issues and Challenges. *Society*, 55(2), 161-169.

Mohorcic, D. G. (2010). *Broadband Communications via High Altitude Platforms.* New York City, NY: John Wiley & Sons.

Monahan, K. (2004). *The Radar Book: Effective Navigation and Collision Avoidance.* Anacortes, WA: Fineedge Publications.

Muspratt, A. (2018, November 22). *New global drone standards proposed.* Retrieved from Defence iQ: https://www.defenceiq.com/defence-technology/news/new-global-drone-standards-proposed

85. Goddemeir, K. D. (June 2015). Role-based Connectivity Management with Realist Air to Ground Channels for Future Applications. *IEEE Vehic. Tech. Mag.* Vol 10, *no* 2, pp. 79-85.

National Conference of State Legislatures. (2018, September 10). *Current Unmanned Aircraft State Law Landscape.* Retrieved from NCSL.org: http://www.ncsl.org/research/transportation/current-unmanned-aircraft-state-law-landscape.aspx

NBC Today Show. (2018, May 9). *How peeping drones could be spying on you without you knowing it.* Retrieved from Today.com: https://www.today.com/video/how-peeping-drones-could-be-spying-on-you-without-you-knowing-it-1229001795967

Newman, L. H. (2017, August 7). *THE ARMY GROUNDS ITS DJI*

DRONES OVER SECURITY CONCERNS. Retrieved from WIRED: https://www.wired.com/story/army-dji-drone-ban/

Nichols, R. K. (1996). *Classical Cryptography Course Volume I / II.* Laguna Hills, CA: Aegean Park Press.

Nichols, R. K. (1996). *Classical Cryptography Course, Volume I.* Laguna Hills, CA: Aegean Park Press.

Nichols, R. K. (2018). *Unmanned Aircraft Systems (UAS) In the Cyber Domain: Protecting USA's Advanced Air Assets. 1st Ed.* Manhattan, KS: New Prairie Press.

Nichols, R. K. (2019, March 14). Hardening US Unmanned Systems Against Enemy Counter Measures. *7th Annual Unmanned Systems Summit*. Alexandria, VA, USA: PPTX presentation , self.

Nichols, R. K. (2019). *Unmanned Aircraft Systems In the Cyber Domain: Protecting USA's Advanced Air Assets. 2nd Ed. Manhattan, KS: New Prairie Press.* Manhattan, KS: New Prairie Press.

Nichols, R. K., Mumm, H. C., Lonstein, W. D., Ryan, J. J., & and Carter, C. (2018). *Unmanned Aircraft Systems (UAS) in the Cyber Domain: Protecting USA's Advanced Air Assets.* Manhattan, KS: New Prairie Press (NPP) eBooks. 21.

Nichols, R. K., Mumm, H. C., Lonstein, W. D., Ryan, J. J., Carter, C., & and Hood, J.-P. (2019). *Unmanned Aircraft Systems in the Cyber Domain.* Manhattan, KS: NPP eBooks. 27.

Nielsen, P. E. (2012). *Effects of Directed Energy Weapons.* Middletown, DE: CreateSpace Independent Publishing Platform.

NIST. (September 2012). *Guide for Conducting.* Washington, DC: GPO.

North Carolina Department of Transportation. (2019, May 30). *Law & Regulations.* Retrieved from NCDOT.GOV: https://www.ncdot.gov/divisions/aviation/uas/Pages/laws-regulations.aspx

Osseiran, A. (Dec 2014). Scenarios for 5G Mobile and Wireless communications: the vision of the METIS Project. *IEEE Communications Magazine*, Vol 52, *no* 5, pp. 26-35.

O'Sullivan, J. L. (1845). The Great Nation of Futurity. *United States Magazine and Democratic Review* Vol 6 Issue 23, pp. 426-430.

Pierson. (2019, May 16). *tuning-fork-waves-sound.* Retrieved from airfreshener.club – Pierson Education: https://airfreshener.club/quotes/tuning-fork-waves-sound.html

Porter, J. D. (2019, June 8). *jdporterlaw.com/intellectual-property-law/.* Retrieved from jdporterlaw.com: http://www.jdporterlaw.com/intellectual-property-law/

Possel, M. (2017). Waves, motion and frequency: the Doppler effect. *Einstein Online, Vol. 5. Max Planck Institute for Gravitational Physics, Potsdam, Germany.*

Price Waterhouse Coopers, LLP. (2018). *Skies without limits – Drones- taking the UK's economy to new heights.* London: Price Waterhouse Coopers, LLP.

PROTECTION OF CERTAIN FACILITIES AND ASSETS FROM UNMANNED AIRCRAFT, H. R. 302 (United States Congress January 3, 2018).

Proyas, A. (Director). (2004). *I, Robot. In. Hollywood,* CA. [Motion Picture].

Ramzy, A. &. (2008). *Tainted-Baby-Milk Scandal in China.* Retrieved from content.time.com/time/world/article/: http://content.time.com/time/world/article/0,8599,1841535,00.html

Randall K. Nichols and Lekkas, P. C. (2002). *Wireless Security: Threats, Models, Solutions.* New York City, NY: McGraw Hill.

Randall K. Nichols, D. (2018). Chapter 20 Acoustic CM & IFF Libraries V SWARMS Rev 1 05142019. In R. K. Nichols, H. C. Mumm, W. D. Lonstein, & J. S. Hood, *Unmanned Aircraft Systems (UAS) in the Cyber Domain: Protecting USA's Advanced Air Assets, 2nd ed.* Manhattan, KS: NPP Press.

Randall K. Nichols, D. (2019 for publication). Unmanned Aircraft Systems in the Cyber Domain: Protecting USA's Advanced Air Assets, 2nd ed. In H. M. Randall K. Nichols, *Chapter 18 Audiology, Acoustic Countermeasures against Swarms and Building IFF Libraries* (p. 2nd ed.). Manhattan, KS: For Publication, NPP.

Randall K. Nichols, J. J. (2018). *Unmanned Aircraft Systems (UAS) in* *the Cyber Domain: Protecting* USA's *Advanced Air Assets*. Manhattan, KS: New Prairie Press.

Rappaport, T. (2014). *Millimeter Wave Wireless Communications*. New York City, NY: Prentice Hall.

Ricker, D. (2017, July 1). *Navigating drone laws has become a growing and lucrative legal niche*. Retrieved from ABA Journal: http://www.abajournal.com/magazine/article/drone_law_attorneys

Said Emre Alper, Y. T. (December 2008). Compact Angular Rate Sensor System Using a Fully Decoupled Silicon-on-Glass MEMS Gyroscope. JOURNAL OF MICROELECTROMECHANICAL SYSTEMS, VOL. 17, NO. 6.

Sanchez, M. (2019, June 4). No *Drones*. Retrieved from Unspalsh.com: https://unsplash.com/photos/oMqswmrie4Y

Schroeder, A. (2018, February 1). *Localizing Humanitarian Drones: Robotics & Disaster Response from the Maldives to Malawi*. Retrieved from medium.com: https://medium.com/radiant-earth-insights/localizing-humanitarian-drones-robotics-disaster-response-from-the-maldives-to-malawi-a1f362432cb1

Signia. (2019, May 16). *Signia Hearing Aids*. Retrieved from Signia Hearing Aids – Hear across America: www.signiausa.com

Singer v. City of Newton, 284 F. Supp. 3d 125 (U.S. District Court Massachusetts September 21, 2017).

slideshare.net. (2019, May 16). *ProudParas/sound-waves-loudness-and-intensity, slide 12*. Retrieved from slideshare.net: https://www.slideshare.net/ProudParas/sound-waves-loudness-and-intensity

Sood A.K. & Enbody, R. (2014, December 19). *https://www.georgetownjournalofinternau-s-military-defense-systems-the-anatomy-of-cyber-espionage-by-chinese-hackers*. Retrieved from georgetownjournalofinternationalaffairs.org/online-edition: https://www.georgetownjournalofinternationalaffairs.org/online-edition/u-s-military-defense-systems-the-anatomy-of-cyber-espionage-by-chinese-hackers

Sovereignty and use of airspace, 49 U.S. Code §40103 (United States Congress July 5, 1994).

Staff. (2008). FINAL ACTS WRC-07. *World Radiocommunication Conference*. Geneva: ITU.

Staff. (2012). FINAL ACTS WRC-12. *World Radiocommunication Conference*. Geneva: ITU.

Staff. (2016, April 17). *Equal Loudness Contours*. Retrieved from Gutenberg Organization: http://central.gutenberg.org/article/WHEBN0001046687/Equal-loudness%20contour

Staff. (2019). FINAL ACTS WRC-15. *World Radiocommunication Conference*. Geneva.

Staff. (2019, May 6). *wikipedia.org/wiki/Doppler_effect*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Doppler_effect

Staff, W. (2019, May 04). 5G. Retrieved from Wikipedia: www.wikipedia.org

Stone, Z. (2007, 11 7). *Stone, Z. (2017). Everything You Need To Know About Sophia, The World's First Robot Citizen. Retrieved from https://www.forbes.everything-you-need-to-know-about-sophia-the-worlds-first-robot-citizen.* Retrieved from Forbes: https://www.forbes.com/sites/zarastone/2017/11/07/everything-you-need-to-know-about-sophia-the-worlds-first-robot-citizen/#1667784246fa

Studios, D. D. (2017). Boaters Ref. USA.

sUAS News. (2018, March 2). *RAS Consulting & Investigations hire Jeff Parisse to offer sophisticated UAS security and surveillance services*. Retrieved from suasnews.com: https://www.suasnews.com/2018/03/ras-consulting-investigations-hire-jeff-parisse-offer-sophisticated-uas-security-surveillance-services/

Sun, W. M. (June 2015). Unmanned Aircraft Systems:Air-Ground Channel Characterization for future applications. *IEEE Vehic. Tech Mag. Vol 10, No 2* , pp. 79-85.

T.C. Dozer, D. A. (2008). High Altitude Platforms for VHDR in-theater communications. *IET Seminar on Military Satellite Communications Systems*.

The Shepard News Team. (2018, September 12). *Liteye Receives Follow-on Contract for C-AUDS – DB – Digital Battlespace.* Retrieved from Aerospace, Defense and Security News and Analysis – Shephard Media, The Shepard Press, Ltd: www.shephardmedia.com/news/digidigital-battlespace/liteye-receives-follow-contract-c-auds

Toomay, J. (1982). *RADAR for the Non – Specialist. London; Lifetime Learning Publications.* London: Lifetime Learning Publications.

TRS, S. (2018, July 10). *Tontechnic-Rechner-Sengpielaudio.* Retrieved from Tontechnic-Rechner-Sengpielaudio Calculator: www.sengspielaudio.com/calculator-wavelength.htm

UAV Coach. (2019, May 30). *Drone Laws in South Carolina* (2019). Retrieved from UAVcoach.com: https://uavcoach.com/drone-laws-south-carolina/

United States Constitution Article VI, Sec.2 (United States of America September 17, 1787).

Uni-wuppertal. (2019, May 15). *Inverse Square Law, General.* Retrieved from hydrogen.physik.uni-wuppertal.de/hyperphysics/: http://hydrogen.physik.uni-wuppertal.de/hyperphysics/hyperphysics/hbase/forces/isq.html

Urban, T. (2018). *Teach Your Robots Well: Will Self-Taught Robots Be the End of Us?* Retrieved from www.worldsciencefestival.com: Urban, T. (2018). Teach Your Robots Well: Will Self-Taught Robots Be the End of Us? Retrieved from https://www.worldsciencefestival.com/programs/teach-robots-well-will-self-taught-robots-end-us/

Usenix.org. (2019, 6 9). *MEMS, Drones, & Sound Sourcing.* Retrieved from Usenix.org: www.usenix.org

WebFinance, Inc. (2019). *Definition of Ethics.* (2019*b*). online: Online: WebFinance, Inc.

Weise, E. (2017, August 23). *could-hackers-behind-u-s-navy-collisions.* Retrieved from USATODAY: https://www.ruidosonews.com/story/tech/news/2017/08/23/could-hackers-behind-u-s-navy-collisions/594107001/

Wiki-E. (2018, August 26). *Equal Loudness Contours.* Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Equal-loudness_contour

Wiki-L. (2018, August 27). *Laser*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Laser

Wikipedia. (2018, August 26). *Human Hearing Range*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Hearing_range

Wikipedia. (2019, May 6). *wikipedia.org/wiki/Doppler_effect*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Doppler_effect

Wong, C. (2017). *Top Canadian researcher says AI robots deserve human rights*. Retrieved from Wong, C. (2017). Top Canadian researcher says AI robots deserve human rights. Retrieveitbusiness.ca: Wong, C. (2017). Top Canadian researcher says AI robots deserve human rhttps://www.itbusiness.ca/news/top-canadian-researcher-says-ai-robots-deserve-human-rights/95730

Wordpress. (2012, 08 29). *The True Sign of Intelligence*. Retrieved from deepthinkings.wordpress.com: http://deepthinkings.wordpress.com/2012/08/29/the-true-sign-of-intelligence/

Wright, T. (2017, August 11). *You've Been Warned: Keep Your Drones Away From Military Bases*. Retrieved from Air & Space, Smithsonian: https://www.airspacemag.com/daily-planet/keep-your-drones-away-military-base-180964451/

Wyvern, T. (2018). *National Critical Intelligence Estimate: Counter Unmanned Aircraft Systems (C-UAS) in the US*. Salina, KS: KSUP.

Xiaoyang Liu, C. L. (2016). High Altitude Platform Station Network and Channel Modeling Performance Analysis. *Mathematics and Computer Science. Vol. 1, No 1*, pp. 10-16. doi:Xiaoyang Liu, Chao Liu, Wanping Liu, Xiaoping Zeng. High Altitude Platform Station Network and Channel Modeling Performance Analys10.11648/j.mcs.20160101.13

Zeng, R. Z. (May 2016.). Wireless communications with unmanned aerial vehicles: opportunities and challenges. *IEEE Communications Magazine.vol.* 54, *no*.5, pp. 36-42.

Yong Zeng, R. Z. (2016). Wireless Communications with Unmanned Aerial Vehicles: Opportunities and Challenges. *IEEE Communications Magazine*, 36-42.

Yunmonk Son, H. S. (2015, August 12-14). Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors. *Proc. 24th Usenix Security Symposium.* Washington, DC: USENIX. Retrieved from https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/son

Zetter, K. (2015). So, The NSA Has An Actual SKYNET Program . *WIRED Magazine(Online).* . Retrieved from Zetter, K. (2015). So, The NSA Has An Actual SKYNET Program WIRED Magazine(Online).

[1] FM 34-40-7

Table of Contents

BACKBONE- TOC

Chapter 2: Understanding C-UAS Purpose and Process [Carter]

Chapter 3: Developing a C-UAS Strategy, Goals, Options, Target Analysis, Process Selection, Operational Metrics, Approaches to Countering UAS Activities (First Principles) [Mumm]

SECTION 4: Legal and Administrative Issues

Adamy, D. (2001). *EW 101 A First Course in Electronic Warfare*. Boston, MA: Artech House.

Barnes, D. E. (2019, September 23). *The Urgent Search for a Cyber Silver Bullet against Iran.* Retrieved from New York Times: https://www.nytimes.com/2019/09/23/world/middleeast/iran-cyberattack-us.html

Fazzini, K. (2019, September 22). *Saudi Aramco Attacks could Predict widespread cyber warfare from Iran.* Retrieved from CNBC: https://www.cnbc.com/2019/09/21/saudi-aramco-attacks-could-predict-cyber-warfare-from-iran.html

Gelfand, S. A. (2009). *Essentials of Audiology, 3rd Edition.* Stuttgart, DE: Thieme.

LRAD Corporation. (2019, October 18). *Product sheet LRADS 1000x.* Retrieved from LRAD Corporation : https://lradx.com/lrad_products/lrad-1000xi/

Nichols, R. K., Mumm, H. C., Lonstein, W. D., Ryan, J. J., & and Carter, C. (2018). *Unmanned Aircraft Systems (UAS) in the Cyber Domain: Protecting USA's Advanced Air Assets.* Manhattan, KS: New Prairie Press (NPP) eBooks. 21.

Nichols, R. K., Mumm, H. C., Lonstein, W. D., Ryan, J. J., Carter, C., & and Hood, J.-P. (2019). *Unmanned Aircraft Systems in the Cyber Domain.* Manhattan, KS: NPP eBooks. 27.

Nicole Gaouette, K. L. (2019, September 21). *US to send troops and air and missile defense to Saudi Arabia as Trump announces new Iran sanctions after oil attack.* Retrieved from CNN Politics: https://amp.cnn.com/cnn/2019/09/20/politics/trump-announces-iran-sanctions/index.html

Taghvaee, B. (2017, July 27). *Shahed 129 Heads Iran's Armed UAV Force.* Retrieved from Aviation Week & Space Technology: https://aviationweek.com/defense/shahed-129-heads-iran-s-armed-uav-force

Tucker, W. (2019, September 23). *Saudi Oil Facilities Attack has created International Risks.* Retrieved from Inhomelandsecurity.com: https://inhomelandsecurity.com/saudi-oil-facilities-attack-has-created-international-risks/

Table of Figures

BOOK SECTIONS / CHAPTERS

Chapter 5 Surveillance and Reconnaissance [Mumm]

Chapter 6 C-UAS Evolving Methods of Interdiction

SECTION 2 C-UAS TECHNOLOGIES AND OPERATIONS

Chapter 7 UAS Area / Airspace Denial [Hood]

Chapter 8 Emerging Interdiction Technologies [Hood]

Chapter 9 Non- Kinetic Military Avionics, EW, CW, DE, SCADA Defenses [Nichols]

SECTION 3 Counter C-UAS

Chapter 10 When the Other Side Fights Back – Cyberwarfare, Direct Energy Weapons, Acoustics, Integrating C-UAS into Planning [Nichols]

Chapter 11 Thinking Like the Enemy – Seams in the Zone [Lonstein]

Table of Tables

SECTION 1: Counter-UAS (C-UAS) Operations as a Concept

Chapter 1: The Role of Information Technology

SECTION 2: C-UAS Technologies and Processes

Chapter 4: Planning for Resiliency and Robustness

Chapter 5: Surveillance and Reconnaissance

Chapter 9: Non- Kinetic: Military Avionics, EW, CW, DE, SCADA Defenses

SECTION 3: Counter C-UAS

Chapter 10: When the Other Side Fights Back – Cyberwarfare, Direct Energy Weapons, Acoustics, Integrating C-UAS into Planning

SECTION 4: Legal and Administrative Issues

Chapter 12: C-UAS Regulation, Legislation & Litigation from A Global Perspective

Table of Equations

Chapter 9: Non- Kinetic: Military Avionics, EW, CW, DE, SCADA Defenses

Chapter 10:When the Other Side Fights Back – Cyberwarfare, Direct Energy Weapons, Acoustics, Integrating C-UAS into Planning

PART I

SECTION 1: COUNTER-UAS (C-UAS) OPERATIONS AS A CONCEPT

Chapter 1: The Role of Information Technology

J.J.C.H. RYAN

Student Learning Objectives:

After completing this block, the student will be able to use the conceptualization of an OODA loop in order to:

– describe the role of automated decisions in UAS operations

– analyze communications pathway weaknesses between UAS components

– identify points of attack in a notional UAS architecture

– explain types of sensing and how they are used to support decision making

–– ideate countermeasures to UAS operations

Introduction

In counter unmanned aerial systems (C-UAS) operations, there are basically just two ways to actually do something to counter the UAS activity: physically interfere with the system(s) or virtually interfere with the system(s). In this text, a wide variety of methods will be presented that employ one or both of these approaches. It is useful to have a structure upon which to consider those methods, which is why this chapter is first.

A UAS is, at its most abstract, an information processing system. Data is sensed, processed, shared, and communicated in order to control flight parameters (speed, altitude, etc.), internal sensors, external sensors, navigation, and mission execution. Data can be shared internally and externally, with other UASs, ground control elements, and computational backend systems. But this abstraction hides an incredible complexity of configuration. The various configurations of UASs range from stratospheric balloons (Loon LLC, 2020) (Sampson, 2019) to high altitude jets (AirForceTechnology.com, 2019) to hobbyist quadcopters (Fisher, 2020). Uses for UASs include surveillance, communications, weapons deployment, and entertainment. They exist in single system configurations, multiple element collaborations, and swarms. Simply put, the complexity and numbers of UAS configurations are legion. Therefore, it can be useful to abstract a construction of a UAS in order to have a way of discussing the issues without being bound by and constrained by implementation details.

In such an abstract description, a UAS consists of at least the following elements: a propulsion system, a control system, and a housing system. The propulsion system is what provides the mechanisms for flight and maneuver. The control system, which may be partially or completely autonomous, is what provides guidance to the UAS. The housing system is the physical structure that brings all components together to create a single operational UAS. A UAS may also include sensors, decision-making systems, communications systems, weapons, and defensive systems. Of all these components, only one may be bereft of information technology: the housing system. It follows, then, that understanding the role of IT in UAS operations is critical to understanding such mission-critical elements as targeting, effects, and execution of counter UAS activities.

Note that UAS operations could (and probably should) consider C-UAS actions prior to actual execution of a mission. In considering the potential C-UAS actions that a particular mission might encounter, the operators of a UAS might engage in counter C-UAS (CC-UAS) activities. These might include mission planning to avoid C-UAS capabilities, hardening of systems to resist C-UAS actions, and engaging in deception activities to confuse or deny C-UAS action effects. Simply put, considering how adversaries might try to disrupt and deny mission execution gives operators the opportunity to plan ways to subvert those adversarial activities. Thus, a mission planner needs to not only plan how to execute the mission but also to how to mitigate the actions that an adversary will take to thwart the mission. From the other perspective, a C-UAS operator must consider that an adversary might anticipate the C-UAS actions and have prepared alternatives and defenses. Whether you are Blue or Red in this scenario, the other side gets a vote.

The following Table 1-1 is a simple exploration of how UAS, C-UAS, and CC-UAS operations relate to each other. These are simply notional, are not intended to be a complete exposition, and are simply offered as a way to more easily integrate the concepts into a single operational construct.

Table 1-1 UAS, C-UAS and CC-UAS Operations Relationships

UAS operations	Counter-UAS operations	Counter Counter-UAS operations
Flight path	MIJI activities	redundant systems alternative flight paths
Surveillance	Dazzling Camouflage	Multiple types and numbers of sensors with different capabilities
Swarm coordination	Communications interference	Redundant channels

Source: Ryan, J.J.C.H (2020) Private Notes

When you think through these possibilities, it becomes clear that the potential for physical interference to UAS operations is limited: you can shoot down a UAS, but that's about it. But shooting down a UAS can be tricky, especially if the UAS is operating very remotely (like a stratospheric balloon) or in a swarm (where there are too many UAS to target individually). Plus, shooting down a UAS can deny the mission but is pretty darn obvious. A more subtle C-UAS operation might be to hijack the data feed or cause the UAS to operate in an area slightly different from the goal target. So, the real target may very well be the information systems embedded in a UAS.

Disrupting the Decision Cycles

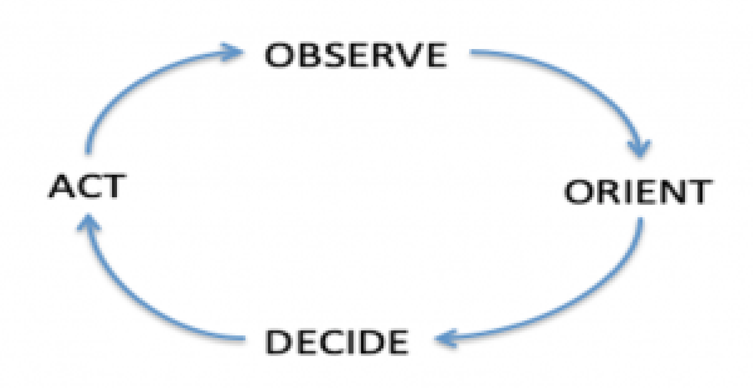
To oversimplify significantly, the importance of embedded information processing technologies is to support and enhance decision-making capability. Should the UAS change course? Does the UAS have enough fuel to get home? If not, what should happen? Is the UAS about to fly into a tree? The entire flight of a UAS, whether alone or in a swarm, is filled with the need to make and execute decisions.

The point of integrating advanced information technologies into UASs is to speed up the ability to make and execute appropriate decisions. Those two phrases: "make and execute" and "appropriate" are critical to understanding the problem space. "Make and execute" imply data input to a decision-making system, data output from such a decision-making system, and a triggering mechanism for a decision acting element. "Appropriate" implies that the decision and triggering processes have been thoroughly tested to comply with the rules of engagement and the policies that exist for the mission profile. These are decision cycles: a decision made based on input, action is done based on the decision, and a reassessment of the situation is performed to see if further action is needed. Rinse and repeat, as needed.

The point of attacking information technologies in UASs is to disrupt or deceive the decision cycle, for one or more purpose. Therefore, it is useful to have a short discussion on conceptualizing decision cycles. There are many different ways to conceptualize how decisions are formed, but one that has currency and broad based acceptance is the OODA Loop, first conceptualized by John Boyd (Richards, 2012) and updated by many, including Julie Ryan in 1996 (Nichols, Ryan, & Ryan, 2000). There have been many other contributors to the nuanced application of the OODA Loop as well, including criticisms (Forsling, 2018). The point is that the useful but only as far as the nuanced application of it allows. Further, the model was developed in a time when decisions were definitely restricted to the human brain, hence the development of OODA 2.0 (Nichols, Ryan, & Ryan, 2000, pp. 477-488). Both versions of the model are useful in planning C-UAS activities. See Figure 1-1.

The original OODA Loop is normally simplified to a simple loop that encompasses four steps connected with arrows. The four steps comprise a decision cycle. The first step is to observe what is going on. The second step is to orient those observations within the context of the environment and activities. The third step is to create candidate decisions based on the observations, the orientation, and mission. The fourth step is to act on the decision(s) that are deemed appropriate. Finally, the cycle repeats as needed. The following diagram depicts the OODA Loop as normally drawn:

Figure 1-1: Simplified OODA Loop



Source: (Richards, 2012)

The literature is clear to point out, however, that the OODA conceptualized by Boyd was much more nuanced, considering the role of feedback, mental biases, and experience level throughout the entire model. Figure 1-2, taken from (Richards, 2012), shows the version of the OODA drawn by Boyd:

Figure 1-2: Boyd's Drawing of the OODA Loop

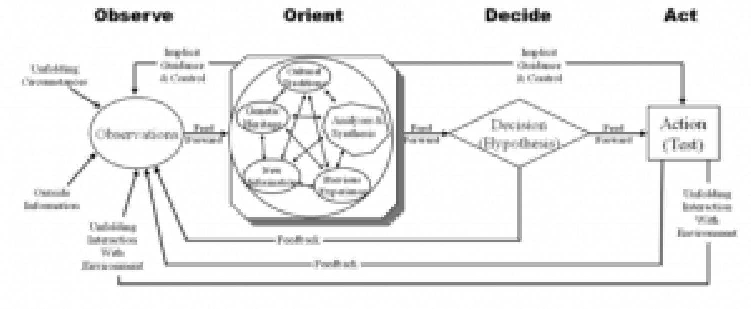


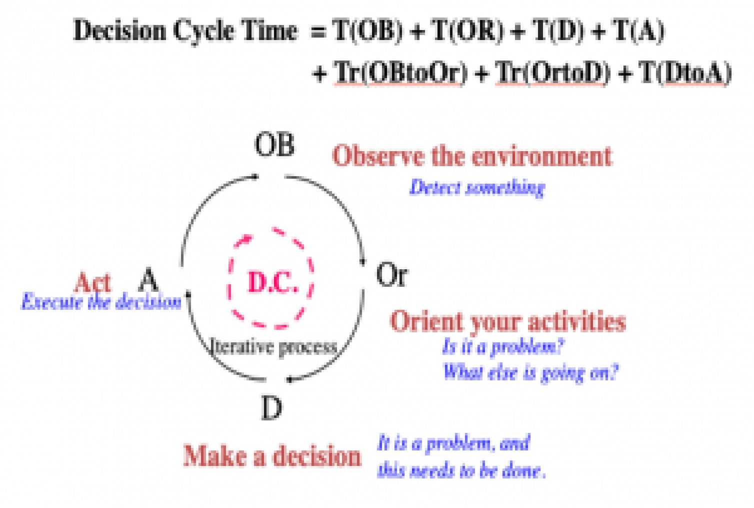
Figure 2. The only OODA "loop" that Boyd actually drew.

Source: (Richards, 2012)

Both versions of the OODA Loop capture the essence of the process, in that a decision is made as a result of observing something in the environment that can be characterized (oriented) as something worth acting upon.

An interesting way of conceiving of this process includes layering time over the various steps. Using the simplistic version, simply to control the resultant complexity of the diagram, one can conceive that there are hard physical limits to each step of the process. Hard physical limits derive from the speed of light, the speed of neural transmission, the speed of thought conversion from sight to context, and the speed at which cognition occurs. These hard-physical limits, when characterized in scenarios, describe the ultimate maximum speed at which any decision cycle can occur. Figure 1-3 shows the simple version of the OODA Loop with such time overlays.

Figure 1-3: Time Elements of the OODA Loop



Source: (Ryan, Lecture Notes, EMSE 218/6540/6537, 1997)

The time elements shown include the times required to execute any of the given steps (T) plus the time to transition between steps (Tr). When the laws of physics and neurobiology have been pushed to their limits, there is a hard stop as to how fast this cycle can be executed.

Effective management of any situation depends on making decisions, typically with less than perfect data. Waiting for perfect data is a recipe for being last in the race to action but jumping into action with data that is imperfect is risky. When the potential impacts of a decision are low, then the pressure to be absolutely correct is reduced. When the impacts of a decision are high, including perhaps causing death or committing an act of war, then the requirement for better data is concomitantly high.

On the other hand, the faster a decision is made, and the necessary action executed, the faster the results occur. Fast, effective, and appropriate decisions depend on experience, education, and supporting capabilities. When a decision is needed very quickly, automation of some or many components of the system is a must.

Advanced information technology allows us to “cheat”, as it were. Incorporating advanced processing and automated reasoning enables a rethinking of this abstraction. Consider: what if all possible flight paths, potentials scenarios, and problem sets were modeled prior to any need for a decision to be made? Would that change the need for observation? What if all possible decisions based on all possible scenarios were categorized and stored prior to the mission? Would that change the need for real-time analysis of potential courses of action?

The answer is, of course: yes. This technology enhanced decision cycle can be modeled as OODA Loop 2.0, which isn’t actually an OODA loop at all but an ODAO Loop. Figure 1-4 shows the modified OODA Loop 2.0, with some technology suggestions associated with each step.

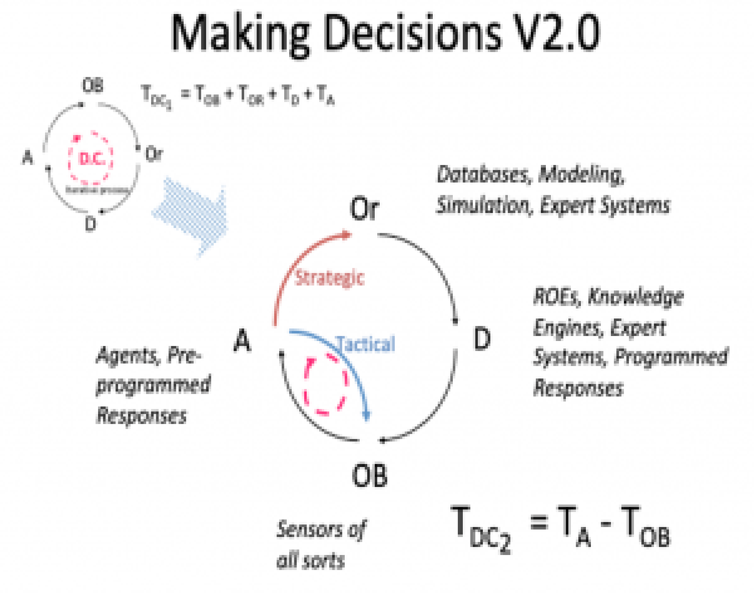
In this OODA 2.0 variation, preliminary preparation using databases, modeling, simulations, and expert systems provide a rich backdrop to the potential mission, allowing strategists to work with tacticians to flesh out the potential variations that the mission can involve. Based on these comprehensive analyses, a set of decisions can be predetermined, not unlike the decisions that are programmed into autonomous vehicles of all sorts. Decision parameters, such as values, rules of engagement, and geopolitical considerations, are integrated with expert systems in order to create a rich environment of allowable decisions responses under certain conditions. Note that the conditions must be completely describable as well: that is necessary in order to characterize the observables that comprise the triggering actions. Those set of activities with those types of technologies create the Orient and Decide phases of the OODA 2.0.

When those are completed, a system instrumented with sufficient sensors and actuated elements can wait for the conditions to be met that trigger a decision. The decision is triggered automatically, which causes the preprogrammed actions to be taken, and then the system goes back to observing. When considering this variation, it is useful to point out that the OODA 2.0 includes not one but two decision cycles: a tactical decision cycle and a strategic decision cycle. Both are critically important to the speed of operations, and both are points of vulnerability. Feedback is provided in two ways: strategically to the expert systems that model potential outcomes and inform decision options, and tactically to the observation sensors.

These decision cycles occur at the speed of computational processes and electronic communications, which is to say: very fast. There are two case studies that inform the design and use of systems employing the OODA 2.0 approach: the stock market crash of 1987 and the Vincennes tragedy of 1988.

The stock market crash of 1987 was the result of automated elements (bots) deployed in financial transaction systems to speed up the purchase or sale of assets in order to react to market conditions faster. In 1987, the number of bots had risen to the point that when the market moved in a certain direction, the bots reacted, as programmed, to buy or sell. These actions were detected and acted upon by other bots, which reacted in kind, and a feedback loop was created very quickly that led to wholesale selling. The humans, who were not in the decision loop, stepped in to stop the market and reassess the system architecture. (Kenton, 2019)

Figure 1-4: OODA Loop 2.0



Making Decisions V2.0
OB
A
Or
D
D.C.
$T_{DC_1} = T_{OB} + T_{OR} + T_D + T_A$
Databases, Modeling, Simulation, Expert Systems
Or
Strategic
ROEs, Knowledge Engines, Expert Systems, Programmed Responses
A
Tactical
D
Agents, Pre-programmed Responses
OB
Sensors of all sorts
$T_{DC_2} = T_A - T_{OB}$

Source: (Ryan, Security Challenges in Network-Centric Warfare, 2001)

The Vincennes tragedy of 1988 was a result of an automated system on a warship mistaking an Iranian airliner for an incoming attack: the warship's systems automatically launched what was thought to be a defensive strike on the airliner. Hundreds of people died. (Halloran, 1988) The relationship between Iran and the US continues to be haunted by this very deadly mistake. (Gambrell, 2020)

These two cautious tales have the side effect of pointing out that any system using the OODA 2.0 approach is vulnerable to two attacks: the incitement of positive feedback loops, which may trigger undesirable decision states, and the enticement of data suggesting eminent danger, which may also trigger undesirable decision states. But these are not all of the opportunities that might be taken advantage of by a clever C-UAS planner. Using the OODA Loop analysis framework, both 1.0 and 2.0, can assist a planner in identifying many such opportunities to subvert, deny, or disrupt UAS missions by focusing on the information systems that enable the UAS operations.

Conceptualizing the Information Systems in UASs

The UAS is a "box" propelled through the air, controlled through remote and onboard means, focused on conducting a mission. The mission can vary both in terms of geospatial coverage and in terms of active or passive interaction with the target. There are several truisms.

- 1) At the beginning of a mission and until some certain point (which may be quite soon after launch), there are usually active communications between the UAS and the ground control station. This time may be a short period of time, such as 2 minutes or less, or it may be for the entirety of the mission.
- 2) The UAS may have some capability to detect and avoid objects, so as to avoid mid-air collisions. This capability may be extremely rudimentary, or it may be quite sophisticated.
- 3) The UAS has a propulsion system that provides adequate power to move in the manner it is intended to move. Control of this propulsion system may be through artificial intelligence, as in the case of the Alphabet Project Loon (Loon LLC, 2020), or they may be controlled through remote pilotage.
- 4) The UAS may have some capability to navigate autonomously or semi-autonomously. In relatively simple systems, like balloons, this may involve means to change altitude. In more complex guided systems, this means that it may be able to simply fly to an emergency landing field when certain circumstances arise. In other systems, this means that there is an onboard computer system dedicated to navigation that controls the flight of the system when released from active external control (whether ground or air based) and

continues that control until commanded to return to base or resume responding to external control.

- 5) The UAS may have some capability to sense its surroundings. This may be rudimentary radar sensing, it may be optical sensing, or it may be multispectral sensing. The interpretation of the sensed data may be computed on board, either partially or completely, or may be computed off-board, perhaps with derived data returned to the system for action.
- 6) The UAS may have some capability for action, depending on the mission. This may include deploying decoys, munitions, or taking evasive action. The capability for action may be initiated remotely or may be autonomous, in which case a decision support system must be onboard.

These capabilities require computational systems and communications. And all of these may be targets for C-UAS activities. So, let's take a look at the information systems in a conceptual UAS.

Internal

A UAS can't fly (very far) if it doesn't have internal systems to parse received instructions, make decisions based on sensed data, and control its onboard systems in a UAS. The internal systems can be thought of as the internal nervous system of a UAS. Sensed data is collected and may possibly undergo some preprocessing, prior to being transferred to a decision support system, a suite of AI support elements, or external communications for relay to other UASs and/or command and control elements, such as an airborne control system or a ground control system. The internal systems interpret and instruct navigational control, mission execution, and propulsion control. When emergency situations occur, the internal systems execute preprogrammed options, which could include autonomously navigating to safe zones or self-destructing. The internal systems also monitor the health and welfare of the UAS according to the instrumentation included onboard. This may include fuel level monitoring, damage assessment, and interference detection. According to design, the internal systems may relay information continuously, on schedule, or in emergencies.

Any successful attack on internal systems could affect mission execution. Internal systems could potentially be attacked in many different manners, many of which will be discussed in the following chapters. But for the time being, consider these two obvious options:

- Electronic beam attack, where the strength of the focused energy disrupts or disables the electronic components of the internal systems. For example, a powerful beam may overwhelm delicate circuits, rendering them inoperable.
- Malicious software (malware) injection using channels of communication to the UAS, or activation where the malware has been included in components of the UAS before launch and triggered by operational parameters.

In order to *a priori* protect against such activities, a UAS designer would need to consider the potential for these types of attacks and design in protections that mitigate the possibilities of such attacks being successful. For instance, the design architecture could include using hardened chips that are resistant to an electronic beam attack or incorporating a Faraday Cage into the design of the housing system to protect vulnerable electronics.

Boundary systems

Boundary systems are those systems that exist on the boundary of the UAS. These include any sensors, such as air pressure, altitude, navigation aids, and mission specific sensors, as well as external communications elements, such as antennae. These are elements that interface between the external conditions in which the UAS is operating and the internal systems.

A successful attack on boundary systems can subvert the entire UAS mission. Designing protections for these systems is tricky, though, since by definition they need to be on the boundary of the physical system in order to operate. Because some missions may be dependent on ground-based data processing backend systems, the compromise of data transfer systems may result in a mission abort. Similarly, if external sensors are compromised, the ability for a UAS to operate safely could be undermined.

Examples of boundary systems include:

- Passive sensors, which receive data without stimulating the environment. These include cameras and navigation aids.
- Active sensors, which stimulate the environment in order to collect data. These include radar and lidar systems.
- Communications system components, such as receivers and transmitters. These include data communications systems and automated identification transponders.

External

External information systems are those that are wholly or partially contained in one or more systems external to the UAS. These may include data servers, control systems, mission execution support systems, or backend processors. Because these elements are external to the UAS, there are two points of vulnerability: the external system itself and the communications pathway between the external system and the UAS.

External systems may include:

- Active mission control, for part or all of a mission. The external elements may include systems tracking many UAS missions as well as navigation assistance.
- Data processing systems to support big data analysis, characterization, and integration.
- Data processing systems to support sensor data processing, interpretation, and application.

Understanding the potential for attack and defense on external systems is specific and dependent on the mission and uses.

How Complex information Technologies Are Used in UAS operations

Decision Support Systems

A decision support system (DSS) is an information technology system that supports the making of decisions concerning mission operations. The DSS requires a knowledge base of facts and rules relevant to the mission. In support of mission planning, a DSS may use models or analytic methods to review and evaluate alternatives. During the mission a DSS may assist the controllers with decisions concerning options for mission execution, using the knowledge base together with sensor data from the UAS and perhaps other current intelligence.

Expert Systems

Expert systems are information technology systems that emulate decision-making by human experts. In a UAS, such systems can make decisions even when communications to mission controllers is not available. An on-board expert system requires access to an appropriate knowledge base of facts about the mission and rules that apply to the mission under various contingencies. The system must have an inference engine capable of applying the rules to facts about the status of on-board systems and sensor data, as well as mission plans and rules, to make decisions regarding continuing operations. For example, if communications is lost with mission controllers, the expert system may take control and direct the UAS to a contingency holding area or landing field.

AI

What is “artificial intelligence” or AI? This is a subject of much debate, even today. The various definitions that have been offered range from a full replication of generalized intelligence (as defined by sensing and reacting to internal and external stimuli of both expected and unexpected nature), an ability to mimic human behavior, an ability to execute specific complex tasks (such as sensory aspects of biological life, including smell, hearing, vision, and touch), and being able to detect patterns in complex data from multiple sources in order to make correct decisions (such as identifying a terrorist in a crowd of people). These are just a few of the types of definitions that have been offered, but they provide a view into the breadth of the contribution for AI in every aspect.

The types of AI are variously referred to as belonging to "strong" or "weak" classes of AI. Strong AI implementations are, as one might imagine, more towards the fully generalized and autonomous types of intelligences. A classic test of a strong AI system is the Turing test, in which an AI is tested as a black box to see if a human can figure out if the system is an actual person or a machine. There are other, more nuanced, tests as well, but this gives you the sense of strong AI. (Huang, 2006) Weak AI is not, in fact, weak, but simply limited by design. Artificial vision, for example, can be considered weak AI. Advanced decision support systems (DSSs) can also be considered weak AI (James, 2019).

Why devote some time to AI in a C-UAS book? Advanced information technology, including all forms of AI, is very important to both UAS and C-UAS operations. Consider: humans are bad at several activities that are critical to UAS operations. Augmenting or replacing humans as decision makers, actuators, or monitors of elements of UAS missions is an important application of technology.

One of the things in which humans have limited capability is multi-tasking: humans have severe limitations in their ability to do more than one thing at a time. Even people who think they are good at multi-tasking are demonstrably not so when tested. (Miller, 2017) This limitation means that an operator, when trying to keep track of many UAS operations and support activities, is very likely to either miss or delay reaction to a problem. The use of specialized AI frees up people to focus on one thing at a time.

Another problem with humans is that they get bored. When bored, their attention wanders, they daydream, and they zone out. Maybe even fall asleep. Also, when they get bored, they make mistakes.

Further, humans are slow to react. Very slow, compared to automation. What counts as fast for a human is a few minutes. Very fast is a few seconds. For automation, fast can be a few milliseconds and very fast can be a few nanoseconds. In the OODA Loop 2.0 (Nichols, Ryan, & Ryan, 2000, pp. 468-489) world, speed matters, a lot. Harnessing the power of automation can mean the difference between success and failure. The speed issue comes into play in several different areas of UAS and C-UAS operations. First, UASs can fly very fast. Hypothetically, a UAS flying at 60 miles per hour can cover 1 mile in 1 minute. In 15 seconds, that UAS can fly 440 yards (1320 feet).

To put that distance in perspective, consider this analysis of human reaction times during an ordinary situation: driving a car.

Suppose a person is driving a car at 55 mph (80.67 feet/sec) during the day on a dry, level road. He sees a pedestrian and applies the brakes. What is the shortest stopping distance that can reasonably be expected? Total stopping distance consists of three components:

Reaction Distance. First. Suppose the reaction time is 1.5 seconds. This means that the car will travel 1.5 x80.67 or 120.9 feet before the brakes are even applied.

Brake Engagement Distance. Most reaction time studies consider the response completed at the moment the foot touches the brake pedal. However, brakes do not engage instantaneously. There is an additional time required for the pedal to depress and for the brakes to engage. This is variable and difficult to summarize in a single number because it depends on urgency and braking style. In an emergency, a reasonable estimate is .3 second, adding another 24.2 feet3.

Physical Force Distance. Once the brakes engage, the stopping distance is determined by physical forces ($D=S^2/(30*f)$ where S is mph) as 134.4 feet.

Total Stopping Distance = 120.9 ft + 24.2 ft + 134.4 ft = 279.5 ft (Green, 2013)

Simple arithmetic tells us that humans cannot keep up with detection and closure rates.

Suffice it to say, automation is needed to augment human actions. Sometimes it replaces the human entirely while other times it simply augments human capabilities. But it is incredibly valuable in all circumstance.

So, let's get back to the types of AI that can be used and what it means in terms of footprint, infrastructure, backend support, and vulnerabilities.

Strong AI, including full replication of generalized intelligence, is still a long way away from existing in a small form factor. While great strides have been made in creating intelligent-like capabilities, some scarily intelligent, the resultant systems are dependent on very large banks of backend processors for computational support so that the user-facing systems can be smaller. (Tozzi, 2019)

Replicating intelligence is actually pretty tricky. Ignoring the methods in which data is collected and transferred from outside a system to inside the system (analogous to human eyes perceiving objects and transmitting the information to the brain to be considered, classified, and integrated into the human's thought process), there are really interesting issues associated with developing a system capable of taking data and making sense of it. Part of the challenge is simply classifying the data as belonging to one type or another: is this a bird or a bear? Is it a duck or a goose? Is it a Canadian Goose or an Arctic Swan? And so on, with increasing detail and specificity.

Another part of the challenge is distinguishing truth from falsehood: is this data input truly representative of reality or is it a falsehood? Falsehoods can come from a variety of sources, including sincerely held beliefs. For AI systems that are collecting textual postings, such as from sources like books, tweets, and newspapers, distinguishing truth can be extremely tricky. This is one of the challenges that Watson, the IBM system, has had to confront in order to execute such things as participating in Jeopardy (Gray, 2017).

All this leads to the issue of training data. AI classifiers are developed, or trained, using data sets. By inserting false or misleading data into the training sets, it is possible to cause the AI to make mistakes when deployed in real world situations (Moisejevs, 2019) (Bursztein, 2018).

A less robust AI, with the ability to mimic human behavior, an ability to execute specific complex tasks (such as sensory aspects of biological life, including smell, hearing, vision, and touch), can fit into a smaller form fit, depending on the function. One of the things most home users don't realize about voice recognition and interpretation systems, such as Siri, is that the voice interpretation and characterization does not occur on the handheld phone or the small speaker system. Instead, the data is collected and transmitted to backend processors, where the actual data crunching occurs (Goel, 2018). This distributed processing is necessary in order to bring the amount of computing power to bear that is needed to interpret all the various types of voices, circumstances, and commands, and even then, mistakes are made. There are examples of voice recognition systems that are fully functional on standalone home computer systems, such as Dragon Naturally Speaking (Nuance, 2020), but these work only because the first thing the user needs to do is to train the software to interpret the user's voice, including cadence, accent, and structure. Every year, these systems are getting more capable but there is still a fair amount of processing needed when more than one unique user is interfacing with the AI.

Systems that are trained to sense and interpret environmental elements may be limited by the technology used for sensing (Vincent, 2017). The examples of automated vehicles hitting pedestrians illustrates some of this challenge (Wakabayashi, 2018) (McCausland, 2019). It becomes even more problematic when complicated scenarios are envisioned, such as being able to detect patterns in complex data from multiple sources in order to make correct decisions (such as identifying a terrorist in a crowd of people) (Tarm, 2010).

It goes without saying that the increasing miniaturization of electronic components, the incorporation of alternatives to electronics, such as optics, and the development of special purpose processors have and continue to revolutionize the ability to squeeze capabilities into a small size form factor. Size reduction has a lot of advantages: it can mean lower power requirements, faster execution of computational cycles, and less heat generation. It can also have some inherent disadvantages, including less robust physical components. Protecting advanced microelectronics from directed energy attacks, for example, can require significantly increased shielding, which can in turn affect overall energy requirements for flight operations. In mission situations where energy efficiency and UAS maneuverability are important, tradeoffs need to be considered in overall system design. However, great strides have been made in both the development of specialized processors that execute AI-like capabilities and the integration of those processors on common chip sets. Integration of multiple special chips in a system can provide a marked improvement in on-board intelligence (Morgan, 2019).

The integration of advanced automation, including AI, into UAS architectures can be thought of as having several faces. First, decision support systems with pre-programmed rules of engagement can be embedded onboard the individual systems. Next, specialized AI processors can be included as well. Naturally, more complex AI and decision support solutions can be implemented that rely on backend (either terrestrial or airborne) processing for the heavy computational lifting. Finally, all of these can be integrated together.

The interesting thing about automated decision support systems is that all possible scenarios must have been considered by the human programmers who created the system. The scenario analysis allows the humans to catalog the potential decisions that must be made. In a trivial example, consider an automated water tap. There is a sensor that detects when something matching the profile of human hands is placed under the tap. The system is programmed to decide in those circumstances: if the profile of the detected object matches the profile loaded into the system, activate a switch that allows water to flow. When the sensor loses detection of that object, activate a switch that stops the water from flowing. All of that needs to be specifically programmed into the system: no decisions are possible without a priori structural design.

The same type of a priori structural design is needed for all autonomous decision systems, including and especially complex systems in complicated situations. For example, in an autonomous car, a scenario to consider might be that an old lady and a child run into the street in front of the car so suddenly that the car must (because of physics) hit one or the other of the people. The decision must be made which one to hit. In a strong AI system, the internal intelligence would process the data and make the decision based on internal logic. If the processing is sufficiently fast, the car would then execute the system's decision, taking out either the old lady or the child. In weak AI or a conventional decision support system, the system would simply execute the pre-programmed decisions embedded in the system. These decisions might take something like the following structures, depending on the programmer team considerations:

- if two objects block the path with insufficient time to avoid both,
- • hit the one to the right

The decision, of course, could have just as easily been:

- • hit the one to the left

OR

- • navigate between the objects

Alternatively, a more complex system might have the following type of logic path:

- if two objects block the path with insufficient time to avoid both,
- • characterize the identity of the objects
- •• are both objects members of a protected class?

If yes, hit the one to the right

If no, then:

- •• is one a member of protected class?

If yes, hit the other object

If no, then hit the one on the right

The point of this thought exercise is to illustrate that “independent thinking” by a machine is dependent on thinking done by programmers in designing the system.

Implications for C-UAS Operations

A UAS may have decision processes in place that impel the UAS to avoid hitting members of its swarm, deploy electronic countermeasures when certain threats are detected, or increase power when the rate of altitude change exceeds certain thresholds. Each of these decisions structures is necessary to support the semi- or fully autonomous aspects of the mission. Each of these decisions can provide an exploitable aspect for C-UAS activities. Understanding what the decision structure is provides the C-UAS mission planner with the opportunity to create situations that trigger certain decisions that can lead to desirable outcomes, like diverting the flight path of a swarm.

Similarly, if the UAS is dependent on backend processing to support decision processes, then denying the link between the UAS and the backend processes will have an obvious effect. A competent architect will have programmed in failsafe decisions in the event of a lost link – forcing this outcome may or may not be a desired outcome. Spoofing the link and replacing the authentic backend processing with alternative processing may be a more desirable outcome, if it can be accomplished (probably very difficult if possible, at all). A middle level attack, where the link is degraded to the point that the decision cycle slows down significantly can be the more desirable outcome, as it provides the C-UAS operator additional time to pursue the C-UAS mission objectives.

Bottom line: understanding the level and complexity of onboard intelligence is an important part of C-UAS planning.

How Sensing is Used to Support UAS Operations

Other elements of the UAS information processing architecture that are potential targets for C-UAS activities include the sensors. A UAS is blind and deaf without sensors interacting with the environment and providing data about the environment to the control systems. Sensors include thermometers, barometers, visual spectrum cameras, multispectral sensors, wind speed sensors, hydrometers, and as many other types of sensors as can be imagined. Some of these may provide data to external systems, such as navigation aids or intelligence data collection systems, while others may provide data solely for use by the UAS.

Each of these sensors should be considered as potential targets for C-UAS activities. Confusing sensors that support navigation may cause a UAS to failsafe into an automated return to base profile. Denying the intelligence data gathering sensors may not do much to the flight operations of the UAS but would degrade or deny the effectiveness of the mission. Finally, attacking the sensor systems though electronic means to physically degrade or destroy the actual sensing apparatus provides a more enduring effect that the adversary would have a harder time recovering from.

In summary, there are more options to C-UAS than simply shooting the systems out of the sky. Although that is always an option.

Summary

UAS operations are complex symphonies of activities of many operators, both automated and humans. Understanding and analyzing interfaces can provide the C-UAS mission planner with many opportunities for vulnerability exploitation. In reading through the rest of this book, think about how each element fits into a larger analysis.

Questions for Reflection

1. Diagram the likely coordination communications network for a UAS swarm. Identify potential points of compromise that would degrade the swarm activity.
2. Describe the probable effect of jamming the ground to UAS control link.
3. Explain the contribution that information technology makes to autonomous UAS operations.
4. Your side is in a tense geopolitical conflict where both sides are using UASs to surveil the situation. There is pressure to avoid escalating the conflict by engaging in overtly hostile actions. However, it is necessary to move some military forces in order to be better positioned to react in case the situation degrades. Movement secrecy is desired, which means that some means must be found to deny the adversary's surveillance capabilities while the move is taking place. The known capabilities of their UAS surveillance systems include radars and visual spectrum cameras with video capabilities. The data is collected onboard the UAS and uploaded to a high-altitude relay system, which sends it through other relays to the adversary intelligence data processing center. Your boss has asked you to come up with a C-UAS plan that is non-aggressive, but which provides cover for the force movement. What options can you provide for C-UAS activities in this scenario?
5. A spy has revealed that The Flaming Arrow terrorist group is planning on using UASs in a swarm formation, designed to

appear as a flying arrow, to deliver many small explosive devices to a key energy generation node. This node lies within a densely populated area that spreads out for 10 miles radius. There is a park one mile away from the targeted node. Once the UAS swarm is launched and released into autonomous mode, the explosives will be armed, with detonation occurring upon collision with some other object. The UASs to be used will be small, capable of flying 40 miles per hour for a distance of 5 miles while under load. There will be approximately 50 UASs in the swarm, flying approximately 50 feet above the ground. Each UAS has a basic decision support system onboard that allows fully autonomous mission execution once launched. Navigation is accomplished through image-based terrain feature recognition, where the visual data is collected through cameras and compared to onboard maps. The lead UAS establishes the route, but each of the UAS is capable of navigating independently. The spy has revealed the structure of the decision support system processes, which includes the following rule: if a swarm member to the right moves within 10 feet distance, move to the left until 10 feet separation is maintained. Your challenge is to design a C-UAS to cause the UAS system to divert to the park rather than hit the energy node. Keep in mind that you don't know where the launch point is, but you know it has to be somewhere within the flight parameter limitations. Also, keep in mind that destruction of any UAS will cause the bomb to detonate. Your goal is to minimize the damage and keep the bombs away from both the energy node and the populated areas.

References

AirForceTechnology.com. (2019, June 19). *The 10 longest range unmanned aerial vehicles* (UAVs). Retrieved January 7, 2020, from AirForceTechnology.com: https://www.airforce-technology.com/

features/featurethe-top-10-longest-range-unmanned-aerial-vehicles-uavs/

Bursztein, E. (2018, May 1). *Attacks against machine learning – an overview.* Retrieved January 29, 2020, from Blog: AI: https://elie.net/blog/ai/attacks-against-machine-learning-an-overview/

Coram, R. (2010). *Boyd: The Fighter Pilot Who Changed the Art of War.* New York: Hatchette Book Group.

Fisher, J. (2020, January 27). *The Best Drones for* 2020. Retrieved January 29, 202, from PC Magazine: https://www.pcmag.com/picks/the-best-drones

Forsling, C. (2018, July 30). *I'm So Sick of the* OODA *Loop*. Retrieved November 6, 2019, from Task and Purpose: https://taskandpurpose.com/case-against-ooda-loop

Gambrell, J. (2020, January 11). Crash may be grim echo of US downing of Iran flight in 1988. *Minnesota Star Tribune*, p. 1.

Goel, A. (2018, February 2). *How Does Siri Work? The Science Behind Siri.* Retrieved January 29, 2020, from Magoosh Data Science Blog: https://magoosh.com/data-science/siri-work-science-behind-siri/

Gray, R. (2017, March 1). *Lies, propaganda and fake news:* A *challenge for our age.* Retrieved January 29, 2020, from BBC Future: https://www.bbc.com/future/article/20170301-lies-propaganda-and-fake-news-a-grand-challenge-of-our-age

Green, M. (2013, January 1). *Driver Reaction Time.* Retrieved January 29, 2020, from Visual Expert: https://www.visualexpert.com/Resources/reactiontime.html

Halloran, R. (1988, July 4). The Downing of Fliight 655. *New York Times*, p. 1.

Huang, A. (2006, January 1). A *Holistic Approach to* AI. Retrieved January 29, 2020, from Ari Huang Research: https://www.ocf.berkeley.edu/~arihuang/academic/research/strongai3.html

James, R. (2019, October 30). *Understanding Strong vs. Weak* AI *in a New Light.* Retrieved January 4, 2020, from Becoming Human AI:

https://becominghuman.ai/understanding-strong-vs-weak-ai-in-a-new-light-890e4b09da02

Kenton, W. (2019, February 12). *Stock Market Crash of 1987*. Retrieved January 29, 202, from Investopedia: https://www.investopedia.com/terms/s/stock-market-crash-1987.asp

Loon LLC. (2020, January 1). *Loon.com*. Retrieved January 29, 2020, from Loon.com: https://loon.com

McCausland, P. (2019, November 9). *Self-driving Uber car that hit and killed woman did not recognize that pedestrians jaywalk*. Retrieved January 29, 2020, from NBC News: https://www.nbcnews.com/tech/tech-news/self-driving-uber-car-hit-killed-woman-did-not-recognize-n1079281

Miller, E. K. (2017, April 11). *Multitasking: Why Your Brain Can't Do It and What You Should Do About It*. Retrieved January 4, 2020, from Miller Files: https://radius.mit.edu/sites/default/files/images/Miller%20Multitasking%202017.pdf

Moisejevs, I. (2019, July 14). *Poisoning attacks on Machine Learning* . Retrieved January 29, 2020, from Towards Data Science: https://towardsdatascience.com/poisoning-attacks-on-machine-learning-1ff247c254db

Morgan, T. P. (2019, November 13). *INTEL THROWS DOWN AI GAUNTLET WITH NEURAL NETWORK CHIPS*. Retrieved January 29, 2020, from The Next Platform: https://www.nextplatform.com/2019/11/13/intel-throws-down-ai-gauntlet-with-neural-network-chips/

Nichols, R. K., Ryan, J. J., & Ryan, D. J. (2000). *Defending Your Digital Assets Against Hackers, Crackers, Spies, and Thieves*. New York: McGraw Hill.

Nuance. (2020, January 1). *Dragon Speech Recognition Solutions*. Retrieved January 29, 2020, from Nuance Products: https://www.nuance.com/dragon.html

Richards, C. (2012, March 21). *Boyd's OODA Loop: It's Not What You Think*. Retrieved July 27, 2019, from Fast Transients Files:

https://fasttransients.files.wordpress.com/2012/03/boydsrealooda_loop.pdf

Ryan, J. J. (1997, September 80). *Lecture Notes, EMSE 218/6540/6537.* (J. J. Ryan, Performer) George Washington University, Washington, DC, USA.

Ryan, J. J. (2001, November 12). *Security Challenges in Network-Centric Warfare.* (J. J. Ryan, Performer) George Washington University, Washington, DC, USA.

Sampson, B. (2019, February 20). *Stratospheric drone reaches new heights.* Retrieved January 5, 2020, from Aerospace Testing International: https://www.aerospacetestinginternational.com/features/stratospheric-drone-reaches-new-heights-with-operation-beyond-visual-line-of-sight.html

Tarm, M. (2010, January 8). *Mind-reading Systems Could Change Air Security* . Retrieved March 1, 2011, from The Aurora Sentinel: http://www.aurorasentinel.com/news/national/article_c618daa2-06df- 5391-8702-472af15e8b3e.html

Tozzi, C. (2019, October 16). *Is Cloud AI a Fad?* . Retrieved January 29, 2020, from ITPro Today: https://www.itprotoday.com/cloud-computing/cloud-ai-fad-shortcomings-cloud-artificial-intelligence

Vincent, J. (2017, April 12). *MAGIC AI: THESE ARE THE OPTICAL ILLUSIONS THAT TRICK, FOOL, AND FLUMMOX COMPUTERS.* Retrieved January 29, 2020, from The Verge: https://www.theverge.com/2017/4/12/15271874/ai-adversarial-images-fooling-attacks-artificial-intelligence

Wakabayashi, D. (2018, March 19). *Self-Driving Uber Car Kills Pedestrian in Arizona, Where Robots Roam.* Retrieved January 29, 2020, from New York Times: https://www.nytimes.com/2018/03/19/technology/uber-driverless-fatality.html

Wikipedia. (2019, December 29). *Loon LLC.* Retrieved January 14, 2020, from Wikipedia: https://en.wikipedia.org/wiki/Loon_LLC

Chapter 2: Understanding C-UAS Purpose and Process

CANDICE CARTER

Introduction

Drone technologies are evolving rapidly and, not surprisingly, counter-drone technologies are as well (Cole, 2019). The threat of UAS used by insurgents for surveillance or to delivery of hazardous payloads has increase

Each industrial revolution has included changes in the industrialization of warfare. An industrial revolution increases the killing power, mobility, and production of weapons along with the growing advancement of technology and population. The Fourth Industrial Revolution has not been different then predecessors, it continues to bring dramatic changes to how war is waged. The addition of space and cyber as domains of battle has made our world more complex than ever before. Unmanned Aircraft Systems (UAS) are unique, they can be used in all war domains (air, land, sea, space, and cyber) in single or multiplex scenarios. The threat of UAS is the strongest multi-domain battlefield weapon of our time. Countering this emerging threat requires strength in understanding how UAS is used for good and evil, the growing technological advancements of UAS, and the ability to predict how UAS will evolve in the future. The global market for C-UAS is to two billion dollars by 2024 (Global Aerospace Techology Network, 2019).

In terms of complexity of C-UAS, the size of UAS needs to be taken into consideration. Small UAS (sUAS) can be used in all war and domestic domains. The sUAS, can carry a deadly payload, be used to identify targets, confuse systems, and send critical target information. sUAS are ideal for asymmetric warfare with the characteristics of being stealth, pervading, and inexpensive. The complexity of sUAS as a multi-vector threat are endless, creating the largest challenge in the Counter Unmanned Aircraft Systems (C-UAS) industry. Larger UAS, while limited in threat vectors, has proven to be an asset in battle. Large UAS can also carry a deadly payload, be used to identify targets, confuse systems, and send critical information. However, they are predictable in execution of these capabilities. UAS can also be segmented into private, commercial, and military. These verticals have similarities and differences, however overall the common characteristic is they are a valid threat vector.

Figure 2-1: Flock of Drones in the Air

Source: (Ruff, 2017)

Driving forces for increasing the demand for C-UAS

UAS can be beneficial when used for good. However, to understand the need for C-UAS, the level of threat of UAS poses has to be considered. Low cost has makes UAS widely attainable at all levels of the population. The evolving risks of UAS used for evil, in the military theater and homeland. Outside the military theater, UAS can be used for attacks against critical infrastructure, terroristic attacks and target intelligence collection, and assist members of organized crime. Inside the military theater, small commercial UAS can transport critical surveillance data and explosives for a terrorist group. As far back as 2014, Daesh militants use DJI quadrotors for reconnaissance against Kurdish fighters (Defence iQ, 2019).

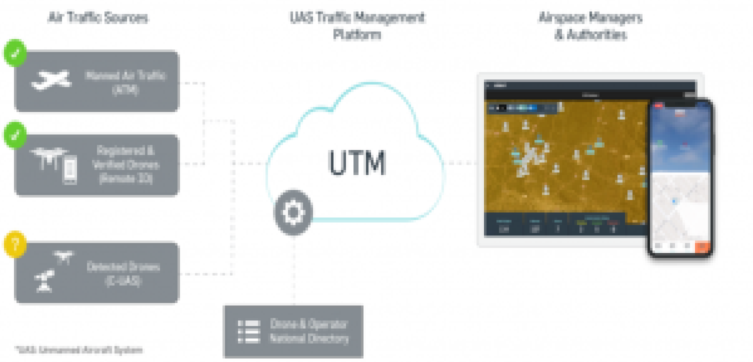
The traditional methods of interdiction serve as the base for the evolution of disruptive technologies needed to build an equal, eventually superior, countermeasure to rogue UAS. Currently when a threating UAS situation can be mitigated, the threat has been met with defense measures verses offensive countermeasures. Viable threats and attacks of UAS has limited the C-UAS space to just interception and detection of all sizes of UAS (Michel A. H., 2019). Predicting the threat of UAS is far from perfection, with the gap growing. Offensive security measures are ideal to have in place to be consistently successful in defeating threats. The progression of C-UAS technologies has the challenge of keeping up with the evolution of UAS, defensively and offensively.

C-UAS and the Fourth Industrial Revolution

The Fourth Industrial Revolution is characterized by an unprecedented speed, scale and scope of technological change, with governments around the world struggling to adapt their approaches to policy and regulation in the face of these transformations (World Economic Forum, 2018). The Fourth Industrial Revolution has not been different then predecessors, it continues to bring dramatic changes to how war is waged. The addition of space and cyber as domains of battle has made our world more complex than ever before. UAS are the airspace Unmanned Aircraft Systems (UAS) are unique, they can be used in all war domains (air, land, sea, space, and cyber) in single or multiplex scenarios. The threat of UAS is the strongest multi-domain battlefield weapon of our time. Countering this emerging threat requires strength in understanding how UAS is used for good and evil, the growing technological advancements of UAS, and the ability to predict how UAS will evolve in the future. The global market for C-UAS is to two billion dollars by 2024 (Global Aerospace Techology Network, 2019).

In December 2018, a commercial UAS became a threat at Gatwick Airport. With over sixty reports of UAS sightings near the runway, airplanes (a prior industrial revolution invention) were under possible attack from its next evolutionary competitor. The majority of modern airports are not prepared to respond to an UAS attack, nor prior to this global impacting incident, had not thought about UAS as a threat. Ben Marcus, Chairman of AirMap, recommends combining to an Unmanned Traffic Management (UTM) system with a C-UAS system to complete the airspace operation environment (Marcus, 2019). The integrated system, will supply information related to any aircraft detected by C-UAS is exchanged with the UTM system and remotely identified as either collaborative (registered) or non-collaborative, requiring intervention (Marcus, 2019). Gatwick is one event of an airport facing the threat of a rogue drone. Events of UAS threat have occurred globally including New York and Dubai. While UAS is widely recognized as part of the fourth industrial revolution, C-UAS needs to be acknowledged at all levels as part of the revolution in order to evolve at the rapid rate necessary to match the advancements of UAS. The use of one vector of C-UAS will not solve an issue, other disruptive technologies will have to be combined to thwart this fourth industrial revolution.

Figure 2-2: UTM and C-UAS


Air Traffic Sources
UAS Traffic Management Platform
Airspace Managers & Authorities
Manned Air Traffic (ATM)
Registered & Verified Drones (Remote ID)
Detected Drones (C-UAS)
UTM
Drone & Operator National Directory
*UAS: Unmanned Aircraft System

Source: (Image: AirMap) (Marcus, 2019)

Disruptive technologies that will innovate the future of C-UAS

A disruptive technology is one that provides a non- typical technological solution to simplify our everyday life. UAS can be considered one of the ultimate disruptive technologies of our time. UAS has been the most dynamic growth sector of the global aerospace industry in the last one decade. The present day UAS is an amalgamation of advances made in different domains of science and technology, such as composite materials, aerodynamics, communication systems, radars, propulsion systems, precision navigation systems, sensors, digital signal processing and so on (Sharma, 2017). These characteristics are true for C-UAS. When combining C-UAS with artificial intelligence (another disruptive technology), the ability to extend flights, identify and remember objects, and understand and collect intelligence.

The difficultly of tasks for C-UAS grows almost daily as technology continues to evolve at a rapid pace. At the time of this writing, the effort to keep ahead of the curve at times is overwhelming.

Proven, is the instability of using one type of technology for countering UAS. The traditional method of high-performance Radio Frequency (RF) is a thing of the past. Deaf drones or drones that do not follow the pattern of library of sounds for acoustic sensors demonstrate RF is not effective as a countering method. Another example is the combination of Electro-Optical systems (EO) with Infrared Sensor (IR) cannot successfully distinguish a bird from an airplane in broad daylight (Michel A. H., 2019). Thus, causing a great deal of false positives, rendering the detection unreliable and unusable. Detection technology must evolve to be able to properly identify the target UAS despite weather, time of day, and/or sound pollution. For example, at a large sporting event, the airspace may be crowded with legitimate aerial cinematography drones that do not pose a security risk (Michel A. H., 2019). In the military theater, C-UAS system that cannot tell the difference between allied and adversary unmanned aircraft could accidentally shoot down friendly drones (Michel A. H., 2019) Therefore, the C-UAS system will need to be able to read intent of the incoming UAS, forcing the need for the disruptive technology of Artificial Intelligence (AI).

Applying countermeasures also comes with legal implications. In the theater, peacetime verses wartime uses of C-UAS different policies apply by country law. The method of C-UAS could also be a factor in legality. If C-UAS is used as a matter of public safety versus military engagement. Could innocent human life being at risk outweigh a defensive measure?

The Need for Innovation of C-UAS

In 2016, commercial UAS new developments included waterproofing, robotic arms, and functionality to remotely control the UAS from mobile device. There was the introduction of a pocket size drone that could identify an object, remember it for tracking at a later time. Today. commercial UAS technology has developed to include sense and avoid capability, artificial intelligence to learn patterns from collected data and run pre-programmed flight path.

In 2020, commercial drones will have sharper picture/video quality, greater storage, longer flight time, all packed into a device that is smaller than an iPhone.

Military C-UAS has traditionally focused on RF and GPS. Future military C-UAS will need to address speed, ease of installation, precision detection, ease of mobility and versatility (large/small UAS, swarms, etc.) Military C-UAS have focused on defending against large UAS verses sUAS.

With the rapid innovation and use of commercial UAS, C-UAS needs to not only match but exceed functionality to be a successful combatant. The ideal future C-UAS will use artificial intelligence (AI) algorithms that automate the detection, identification, locating, and tracking of drones with minimal false detections, and directed energy weapons that can mitigate multiple drones quickly and/or simultaneously (Global Aerospace Techology Network, 2019).

There is a need integrate multiple technologies to combat the multiply vectors of attack; for example, anti-swarm, complex tracking, signal jamming, ability to be cellular controlled and operate in a congested air traffic area. The commercial user community would like the future C-UAS have functionality to locate drone operators and operate on open architecture software that allows for integration into existing security systems (Global Aerospace Technology Network, 2019).

Figure 2-3: Black Sage UASX-L3 Automatic Drone Disruptor

Source: (Black Sage, n.d.)

The Black Sage C-UAS, UASX-L3 Automatic Drone Disruptor, is leading the market with functionality. The UASX-L3 detects, tracks, identifies and disrupts UAVs using a new type of doppler Compact Surveillance Radar (CSR), artificial intelligence and long-range video tracking and RF jamming components (Black Sage, n.d.). Black Sage was recently acquired by Acorn Growth Companies, a private equity firm. This could impact the advancement and direction of Black Sage. Other C-UAS start-up companies in Silicon Valley have felt backlash in the form of protests and code deletion, based on political and ethical beliefs of the employees.

UAS and C-UAS Qualify as the New Global Arms Race

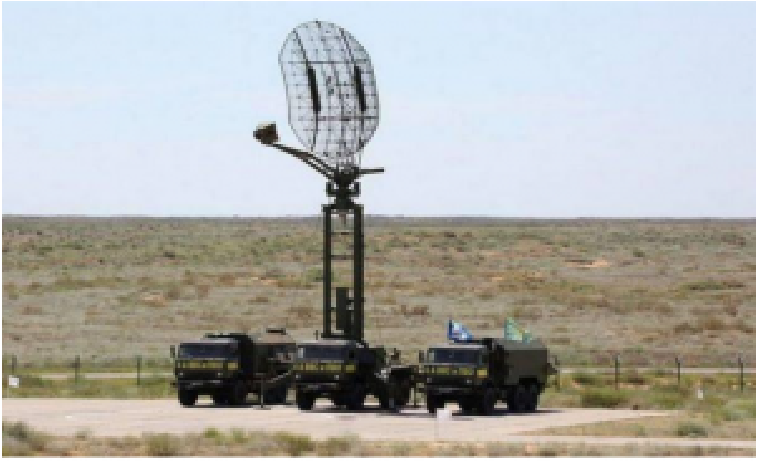
At the end of World War II marked the beginning of the arms race between the U.S., Russia, and respected allies to build the best nuclear warfare program in the world. Starting in 1987, countries came together and through a series of treaties and initiatives the global superpowers and their allies agreed to take steps to limit and stop the creation of nuclear missiles and cap military wartime inventory. For thirteen years, Russia and the U.S. did not change their approach. Suspicions let to cracks in agreements, and slowly the effort to control arms has crumbled. The new arms race is not between two nation-states, it is become a global race among larger players that threaten not only each other but are all face a common unpredictable threat of terrorism.

Russia has developed a comprehensive strategy for using UAS in warfare. The Russian military perceives this strategic approach foremost as "no-contact warfare", described as a war where Russian military can defeat a hostile state without the engagement of regular Russian forces (Sharma, 2017). February 2019, the anti-drone forces development by Russia released their first mobile units, part of the radio engineering forces armed with the "Kasta 2-2″ radar and an automated air defense control system (ACS) (Bendett, 2019). Kasta 2-2 uses landscape features combined with the ability to monitor objects that fly at a low altitude with little false positives.

Russia's "Silok" C-UAS can debilitate the control channels, communications, and telemetry of sUAS. Another Russian C-UAS solution, created by the Sozvezdiye Group, is a radio electronic system based on artificial intelligence to fight illegal drones (Bendett, 2019). This C-UAS learns10,000-20,000 standard situations to produce selective impacts on objects. Enabling this C-UAS to make 'friend or foe' decisions based on an array of signs, situations and the object's behavioral characteristics (Bendett, 2019).

Currently the U.S. Air Force is embarking on a year of testing and training of High Energy Laser Weapon Systems (HELWS) supplied by Raytheon. According to Raytheon's website, HELWS is an open architecture laser weapon system that can work on land, in the air and at sea, providing 360-degree coverage (Raytheon, 2019). In addition, the U.S. Air Force is testing Lockheed Martin's Advanced Test High Energy Asset (ATHENA), an anti-drone laser. ATHENA has the capability to shoot down multiple fixed wing and rotary drones. Raytheon's defense customers are "likening drones to the improvised explosive device (IED) situation 20 years ago, when we saw an adversary take a readily available technology and weaponize it in a low-cost way," says Todd Probert, vice president of Raytheon Intelligence, Information, and Services (Dulles, Virginia) (Cole, 2019).

Figure 2-4: Russia's Kasta 2-2



Source: (Bendett, 2019)

Figure 2-5: U.S. High Energy Laser Weapon Systems (HELWS)

Source: (Raytheon, 2019)

The Italian company, IDA Ingegneria Dei Sistemi, has created a military grade system, NO-DRONE. The system has been tested in China and in North America. NO-DRONE has been released in North America by a third party, 34 North Drones, for all government and civilian protection applications. NO-DRONE uses EMP, powerful multiband jamming, GPS spoofing or live fire systems to disable, redirect or destroy threats (UAS Weekly, 2019) Italy is not the only smaller country exploring C-UAS. Singapore's ST Engineering Electronics Ltd. sells a 6.6-pound radar gun powered by a 24-pound battery backpack that can jam a drone's GPS signal and disrupt the radio link to its operator (Wall, 2019). Diehl Defense has a fire electronic laser that has a range of more than 0.6 miles and also comes in a smaller, civil version with about half that range (Wall, 2019).

Figure 2-6: IDS NO-DRONE

Source: (UAS Weekly, 2019)

China Central Television reported in September 2019, China Aerospace Science and Industry Corporation (CASIC) has developed a counter-drone system consisting of multiple weapons and equipment, including land-based rockets and drone-hunting drones that can shoot huge webs and vehicle-based detection devices (Chan, 2019). In 2018, at the China Airshow CASIC showcased a vehicle-based laser weapon called LW-30, which could use a directional-emission high-energy laser to quickly intercept many kinds of aerial targets (Chan, 2019). Early in 2018, in Abu Dhabi, the Chinese “Silent Hunter”, the portable drone killing laser, can shoot from 2.3 miles (Military Aerospace Electronics, 2018). Chinese state-owned Poly Technologies Inc. has a truck mounted drone downing laser with range of up to 4 kilometers.

Figure 2-7: China’s LW-30

Source: (Chan, 2019)

Conclusions

The rapidly growing industry of C-UAS is a needed force to combat rogue UAS activity. C-UAS are used to locate, track and neutralize unwelcomed UAS. The growing need for C-UAS spans from the commercial to the military space, since the threat of unidentified UAS in the civil and military theater increases. The is not an international standard for the design of C-UAS and not all C-UAS systems work as advertised. Along with evolving C-UAS technology, global standards and policies will need to be developed. But make no bones about it, the need is being addressed. From jamming rifles to ground installations that fire nets, a new report lays out the expansive Wild West of anti-drone tech entitled: "*Report on 537 Anti-Drone Systems Shows How Wild the Market Has Become.*" (Gault, 2019) Bard University also has addressed the Counter Drone Systems 2nd Edition. (Michel A. H., 2019)[1]

References

Bendett, S. (2019). *Updates on Russian CUAS Capabilities and Rising SUAS Capabilities.* Arlington: CNA Analysis and Solutions.

Black Sage. (n.d.). *Black Sage Technology C-UAS* . Retrieved from Black Sage Technology : https://www.blacksagetech.com

Chan, D. (2019, September 16). *Asia Times*. Retrieved from Asia Times China Digest: https://www.asiatimes.com/2019/09/article/china-has-systems-to-counter-drone-attacks-source/

Cole, S. (2019, November 16). *Military Embedded Systems*. Retrieved from Military Embedded Systems Unmanned Systems: http://mil-embedded.com/articles/counter-drone-technologies-are-evolving-to-counter-countermeasures/

Defence iQ. (2019). *Counter UAS Efforts*. Retrieved from Defence iQ: https://www.defenceiq.com/events-counteruas/downloads/counter-uas-efforts-an-interactive-timeline?-ty-m

Gault, M. (2019, December 13). *Report-on-537-anti-drone-systems-shows-how-wild-the-market-has-become*. Retrieved from www.vice.com: https://www.vice.com/en_us/article/z3bb59/report-on-537-anti-drone-systems-shows-how-wild-the-market-has-become

Global Aerospace Techology Network. (2019, October 25). *Unmanned Intelligent Aerospace*. Retrieved from Intelligent Aerospace: https://www.intelligent-aerospace.com/unmanned/article/14069350/counter-uav-uas-drone-market

Keller, J. (2018, September 6). *Military Aerospace Electronics Computers*. Retrieved from Military Aerospace Electronics: https://www.militaryaerospace.com/computers/article/16726639/three-us-companies-takeon-challenges-of-nextgeneration-electrooptical-and-radiofrequency-sensors

Lei, Z. (2019, November 18). *China Daily*. Retrieved from China Daily Global: http://www.chinadaily.com.cn/global/2019-11/18/content_37523716.htm

Marcus, B. (2019, January 23). *World Economic Forum*. Retrieved from World Economic Forum Emerging Technologies:

https://www.weforum.org/agenda/2019/01/3-steps-to-prevent-the-next-gatwick-incident/

Michel, A. H. (2018, December 3). *The Washington Institute*. Retrieved from Improving the Quality of U.S. Middle East Policy: https://www.washingtoninstitute.org/policy-analysis/view/counter-drone-capabilities-in-the-middle-east-and-beyond-a-primer

Michel, A. H. (2019, November 10). *The Center for the Study of Drone at Bard College*. Retrieved from Drone Center Bard College: https://dronecenter.bard.edu/projects/counter-drone-systems-project/counter-drone-systems/

Military Aerospace Electronics. (2018, October 1). *Military Aerospace Electronics*. Retrieved from Military Aerospace Electronics Unmanned : https://www.militaryaerospace.com/unmanned/article/16707244/china-in-race-for-counterdrone-technology-and-laser-weapons-as-it-tries-to-catch-up-with-us

Raytheon. (2019). *Raytheon Laser Solutions*. Retrieved from Raytheon: https://www.raytheon.com/capabilities/products/lasers

Ruff, N. (2017, September 1). *SIA Technology Insights*. Retrieved from Security Industry Association: https://www.securityindustry.org/2017/09/01/drones/

Sharma, M. (2017, August). *Centre for Joint Warfare Studies*. Retrieved from UNMANNED AIRCRAFT SYSTEMS: A DISRUPTIVE TECHNOLOGY: https://cenjows.gov.in/pdf/synergyarticle/Book_unmaned_aircraft.pdf

UAS Weekly. (2019, November 13). *UAS Weekly Counter UAS*. Retrieved from UAS Weekly : https://uasweekly.com/2019/11/13/military-grade-no-drone-counter-uas-radar-detection-system-released-for-airports/

Wall, R. (2019, March 3). *Wall Street Journal*. Retrieved from Wall Street Journal Business: https://www.wsj.com/articles/weapons-makers-declare-war-on-drones-11551627000

World Economic Forum. (2018). *Advanced Drone Operations*

Toolkit: Accelerating the Drone Revolution. Cologny/Geneva: World Economic Forum.

[1] Both Gault & Michel references are based on the same report from Bard University – just with different emphasis.

Chapter 3: Developing a C-UAS Strategy Goals, Options, Target Analyses, Process Selection, Operational Metrics Approaches to Countering UAS Activities (First Principles)

H.C. MUMM

Student Learning Objectives

The student will gain knowledge on the concepts and framework as it relates to the process of developing an end-to-end Counter-Unmanned Aerial System (C-UAS). The student will gain knowledge through real-world examples and a case study, allowing the student to use critical thinking skills to apply learning to multiple C-UAS situations.

History

When drones became dangerous, counter-drone responses had their start. One of the more famous counter-drone operations was waged against the German V-1 Buzz Bomb. Due to its speed and size, this was a difficult drone to destroy. The British air defense used anti-aircraft guns, static balloons where the cable was the kill mechanism, and fighter aircraft. (Military-history-now, 2015) Only the fastest fighters would do, such as the de Havilland Mosquito. British fighter aircraft would be alerted and guided to the V-1 by ground radar. Once the fighters intercepted the V-1, they would place their wingtip under the wingtip of the V-1. The disruption in the airflow would tip the V-1, which would cause the primitive gyro stabilization to tumble and send the V-1 crashing to the ground. The fighters would also shoot down the V-1, which was a risky decision as the V-1 could detonate and also destroy the attacking fighter. Post-World War II, counter-drone tactics have been mostly anti-aircraft guns.

C-UAS Analysis Framework

1. Analyzing the Threat

Careful study will allow for an in-depth analysis of the threat, and thus a critical first step in the process. By answering the questions in the C-UAS analysis phase, the requirements will be determined, and a solution can be devised to build an appropriate counter-drone system. Mistakes in this first step can result in developing an ineffective system or a system inappropriate for the job. There are several types of questions that need to be answered within the analysis steps: what is the nature of the threat; what are the aerodynamic abilities of the threat; what is the overall design of the threat; is it a singular or multiple entity threat? As well as what is the navigation method used by the threat?

Understanding the Purpose and Weaponization of the Threat

The analysis needs to include answers to the following questions: What is the nature of the drone threat? Is it just surveillance? Is it reconnaissance? Is it directing fire support? Is it a Kamikaze drone? A Kamikaze drone can be as small as a commercial quadcopter with explosives onboard to a significantly larger aircraft or even cruise missile. Does the drone have the ability to release weapons and return home? If the vehicle is equipped with a warhead, can it be detonated in flight? Is the drone delivering contraband items over a barrier? Small drones are commonly used to drop contraband drugs over prison walls (Biesecke, 2011). Once the nature of the threat is determined, the next step is to determine the aerodynamic capabilities of the threat.

Understanding the Aerodynamics of the Threat

These questions should include as much information as possible about the offending drone (s): How fast? How high? What is the range? What is its payload capacity? As the speed of the drones increases, the potential response methods decrease. As these questions are answered, the expense and level of effort to develop the defense can be determined. Additional questions that need to be asked include: How can it be tracked? Does the drone use stealth technology? Stealth technology may be applied to radar, infrared, visual, or auditory signatures. Most of the time, the drone is considered stealthy just because of its size and that it is made from material with little or no metal except for the avionics. Another component of a drone's signature is speed. It is very common for modern radars to be dependent on the Doppler Effect for detection and tracking. Slow objects can fall into the notch designed to eliminate ground clutter (vehicles) and birds. Objects that are not moving towards or away from the radar (called the beam) can disappear altogether from the radar scope (Saabgroup, 2018).

Understanding the Air Vehicle Design of the Threat

Air vehicle design is an important factor in creating an effective defensive response. Questions need to be asked to determine what materials were used to construct the aircraft. Is it metal, plastic, or a composite? Non-metallic aircraft are more susceptible to a variety of counter technologies, including tactical lasers. For the main body and flight surfaces: what will it take to breach the body or disable the flight surface? Does the vehicle have exposed rotors or propeller that can be attacked? Rotors and propellers can be destroyed by lasers, broken by impact, or snagged by a net. Does the vehicle has exposed electronics or electronics that can be easily jammed, interfered with, or destroyed using lasers, jammers, radio waves, or by overpowering a frequency? Can the warhead (if equipped) be detonated in flight?

Is it One Drone or Multiple Drones?

Are there current intelligence reports that indicate the tactics that are or are expected to be employed by the enemy? Are they using one type of drone or multiple types? Are these drones operating independently, together, or using swarm tactics? As the numbers of drones increase, so does the complexity of the response. Drone tactics, techniques, and procedures are largely unwritten as the technology is adopted and adapted into the civilian and military arena at a rate of speed that has not allowed for in-depth, intelligent gathering, databasing or analysis to occur.

Understanding the Navigation

Threat control and navigation methodology can be fundamental to the potential solution. What frequencies is the drone using for control, information gathering, and distribution? What navigation platform does the drone use? A great variety of drones use either GPS (Global Positioning System) or GLONASS (Global Satellite Navigation System) or both. Some drones are extremely dependent on these navigational signals. Other drones have an IMU (inertial measurement unit) that provides both altitude and location references. The smaller the IMU, the higher the drift rate usually is and thus the dependence on GPS type signals for frequent corrections. (UNOOSA, 2019)

2. Solution Limitations

Before starting on a proposed response solution, limitations must be identified. Many limitations are governmental in origin, while others are weather or terrain-related, based on the location for the deployment of the counter-drone solution.

Frequency Limitations

Many world governments control the frequency spectrum for their country. In the U.S., that control comes under the Federal Communications Commission (FCC) (Commission-Licensing, 2019). UAV operators can passively listen to the frequency spectrum, but as soon as the solution involves transmitting on a particular frequency or frequencies, then permission and approval must be sought from the FCC (or similar agency) for that transmission. This is especially true when it comes to using jammers as part of the solution as "Federal law prohibits the operation, marketing, or sale of any type of jamming equipment, including devices that interfere with cellular and Personal Communication Services (PCS), police radar, Global Positioning Systems (GPS), and wireless networking services (Wi-Fi)" (FCC, Jammer Enforcement, 2019). When it comes to exemptions: "Only federal agencies are eligible to apply for and receive authorization" (Commission-Licensing, 2019). Smaller drones often fall into the Wi-Fi set of frequencies, while larger drones often use a variety of radio or satellite frequencies. There are other countries in the world where this limitation is not as restrictive. Combat operations also open up the solution to a variety of jammers. During combat operations, it is easier to coordinate the jamming of data linked frequencies than it is to coordinate GPS jamming, due to the dependence that U.S. military forces have on GPS. As more GPS jam-resistant equipment makes it into military services, this limitation of GPS jamming will decrease.

Global Governance

In addition to particular frequencies, airspace is also controlled in many countries. In the U.S. that airspace control is governed by the Federal Aviation Administration (FAA). Drones in the U.S. are currently limited to 400ft AGL (above ground level) unless otherwise approved by the FAA. There are at least two drone-on-drone counter methodologies that would also fall under this limitation. Other countries have different limitations, and some countries have little or no limitations defined at this time. Any drone defense system will need to be coordinated with the host country or the combatant command within a war zone. Mutual coordination is especially true for any projectile or tactic that destroys the UAS, commonly referred to as a kinetic kill mechanism.

If the area to be defended is urban or suburban versus rural, the kill mechanism may be further limited; especially kinetic kill mechanisms. Bullets or missiles that are deployed and do not hit the intended target and can potentially injure or kill someone, and if the drone is large enough, the drone itself may crash into people or property. There are two caveats to consider when determining the risks of kinetic C-UAS against a lethal drone. One, the drone may cause much more damage if it is not destroyed, and two, even though an urban environment has a high population density, the odds of a drone crashing on an individual is surprising low. This is because people are physically a small portion of the area in an urban environment and often protected from this type of impact by buildings and other sturdy structures. This is especially true of all but the largest of drones; even they have limited mass per square foot of impact area. (C. Horowitz, 2016).

Legal Ramifications

Country, State, and local laws regarding drones and counter-drone operations are proliferating at a great rate around the world with no consistent theme. Some counter-drone technologies have been designated as illegal in some countries while not being recognized in other countries. Additionally, there are anti-hacking and technology laws that affect aircraft (in general) that can impact the use of certain counter-drone technologies. Hacking a drone to render it safe seems like a technically good idea; however, the legal ramifications can be significant, including being charged with grand larceny for drones ranging in price from $400 to $1,000. According to 18 U.S.C. § 32, it is a felony to willfully damage or destroy aircraft (§130i., 2019). Although many courts have chosen to sidestep these cases, a counter-drone engagement could subject the operator to civil, criminal, and tort liabilities. In the U.S., criminal and liability limits are disclosed, but these penalties (many severe) are not always disclosed in other countries. It is critical for the solution to adhere to the national and local laws including getting proper permissions or exemptions before any drone engagement. A major exemption falls under 6 U.S.C. § 130i Protection of certain facilities and assets from unmanned aircraft (§130i., 2019). Similar laws give the Coast Guard and Secretary of Energy Counter UAV authorization. Other countries are developing their own laws/rules for facility and asset protection.

Atmospheric Limitations

Weather is another limitation of a C-UAS solution. Atmospheric considerations are a key element in support of UAS flight testing. The local atmospheric environment (wind speed and direction, wind shear, temperature, precipitation, and turbulence) must be characterized and understood (Edward Teets, 1998). In regions where cloud cover and/or fog are prevalent for a significant portion of the year, most sensors used for the identification of UAS are significantly degraded.

3. Developing a Counter-drone Response:

Range

The range required for detection and interdiction of the drone or drones must be determined. If the drone can release weapons, that adds to the range required for detection and interdiction. The faster the incoming threat, the lower the approach, the larger the area needed to defend, the more lethal the weapon portion; the further out the drone needs to be detected and interdicted.

There is also the need to identify the number of response layers for the appropriate range. Will there be two or more response layers or just a one-point defense layer? Will there be a shoot-look-shoot requirement to produce the desired probability of kill on the drone? If there is a wave of attacking drones, more than one layer of defense is recommended.

Detection

There are several passive and active detection technologies available to include as part of the solution. Electronic Signal Monitoring (ESM) is a very desirable passive detection system. ESM systems detect the communication frequencies of the drone and its associated ground station. Depending upon the antenna sensitivity and the output power of the drone, these signals can be discovered at significant ranges. The key advantages of these systems are is that the ground station controlling the drone may be located and engaged and that the systems are numerous (İ, 2017).

When selecting a signal detection system, all of the potential frequency ranges must be considered to counter all of the potential threats. If only a sample of frequencies is known, then the solution might be lacking during execution. The systems that receive commercial drone frequency bands are proliferating and significantly increasing in capability. Additionally, these frequency detection systems can quickly identify the signals for the drone and ground station. Some frequency detection systems include the ability to produce a digital fingerprint that can be leveraged as evidence for later prosecution. However, these frequency detection systems that are available on the open market lack the frequency bands of the more sophisticated commercial drones as well as the military drone frequency bands.

There are acoustic sensors to detect drone sound signatures, but because of their short-range and limitations in noisy environments, they can be part of a solution; however, it is rare that a single sensor technique be a part of a complete in the overall C-UAS solution.

A key part of detection is identification. Other passive types of detectors such as long-range cameras, IR (infrared) sensors, and SWIR (short-wave infrared) can provide the necessary identification (Red-ID) that the object is a drone and a threat. There are software packages available that can provide a much quicker and longer-range identification than a human operator. Additionally, some detectors include powerful illuminators within a frequency band that provide a stronger return and fewer false alarms. Illuminators in the infrared bands are invisible to the eye.

Active detection is primarily centered on various radar types. Conventional military radars pick up large and fast-moving targets easily and reject slow or non-moving targets to reduce false alarms. There are some new tactical radars that are designed to pick up the smaller, slower set of drones in addition to the larger ones. One radar variety uses an active electronically scanned array (AESA), and another variation uses a continuous wave radar. The latter is currently range limited, but technology can be extended (İ et al., 2017).

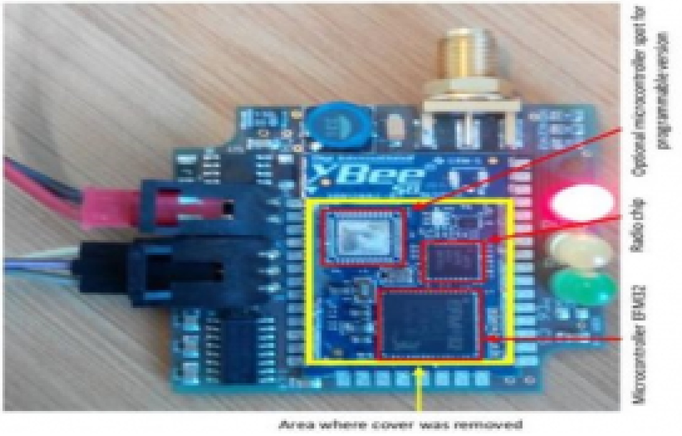
4. Interdiction

Small Drones

As small drones have proliferated, so too have the small drone counter systems. An initial favorite is the Radio Frequency (RF) jammer. These are designed to jam the control uplink for the drone. If a drone frequency is successfully jammed, there are multiple possible outcomes. One possible outcome could be the drone flying back to home base, which would be useful in capturing the operator. However, if the operator designated the target as the home base, this method would be ineffective. A second outcome might be that the drone makes a controlled landing. The least desirable outcome is that the drone exhibits uncontrolled behavior and crashes.

A GPS spoofer can gain a type of control over the drone by manipulating the GPS location. The drone can be directed to a safe location for capture and de-arming if necessary.

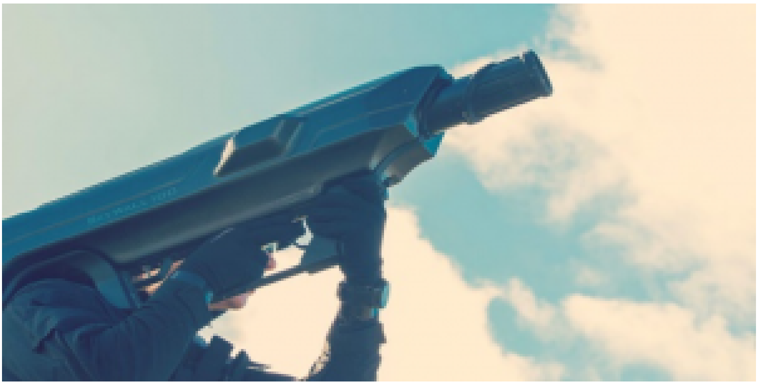
Figure 3-1: XBee Chip


XBee
Optional microcontroller spot for programmable version
Radio chip
Microcontroller EFM32
Area where cover was removed

Source: (BBC, 2016)

Hacking a drone is facilitated by having multiple manufacturers using similar avionic designs and somewhat predictable drone behaviors. A relatively inexpensive set up like a telemetry module by Mr. Rodday using an XBee chip acquires the unique key and takes command of the drone, rendering it harmless. This action is significantly more difficult if the chip has been encrypted. (BBC, 2016). Nets are an effective tool against the typical small commercial drones as long as they are not too fast. See Figure 3-2. There are several varieties of employment: e.g., another small drone can carry a small net cannon and launch the net at another drone.

Figure 3-2: UAV Net



Source: (Openworksengineering, 2019)

This methodology usually comes with an attached line that allows the shooter to gently lower the offending drone to the ground. Nets can also be launched from the ground using equipment that looks like a bazooka. Less reliable unless used by an expert are the nets deployed by a shotgun shell.

A relatively inexpensive but effective system is a kamikaze type drone. See Figure 3-3. This can protect a fairly large area and can "shoot down" a variety of small drones. The key challenge is they must hit a vulnerable part of the target drone. As opposed to a missile, these types of systems can reattack if they miss.

Figure 3-3: Kamikaze Drone Example

Source: (Dormehl, 2019)

This capability is a function of the target drone speed. Another proven method is the use of a predatory bird to attack and potentially capture the drone. Though proven effective, this method requires a high level of maintenance.

Medium Drones

The medium drone classification is mostly made up of military drones designed for surveillance. The world market is seeing more and more kamikaze type drones entering the medium-sized classification. Iran has placed significant emphasis in this area and has a variety of direct attack drones.

Some of the same counter techniques used for small drones are also effective on medium drones. RF jamming, for example, can be effective, albeit with some limitations. Medium drones generally require more RF jamming power and across a variety of frequency bands. However, once in the target area, they may no longer need external control from a ground station. These drones can proceed to the target coordinates on their own. If the attack drone requires GPS/GLONASS, this can be jammed to limit precision, but the drone will land somewhere.

A more direct counteraction is required to be effective against this class of drones to include the use of missiles, bullets, and lasers. The type of missile to be used is dependent on the size of the offending drone and its signature. Generally, medium-sized drones have a very small infrared signature, which makes it difficult to deploy IR missiles as a countermeasure. This category of drones also has a limited radar signature. Radar guided missiles are most effective when they have their own terminal radar and can be guided by a more powerful ground radar data uplink. Surface-launched AMRAAM (SLAMRAAM) is an example of this type of weapon. The SLAMRAAM is no longer used by the U.S. military due to priority changes; however, there are indications that other countries will employ these weapons in a C-UAS scenario. An effective weapon is a laser-guided missile that does not have the signature limitation that the other missiles do, and it has a very limited countermeasure set to work against.

Bullets tend to be a last line of defense due to their limited range. There are two techniques that can be effective. First is the hail of bullets typically from a Gatling gun type system. The second is from a rapid-fire cannon that has bullets that fragment just before hitting the drone. There are 25mm bullets that fit into this desired capability. As a point of consideration, as the area to be defended increases, so does the required number of gun sites and ammunition needs.

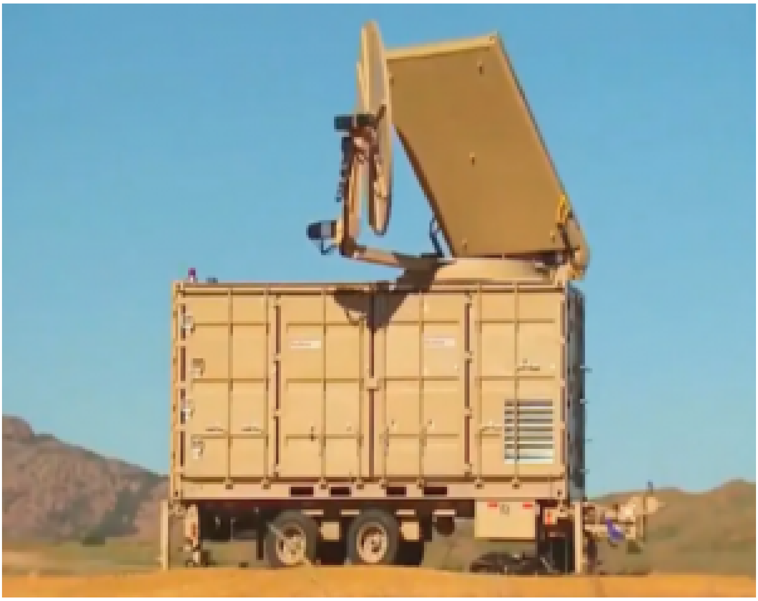
High-Powered Microwave (HPM) systems directly attack the electronics onboard the drone. Depending on the power and range, the system disrupts the data links, and eventually, the actual circuitry as the power increases, and the range decreases. These systems can be indiscriminate, so a focused system and a clear background are important. See Figure 3-4.

Lasers, because of their price tag, are normally limited to military applications. These systems are getting more and more powerful and, therefore, more effective and capable of engaging at longer ranges. These systems target a vulnerable flight control on the drone. See Figure 3-5.

Large Drones

This classification includes both commercial and military drones; however, it is the military drones that represent the threat. [Figures 3-6 and 3-7] These military drones range from slower, higher altitude, surveillance drones (some with weapon capabilities) to stealthy fighter-type drones. The latter of these two is more dangerous and more difficult to eliminate.

Figure 3-4 High Powered Microwave System



Source: (Trevithick, 2019)

Figure 3-5: Laser Sensor Ball

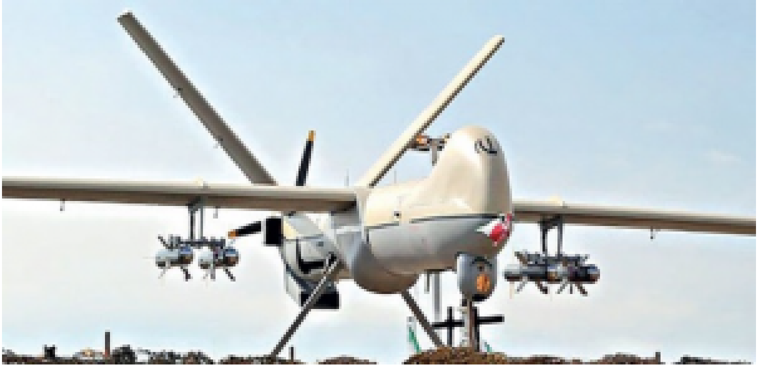
Source: (spazio-news.it, 2019)

The flight control is damaged, which then sends the drone out of control and to an eventual crash. There are now several versions of laser weapons available.

Manned attack aircraft are also included in this response category, especially for cruise missile type systems. For attack drones that fly under 200 knots, a propeller-driven light attack aircraft with an onboard gun system is sufficient. Once the speed rises about 200 knots, a jet-powered fighter-type aircraft is required. While missiles and guns are available, generally, the most effective choice is the gun for single drone engagements. In a situation where there are several attacking high-speed drones, the fighter aircraft will be required to use its missiles and follow up with guns or missiles on the ones that survive the initial response.

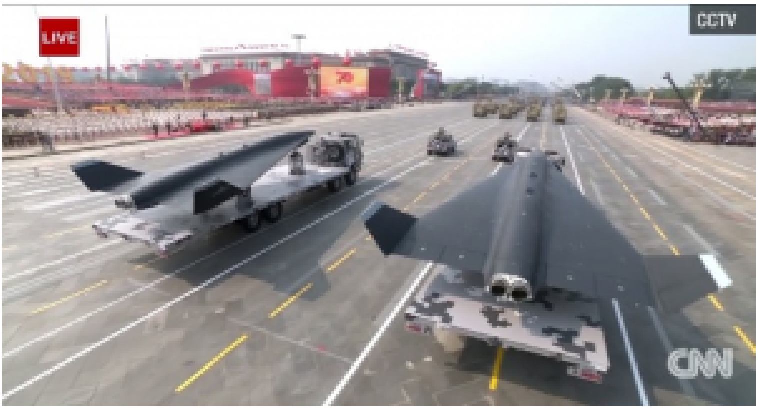
Some of the defenses for medium-sized drones carry over into the large drones. Defensive systems designed for attacking manned aircraft become prominent in this large drone category.

Figure 3-6: Iranian Drone



Source: (Singh, 2019)

Figure 3-7: Chinese Drones on Parade



Source: (George, 2019)

Jamming systems, though somewhat effective on some drones in this category, generally fall off as a primary defense system because the satellite uplink can be jammed. Jamming the uplink is a typical point defense solution unless it is space-based or has an included airborne relay. Bullets can no longer be used as a primary point defense system due to their short range and limited altitude coverage.

High-end missile systems, such as the US Patriot system, can be brought to bear for these type threats. Typically, missile systems are an early choice because they are already in the military inventory. For wealthy countries, the poor cost exchange of using expensive missiles against often less expensive UAS is not much of a factor. The potential cost of damage from an enemy UAS often outweighs the cost of the missile. Interdiction success is the primary metric. Stealthy drones are the most challenging, but acquisition ranges, though shorter, are typically sufficient for a successful engagement. The most significant limitation of this drone response is the amount of area that is being protected is relatively small.

Directed energy weapons, though of limited use against manned aircraft, are becoming a weapon of choice for larger drones. Directed energy weapons include high powered microwaves and lasers, which are considered point defense systems. If the attack corridors are known and limited, then these types of systems can be set up like a picket fence formation to protect a much larger area and engage threats much earlier. Of the two, the high-powered microwave systems tend to be more effective due to the short engagement time required. Lasers often must dwell on the target for several seconds to be effective. Against the slower end of the large drone category, lasers can be extremely effective. Faster aircraft are more problematic for current lasers, but as the lasers become more powerful, the dwell time required will go down, and this type of weapon system will be effective against the fast-moving UAS in this category.

Manned aircraft become a primary part of the defense to protect larger areas and engage the threat much earlier. Large drones, including the stealthy ones, can be easily terminated by a fighter jet as these drones have no self-awareness and have limited maneuverability. Since these drones usually have no weapons to fight back, they can be attacked and re-attacked with impunity. Fighter pilots quickly become drone aces. The most challenging scenario is a swarm of stealthy attack drones. Fighter squadrons must determine if there are enough missiles and gun rounds to take out all of the attacking drones before the drones reach their intended targets (U.S. Air Force Major Jay Snyder, 2019).

Case Study

The case study below reviews the swarm drone attack in Saudi Arabia on the morning of September 14, 2019. Although the event is real and well documented, the analysis, limitations, and solutions are fictional and designed to demonstrate the C-UAS analysis framework.

Background:

On the morning of September 14, 2019, two state-owned Saudi Arabian oil production sites were attacked. The Abqaiq and Khuraid oil fields are the largest oil production facilities in the world. These two plants account for almost 8% of the world's oil supply (bbc, 2019). The attacks were conducted using drones and cruise missiles from an unknown origin. "According to the Saudi Defense Ministry, eighteen drones and seven cruise missiles were fired at the kingdom" (Frantzman, 2019). Defense News stated, "If ever the world needed a reality check for the threat posed by drone swarms and low-altitude cruise missiles, this was it" (Frantzman, 2019).

The news reports differ as to the specific number and types of drones and missiles used in the attack. Four missiles did hit their intended oil field targets; however, it is unclear how many did not complete the mission. (Frantzman, 2019). This was a major escalation in UAS attacks given the type and number of utilized drones. There also continues to be speculation as to the geographical origins of the attack. Previous drone attacks had come from Yemen and were limited in size, scope, and range. It is widely believed by Saudi Arabia and the United States that Iran was the source; however, Iran has not claimed credit for this attack.

What is remarkable is that despite the heavy defenses of the Abqaiq oil field, none of the systems or technologies thwarted the attack. The facility is believed to have air defenses that include an American Patriot system, a Swiss-made 35 mm anti-aircraft Oerlikon cannon in conjunction with a Skyguard radar, and a French-designed Shahine, which is a surface to air missile system.

(Frantzman, 2019). The Patriot missile defense system is the only component specifically designed to defend against UAVs. It is highly possible that the drones were guided using on-board sensors and not GPS programmed, which, given the infrastructure of an oil processing facility, was quite advantageous.

If US-supplied air defenses were not oriented to defend against an attack from Iran, that's incomprehensible. If they were, but they were not engaged, that's incompetent. If they simply weren't up to the task of preventing such precision attacks, that's concerning, said Daniel Shapiro, a former U.S. Ambassador to Israel. (DM, 2019).

Brig. Gen. Pini Yungman believes that the "primary challenge in stopping an attack like that in Saudi Arabia is not the ability to shoot down the threats, but rather to detect things that can sneak in near the ground" (DM, 2019).

Creating a Solution

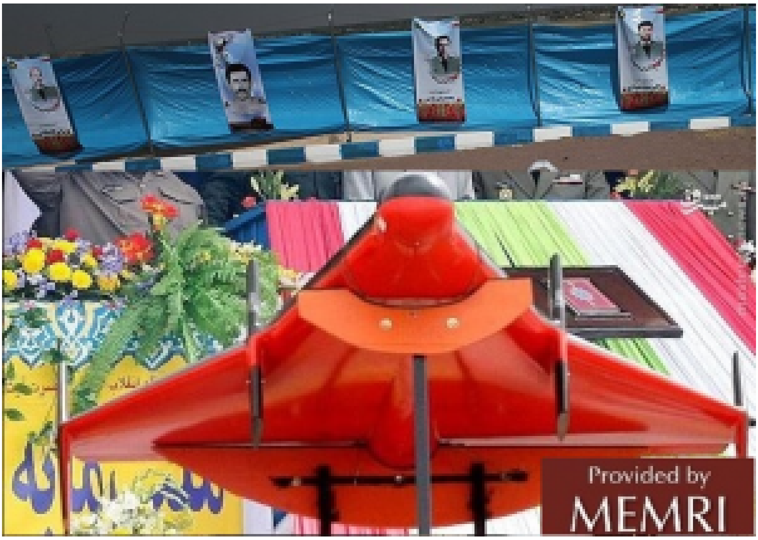
Analyzing the Threat:

In this case study, the threat determination is more speculative than defined. Iran denied launching the attack, but the weapon systems were most definitely Iranian in design and possibly in manufacturing. The origin of the drones was determined by these same drones being previously used against Saudi Arabia and the recovered wreckage. There is some speculation that one type of drone was used against the Patriot defense system, while the second type of UAS was used against the oil facility, based on the wreckage from numerous sites. The recovered delta-winged drone was determined to be most likely from a Toofan Iranian drone or a similar design class with a greater range.

Toofan Drone

The Toofan drones are a series of drones developed and used by Iran specifically for suicide missions. Iran does not publish information about the drones it builds and designs. The Toofan drone is considered small and is known to be very fast – up to 250km/hr. One of the advantages is its' undetectable launch. All of these features make it difficult for an effective C-UAS response. See Figure 3-8.

Figure 3-8: Toofan Drone



Source: (“Iran Suicide Drones,” 2019)

Industry analysts who have seen the Toofan describe it having a small radar cross-section and appearing to be made with lightweight radar-absorbing materials and guided by cutting edge avionics. It can fly for over one hour. There is also a front-facing camera in the nosecone which transmits live images until the moment of impact. All of these characteristics make the Toofan a very effective suicide drone (memri, 2019).

Although the Toofan has a small radar signature, the estimated speed of approximately 135 knots places it in the detectable range. The other possible drone used in the attack was most likely a Yemeni Houthi militia Quds-1 cruise missile (memri, 2019).

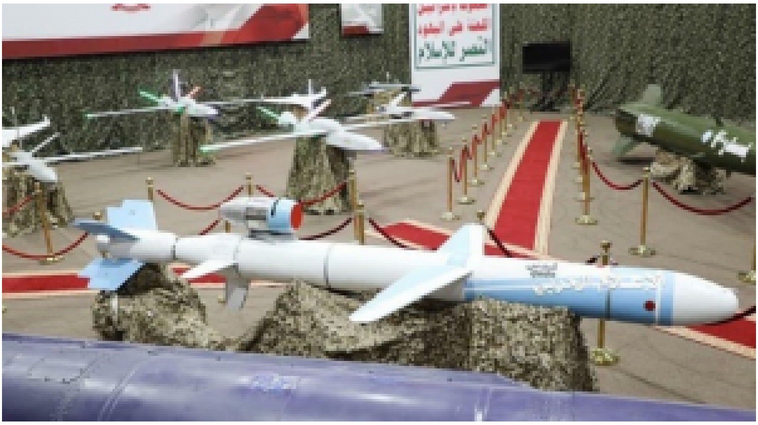
Possible Cruise Missiles

Cruise missiles are slower than traditional missiles, fly at lower altitudes, and are small – all radar-evading advantages. Another advantage is that cruise missiles are typically lower in price than other types of missiles. (armscontrolcenter, 2017) Cruise missiles can be launched from almost any location: by land, from the air, or an ocean vessel (armscontrolcenter, 2017). These types of missiles can have multiple guidance systems depending upon the design. The missiles can be completely pre-programmed for GPS flight or can be guided by an operator using a forward-positioned camera.

Quds-1 Missile

Initially thought to be designed in Yemen by the Houthi, the Quds-1 cruise missile is powered by a Czech built turbojet engine. See Figure 3-9. However, based on an Iranian industry analyst, the Qud-1 might have been developed and designed in Iraq (armscontrolcenter, 2017). The Iranians have been developing several different types of missiles for the past few decades. The Quds-1 is smaller than the Soumar and Hoveyzeh missiles and has less thrust than the Ya Ali missile. (armscontrolcenter, 2017). The Quds-1 appears to be primarily made out of metal, based on the wreckage. The signature is likely small but in line with other cruise missile signatures (Hinz, 2019).

Figure 3-9: Quds-1 Cruise Missile



Source: (Hinz, 2019)

Potential DIANA Missile Usage

Since little is known about the Quds-1 cruise missile besides the suspected range of 425 miles, the DIANA target cruise missile can be used as a surrogate for analysis since it has the same engine and is approximately the same size (Hinz, 2019). This gives the Quds-1 a suspected speed of 330-350 knots. Manufactured by Equipaer Industria Aeronautica, the DIANA has a flight altitude variance of 10m – 8,000m and is designed for high speed / high maneuverability. It is advertised to have a maximum speed of 380 mph (equipaer, 2011).

Tactical Analysis:

The oil facility attack demonstrated a precise and sophisticated attack utilizing multiple drones with different attack profiles to multiple locations within a small amount of time. It is suspected that multiple Toofan drones first attacked the Patriot radar, followed by additional Toofan drones and Quds-1 cruise missiles attacking the oil facilities. The Toofan's optical final guidance could have been employed. That would mean the human controller(s) would have to be part of the attack. The Quds-1 most likely uses an IMU and GPS for guidance (Hinz, 2019). This is consistent with what is known about their anti-ship cruise missiles. The attackers used low-cost attack vehicles specifically designed to evade radar. The attackers knew the specific locations for the radar defenses and the overall defenses of both facilities. Additionally, the attackers used a combination of manned and unmanned systems – but no human support was physically located at either oil field.

Solution Limitations:

In this scenario, the use of the Patriot radar and patriot missile response, coupled with little intelligence against an unknown number of targets, limited the effectiveness of the system. It has been reported that the guards at the facility attempted to use their rifles and handguns to defend the installation (DM, 2019).

Preservation of Existing Infrastructure

Saudi Arabia's oil fields have high value and are in a protected area, which is relatively remote; there are fewer limitations on the potential solution. As this is an industrial site, the solution needs to consider minimal damage to the physical facilities as well as the electronic and communication systems of the facility infrastructure. Returning to the concept of not incurring damage to the physical facilities, mitigation plans need to be developed if friendly or threatening drones are destroyed over the oil fields. There should be special care taken to consider any combustible materials.

Governance

Additionally, military and commercial air traffic need to be accounted for in the plan. If GPS/GLONASS jamming is to be part of the solution, it needs to be coordinated and approved by the Saudi government. The oil fields are owned by the Saudi government; this fact should assist in any governance being written, altered or waivered to protect this critical infrastructure.

Atmospheric Limitations

Several atmospheric limitations exist in the Middle East Region. The weather in Saudi Arabia is normally sunny with mixed or no cloud cover, and the week of September 8 – 14, 2019, the weather in this region averages from 80 – 107 degrees Fahrenheit. The days are coolest just before midnight until approximately 7 am. During September, the dew point average is 6 %. Abqaiq skies experience cloud cover between 7-29 % of the time for this month (weatherspark.com, 2019). In this region, there are sand storms, heatwaves and even fog in the air near the ground. These conditions don't preclude laser solutions, but it does have an impact on them. Consideration should be made to elevating the laser above the ground if it is part of the system, possibly in a guard tower or in an airborne platform. The topography is considered to have modest variations with a 1,270 ft variation for a 50-mile radius.

A Multi-Layered Counter Drone Response Plan

The multiple drones used in the Saudi oil field attacks are considered medium drones; therefore, the solution should consider all appropriately sized and quantity countermeasures. The countermeasure response should account for multiple drones attacking at once; more than one type of drone; with one drone being relatively high speed; and a sprawling soft infrastructure to be protected; all lead to more than one layer of defense and that the first engagement should far enough away to allow for an assessment and engagement of leakers before they can reach the facility. As the first layer of defense is extended out, the larger the engagement arc distance grows.

For this case study, the first layer should be about 25 miles out from the protected area. This perimeter allows for advancing targets and receding targets, as well as enough time to coordinate the second layer response. The proximity of the coastline is a factor in the system placement. The expanse of the perimeter precludes the use of shorter-range systems because of the number of sites required. Bullets, lasers, and high-powered microwaves concede to missile-based solutions at this range. Ground-based missile systems are a more practical choice for protection than aircraft-based missile systems. The cost of the aircraft and pilot patrolling the airspace becomes astronomical for an irregular threat.

The range for the point defense second layer needs to be far enough out to interdict the drone and not have it come down within the facility boundaries; while at the same time not creating an arc distance that is too big not to be cost-effective. In this case that range would be approximately 5 miles to account for the cruise missile type attack drone. With the shorter coverage zone, the variety of shorter-range systems can be considered.

Detection

Detection is one of the more challenging portions of the solution. At least one of the threat drones is a low altitude ingress type drone, and therefore the detection system needs to be elevated. The Quds-1 is unlikely to be transmitting any signal for an ESM type system. The Toofan may or may not be transmitting. The interdiction system selected needs a precise location for weapon guidance, and since sensors in the light spectrum have too short of a range for this protection ring, the best choice is a radar type system.

The next decision is the type of elevation method. Is the radar system on a tethered balloon or an extendable arm or a fixed tower? Due to the risk of sand storms, a tethered balloon is not the best solution. For maintenance reasons and sand storm considerations, the extendable arm is preferable over the fixed tower. Although stationed on the outer perimeter, the radar needs to be effective across the entire facility.

Interdiction

Interdiction is best done when layering defense technologies, methodologies, and systems. Numerous scenarios need to be considered when designing an effective counter-drone defense solution. Combination systems can be more effective, especially when defending against different types of drones. As an example, the Toofan type drone is more susceptible to a directed energy weapon, whereas the Quds-1 cruise missile is more susceptible to a hard kill. Each layer should have overlapping interdiction systems to preclude multiple attack drones attempting to overwhelm a single sector. Additionally, if ground missiles are part of the overall solution, then, the number of ground stations, missiles and support personnel need to be considered as part of cost and maintenance.

Graphical representation of the anticipated engagement envelope can be particularly useful when determining point positioning. Most engagement envelopes are not a circle; effective engagement zones look much more egg-shaped. The narrow end is drawn for the receding targets and the wide end for the advancing targets. The faster the incoming target, the more the egg shifts such that the receding target zone gets smaller. The faster the intercepting missile, the larger the egg gets, and the greater the receding target capability (Snyder, 2019).

Integration

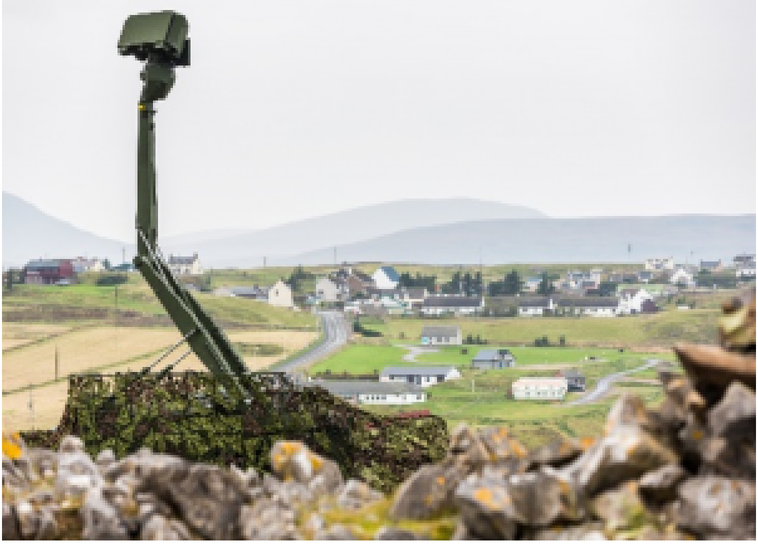
When dealing with a variety of interdiction methods, the system needs to be evaluated so that no one part of the system conflicts with any other part of the system. It would be counterproductive to have a communications system that is susceptible to the jamming solution. If an HPM is being integrated, it should be analyzed to make sure it will not damage other system components. Additionally, shots fired at receding targets should not cause collateral damage to the property being protected. All components should be tested with every other component to validate that all components work harmoniously together and do not harm the home facility (U.S. Air Force Major Jay Snyder, 2019)

The Chosen Solution:

Figure 3-10 shows a SAAB Giraffe AMB Radar. The Giraffe is a 3D detection system that can detect small, low, and slow targets as well as aircraft, cruise missiles, rockets, artillery, etc. The radar is on an extendable arm to increase the detection range of low-level targets.

Outer Layer

Figure 3-10: SAAB Giraffe AMB Radar



Source: (Saabgroup, 2018)

The radar system operates out to approximately 65 nautical miles. The small signature of the Toofan drone reduces the maximum detection and tracking range of the system. SAAB demonstrated detection and tracking of a small drone with a signature of .001 square meters at a range of 4 km. (SAAB, 2019)

Extrapolating this information to the Toofan (using the Harpy drone as a surrogate) delivers an approximate detection and tracking range of 25 km. By placing the radars approximately 40 km apart, there is good detection range throughout the arc with small notches. See Figure 3-11. (US Army, 2019)

Figure 3-11: Toofan Detection System

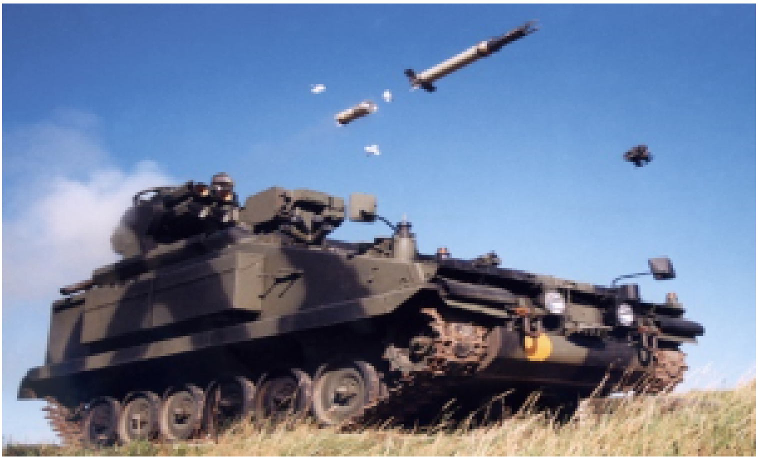
Source: (US Army, 2019)

Interdiction is provided by a ground-launched version of the AMRAAM-ER missile. It comes in a six-box configuration that can be ground or vehicle-mounted. This is called NASAMS II (National Advanced Surface to Air Missile System). The AMRAAM-ER is a Mach 4 missile with an approximate range of 27 nautical miles (50 km). (globalsecurity.org, 2019) The missile launch systems will also be 24 miles (40 km) apart to provide dual coverage to the arc. Twelve missiles per site deliver the capability to shoot down up to 24 drones in any given sector before requiring a reload (US Army, 2019) Based on the potential threat approach directions, an initial arc of 270 degrees will be used for the outer layer. The arc can be reduced or increased depending on enemy tactics.

The StarStreak II is a Mach 4 class missile system is designed for a kinetic kill with a range of approximately four nautical miles. It employs three tungsten darts that are laser-guided and immune to all known countermeasures (Sparks, 2017). See Figure 3-12.

Inner Layer

Figure 3-12: Stark-Streak II Missile System



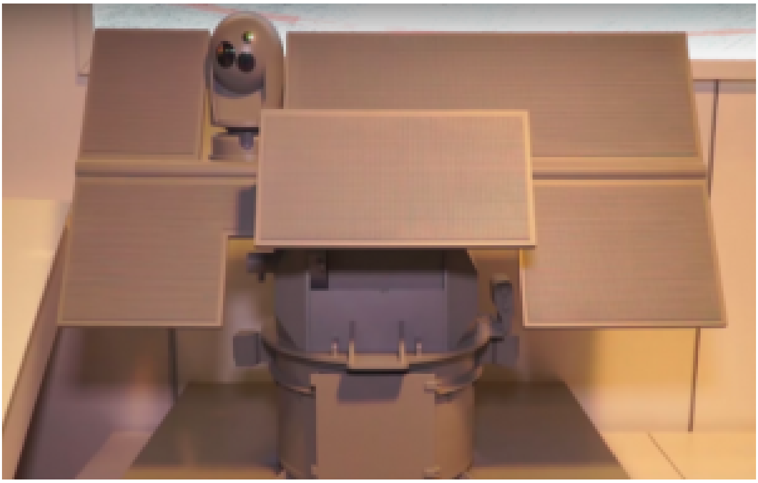
Source: (Sparks, 2017)

This permits the engagement of targets with extremely small signatures. (Minister, 2008) To complement this system for the inner layer is a High-Powered Microwave (HPM) system designed to fry the internal electronics of the attacking drone.

The system will be deployed on a fixed turret with an 8-missile configuration. The turrets will be remote-controlled from the Command Center. They will be deployed at six nautical mile increments around the inner 5-mile ring. This provides continuous and overlapping coverage. The typical concept of operations would use a shoot-look-shoot methodology. The concept of operations is facilitated by the speed of the missile. The StarStreak II is a very versatile weapon system and is capable of handling inner layer defense against a large variety of medium and large drones.

To complement the StarStreak system for the inner layer is a High-Powered Microwave (HPM) system designed to destroy the internal electronics of the attacking drone. There are two viable systems for this particular solution: Boeing's Thor and BAE Systems' HPM. See Figure 3-13.

Figure 3-13 Example of a High Powered Microwave System



Source: (Vavasseur, 2019)

Since this will be a component of the inner layer of defense, the BAE Systems' HPM is a logical

choice. The Boeing system is overkill for the inner layer due to its size and power output (Vavasseur, 2019)

BAE Systems HPM is "Scalable and designed for use on all sizes of surface combatants[.] HPM instantaneously defeats a wide range of air and surface threats at tactically significant ranges (such as UAV, Aircraft, Helicopters, USV, Fast Attack Craft…)" (Systems, 2018) A High-Powered Microwave System was chosen to prevent the overall system and especially the inner layer from being overwhelmed with the number of simultaneous attacking drones. The HPM type of defense system also permits the overall system to defend against swarming small drones if or when those also become part of the threat matrix. The HPM system will be deployed on a six-mile arc, halfway between the StarStreak systems. This slightly more forward deployment is to prevent possible interference with the StarStreak systems (Vavasseur, 2019).

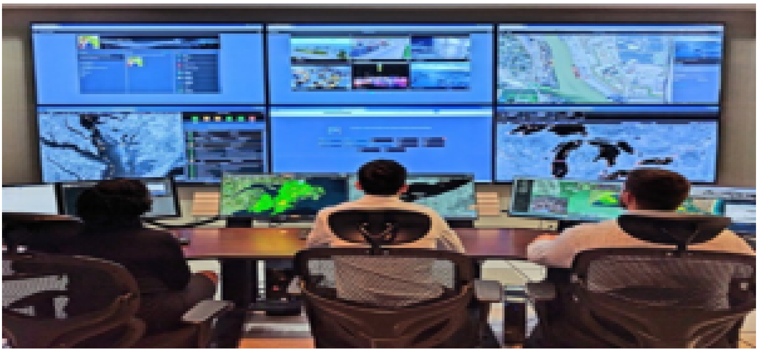
Command and Control

The more complex the system and the more layers involved, the more integrated the command and control system must be. Sensors, weapons, and communications need to be integrated and robust. Threat or no threat determinations need to be made in a quick and efficient manner to include an appropriate method of engagement. The number of personnel to accomplish this can be reduced by an expert or an AI system (U.S. Air Force Major Jay Snyder, 2019).

For this case study solution, all of the detection and interdiction components will be commercial off the shelf components to create the final comprehensive, integrated command and control center. Although many of these components have been integrated in the past, they have not been integrated with the inner layer systems. To minimize labor hours required and to maximize effectiveness, Artificial Intelligence (AI) will be leveraged as much as possible into the solution. When integrating a system of systems, it is always best to involve a major system vendor in that integration. There are several defense contractors who excel at complex integration, testing, and receiving government authorization for the final solution. Creating a new command and control system will most likely involve multiple vendors including one like the ARES Corporation to work with the lead integrator (Snyder, 2019). The ARES' mantra is "Protecting the world's most critical assets" (ARES Security, 2019).

ARES AVERT C2 product, as seen in Figure 3-15, creates a singular scalable interface that integrates partners' command and control portal. The company touts the configurability of the system to adapt to multiple situational awareness and incident response needs utilizing role-based security. The proprietary system can link unique network systems, sensors, with unique customizable client requirements collaborative response. (ARES Security, 2019) See Figure 3-14.

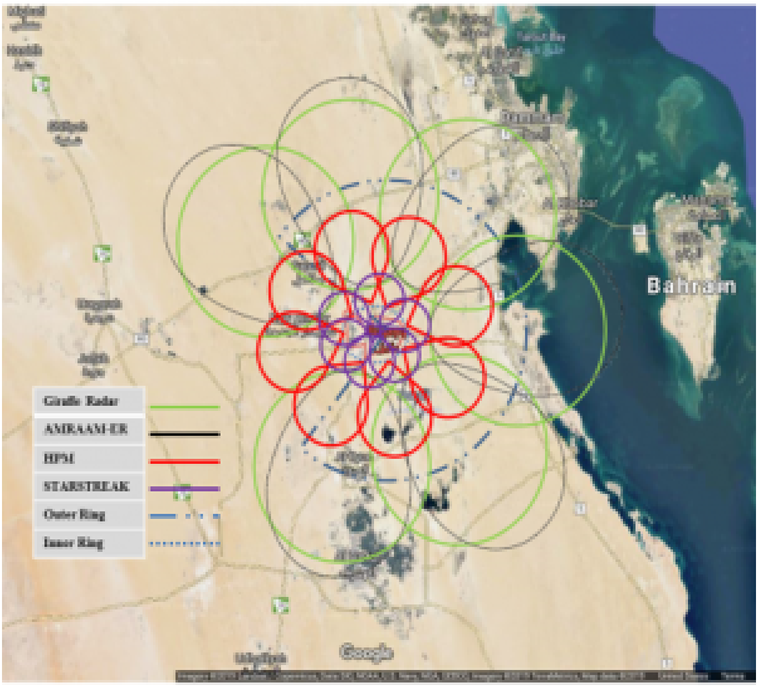
Figure 3-14: Sample Image of an AVERT C2 System



Source: (Vavasseur, 2019)

As this is a static design, the primary communications solution should be fiber optic cabling. The hard-wired cable provides a stable, consistent communication platform and avoids possible interference problems with the radars and HPM systems and can be secured. Wi-Fi or satellite links could be jammed, cause interference, receive interference, or have intermittent to poor performance (Snyder, 2019). Figure 3-15 is a composite of the overall solution coverage.

Figure 3-15: Case Study C-UAS Solution Diagram



Source: (U.S. Air Force Major Jay Snyder, 2019)

Conclusions

This chapter has examined some of the challenges and thought processes required to build a C-UAS framework for a given area. Developing a solution requires a multi-step process to avoid potential pitfalls and achieve a very high degree of success. Analyzing the threat or threats is the first step in the process. This process could involve something as easy as a quadcopter delivering contraband into a prison yard or as hard as cruise missiles and attack drones with the added challenge of having limited intelligence data available. The drone's mission and potential level of weaponization will determine the appropriate C-UAS response. The number of attacking drones will also govern the complexity of the overall solution.

Before contemplating a counter-drone solution, careful consideration needs to take place regarding the limitations to the possible solution set. Some limitations are physical, such as the weather, but some limitations could create legal issues, including jail time. Those limitations are set by the government of the respective country. Working with a government agency or requesting a waiver may be the only path to a successful counter-drone system.

As a counter-drone system is developed: range, detection, and interdiction will be the supporting foundation. At what distance does the drone need to be detected, and at what distance does the drone need to be engaged or interdicted? As these distances and perimeters increase, so does the need for a line-of-sight limitation solution. More than one layer or ring may be needed. Passive detection systems are fantastic if the drone and possibly the ground station are emitting RF signals. However, if the attacking drones are radio silent, then a radar type system will likely be necessary. Interdiction choices are often driven by the size of the drone and whether it is carrying weapons that can be released. As the size increases, the interdiction methods move from a soft interdiction using jammers, nets, etc. to more traditional weapons for aircraft that include bullets and missiles. As the number of attacking drones increase, the interdiction method moves from kinetic attacks to the non-kinetic realm of directed energy such as lasers and high-powered microwaves.

Do not forget the limitations and requirements for command and control in the overall solution. The command and control solution may be extremely simple and potentially designed for a variety of commercial drones. As the threat grows and the number of defense layers grows, so too does the complexity of the command and control system. The necessary level of complexity may require an expert software solution embedded with artificial intelligence to help guide the attack and response phases. C-UAS will continue to change and adapt as the technology improves, and the drone/counter-drone issues are more constrained by human innovation than the science that empowers the machines.

Questions

1. Name three factors that must be taken into consideration when building the framework for C-UAS?
2. What are the limitations of a C-UAS solution?
3. Can C-UAS be countered? If yes, how?
4. Why would a non-kinetic kill be chosen over a kinetic kill in C-UAS around populated areas?

References

130i., U. C. (2019). *U.S. Code §130i.Protection of Certain Facilities and Assets From Unmanned Aircraft.* Retrieved from www.law.cornell.edu/uscode: https://www.law.cornell.edu/uscode/text/10/130i

ARES Security. (2019). *ARES Security.* Retrieved from aressecuritycorp.com: https://aressecuritycorp.com/#home1

armscontrolcenter. (2017). *Fact Sheet: Ballistic vs. Cruise Missiles.* Retrieved from armscontrolcenter.org: https://armscontrolcenter.org/fact-sheet-ballistic-vs-cruise-missiles/

BBC. (2016). *Police drone can be hacked with $40 kit says researcher using* XBEE. Retrieved from BBC.com: www.bbc.com/news/technology-35709676 bbc. (2019). *Saudi Arabia oil facilities ablaze after drone strikes.* Retrieved from www.bbc.com/news: https://www.bbc.com/news/world-middle-east-49699429

Biesecke, C. (2011). CBP Continues To Explore Small UAS Options. *Defense Daily*, 249(16), 2-2. Retrieved from Biesecker, C. (2011). CBP Continues To Explore Small UAS Options. Defense Daily, 249(16), 2-2. : Biesecker, C. (2011). CBP Continues To Explore Small UAS Options. Defense Daily, 249(16), 2-2.

42. Horowitz, K. S. (2016). Separating Fact from Fiction in the Debate over Drone Proliferation. *International Security*, 41(2), 7-42. doi:10.1162/ISEC_a_00257.

Commission-Licensing, F. C. (2019). *Federal Communications Commission-Licensing.* Retrieved from www.fcc.gov/licensing-databases/licensing: https://www.fcc.gov/licensing-databases/licensing

Congress Bills. (2018, May 14). Retrieved from Protection of certain facilities and assets from unmanned aircraft: https://www.congress.gov/115/bills/s2836/BILLS-115s2836is.xml

DM, C. (2019, October). *Can anything stop attack drones?* . Retrieved from www.asiatimes.com: https://www.asiatimes.com/2019/10/article/the-rise-of-stealth-combat-drones/

Dormehl, L. (2019). *DroneBullet is a kamikaze drone missile that knocks enemy* UAVs *out of the sky.* . Retrieved from www.digitaltrends.com: Dormehl, L. (2019). DroneBullet is a kamikaze drone mihttps://www.digitaltrends.com/cool-tech/dronebullet-anti-drone-tech/

Edward Teets, J. D. (1998). Atmospheric considerations for uninhabited aerial vehicle (UAV) flight test planning. *In 36th* AIAA *Aerospace Sciences Meeting and Exhibit.* Washington: AIAA.

equipaer. (2011). DIANA: *Aerial Target Drone.* Retrieved from www.equipaer.com: http://www.equipaer.com/diana.php

FCC. (2014, December 8). *Enforcement Advisory No. 2014-05.*

Retrieved from https://transition.fcc.gov/eb/Public_Notices/DA-14-1785A1.html

FCC. (2019, November 19). *Jammer Enforcement*. Retrieved from Jammer Enforcement FCC: https://www.fcc.gov/general/jammer-enforcement

Frantzman, S. J. (2019, September 26). *Are air defense systems ready to confront drone swarms?* Retrieved from www.defensenews.com/global/mideast-africa: https://www.defensenews.com/global/mideast-africa/2019/09/26/are-air-defense-systems-ready-to-confront-drone-swarms/

George, S. G. (2019). *China shows off new stealth drones*. Retrieved from https://www.cnn.com/asia/live-news: https://www.cnn.com/asia/live-news/china-hong-kong-oct-1-live-intl-hnk/h_1ba984e1cf9a99769648fe35eb06cec5

globalsecurity.org. (2019). *AMRAAM-Extended Range – AMRAAM-ER*. Retrieved from www.globalsecurity.org: https://www.globalsecurity.org/military/systems/munitions/aim-120-er.htm

Hinz, F. (2019). *Meet The QUDS 1*. Retrieved from www.armscontrolwonk.com: https://www.armscontrolwonk.com/archive/1208062/meet-the-quds-1/

İ, G. O. (2017). Detection, localization, and tracking of unauthorized UAS and Jammers. *2017 IEEE/AIAA 36th Digital Avionics Systems Conference* (DASC). Washington: DASC.

memri. (2019). *Iran Presents its Suicide Drones*. Retrieved from /www.memri.org: https://www.memri.org/reports/iran-presents-its-suicide-drones

Military-history-now. (2015, February 6). *Buzz Kill – 13 Remarkable Facts about the V-1 Flying Bomb*. Retrieved from Militaryhistorynow.com: https://militaryhistorynow.com/2015/02/06/buzz-kill-15-amazing-facts-about-the-v-1-flying-bomb/

Minister, M. (2008). *MoD Minister Announces Missile Support Contract Win to Thales in Belfast*. Retrieved from www.copybook.com: https://www.copybook.com/companies/thales-uk/articles/missile-support-contract

Openworksengineering. (2019). *Sky Wall Patrol.* Retrieved from openworksengineering.com: https://openworksengineering.com/skywall-patrol/

SAAB. (2019). *Giraffe Elss Uav Detection and Tracking.* Stockholm, Sweden: SAAB.

Saabgroup. (2018, June 1). *United Kingdom Becomes Largest Operator of Saab Land-based Giraffe AMB Radars.* Retrieved from saabgroup.com: https://saabgroup.com/media/news-press/news/2018-06/united-kingdom-becomes-largest-operator-of-saab-land-based-giraffe-amb-radars/

Singh, S. (2019). *How military drones are becoming deadly weapons across the globe* . Retrieved from economictimes.indiatimes.com/news/defence: https://economictimes.indiatimes.com/news/defence/how-military-drones-are-becoming-deadly-weapons-across-the-globe/articleshow/71236124.cms

Snyder, J. (2019). *Engineering Solutions for Countering Autonomous Systems.* Arlington, VA: Mongo 1, LLC.

Sparks, M. (2017). *Starstreak Multi-role Missile- not just a SAM.* Retrieved from www.angelfire.com: http://www.angelfire.com/art/enchanter/starstreak.html

spazio-news.it. (2019). *Raytheon Delivers First Laser Counter-UAS to US Air Force.* Retrieved from spazio-news.it: Retrieved from http://spazio-news.it/raytheon-delivers-first-laser-counter-uas-to-us-air-force

Systems, B. (2018). *SNA 2018: BAE Systems Unveils High Powered Microwave.* Retrieved from www.navyrecognition.com: www.navyrecognition.com/index.php/news/naval-exhibitions/2018/sna-2018/5854-sna-2018-bae-systems-unveils-high-powered-microwave.html

Trevithick, J. (2019). *Air Force Set To Deploy Its Counter-Drone "Phaser" Microwave Weapon Overseas.* Retrieved from www.thedrive.com: https://www.thedrive.com/the-war-zone/29992/air-force-set-to-field-test-its-counter-drone-phaser-microwave-weapon-overseas-in-2020

U.S. Air Force Major Jay Snyder, R. (2019, October 30). Counter

Drone Tactics, Techniques and Procedures. (L. L. H. C. Mumm. Victory Systems, Interviewer)

UNOOSA. (2019). *Global Navigation Satellite Systems* (GNSS). Retrieved from www.unoosa.org: https://www.unoosa.org/oosa/en/ourwork/psa/gnss/gnss.html

US Army. (2019). NASAMS *Norwegian Advanced Surface to Air Missile System.* Retrieved from www.armyrecognition.com: https://www.armyrecognition.com/norway_norwegian_army_missile_systems_vehicles_uk/nasams_norwegian_advanced_surface_to_air_missile_system_technical_data_sheet_pictures_video_1

Vavasseur, X. (2019, January 1). *Video: BAE Systems High Powered Microwave at* SNA *2019.* Retrieved from www.navalnews.com: https://www.navalnews.com/event-news/sna-2019/2019/01/video-bae-systems-high-powered-microwave-at-sna-2019/

weatherspark.com. (2019). *Average Weather in September in Abqaiq Saudi Arabia.* Retrieved from weatherspark.com: https://weatherspark.com/m/104790/9/Average-Weather-in-September-in-Abqaiq-Saudi-Arabia#Sections-Precipitation

Chapter 4: Planning for Resiliency and Robustness

J.J.C.H. RYAN

Student Learning Objectives:

After completing this block, the student will be able to:

– describe the difference between resiliency and robustness

– describe different ways that resiliency might be enhanced

– explore ways in which resiliency can be measured or estimated

– describe difference ways that robustness might be enhanced

– describe how robustness can be measured

– conceptualize attacks on resiliency and explain cascading effects of successful attacks

– conceptualize attacks on robustness and explain cascading effects of successful attacks

– describe the cost-benefit trade space associated with resiliency and robustness

– explain how operational secrecy can be used as part of resiliency and robustness

– conceptualize protections to systems than can shore up resiliency

Understanding the Difference between Resiliency and Robustness

A stone aqueduct built by the Romans to carry water over hundreds of miles exists to this day. It is robust. An aspen tree quivers in the winds, perhaps loses a few leaves, but continues to live after the storm has passed. It is resilient.

Both of these attributes are important. But they can be the subject of choices in design: the aspen tree is both resilient and robust while the aqueduct is only robust and not resilient. Should assault or insult cause an aqueduct to break and fall to the ground, it would take a great deal of effort to rebuild and mend the structure (World Monuments Fund, 2016). Were the aspen tree to be subjected to an axe, the individual tree would be felled quickly enough, but the organism would continue: the vast majority of the "tree" is a large underground root system (Featherman, 2014). Soon a new shoot would emerge to replace the aspen that had been cut down.

The concepts of robustness and resiliency seem simple enough, so it is striking that they are so difficult to define and measure. The New Webster's Dictionary simply defines robust as "strong, healthy." It defines resilient as "springing back; buoyant." (Bolander (ed.) & Stodden, 1986) These definitions are not useful for engineering purposes. In this chapter, the concepts of resiliency and robustness will be explored through the lens of security, focusing on how C-UAS operations can exploit the various aspects of both attributes for compromise. To start, baseline operational definitions are offered so that a common language is possible for the subsequent analyses.

Resiliency

In exploring the literature, the varying definitions of resiliency do not stray far from the definition quoted above. Two ideas permeate the definitions: first, the ability to return to a previous state; and second, the amount of time needed to return to that state. Systems that are able to return to the previous state in a short period of time are said to have high resilience while those that take a longer period of time are said to have low resilience. (Hollnagel, 2016) (National Academy of Engineering, 1996)

There are several design features that enable or increase resiliency. First, a system must have an ability to respond to anything that changes its state. Next, the system needs to be able to monitor its state, being alert to internal or external changes that could affect it. Third, the ability to "learn" is useful: keeping track of previous experiences, responses to those experiences, and the results of those responses can provide the ability to more quickly respond appropriately. Finally, the ability to anticipate challenges or changes can accelerate the detection of issues and subsequent responses. (Hollnagel, 2016)

For the aspen tree, the ability to bend in the wind allows it to return to its previous state quickly, once the wind has calmed. Evolution has provided the aspen with that ability, having “learned” over millennia that wind exists and how to respond appropriately. These functions are internal to the aspen ‘system’ and are reproduced for each instantiation of aspen. Thus, it is possible to characterize the aspen as having high resilience.

The aqueduct, on the other hand, is entirely dependent on external forces to return to its functioning state: people to identify a problem, care enough to respond, and commence the labor needed to repair the structure. In the context of an aqueduct system that includes the architects, laborers, and tax payers, it has many of the design features, such as learning and anticipating, but the time to respond and repair is very long. The aqueduct has low resilience.

Robustness

The definitions in the literature regard robust design as a concept separate from robustness. There is some suggestion that following robust design processes will result in robustness, where the definition of robustness is a system that is insensitive to variations, both internally and externally. There is no time component noted in these definitions although time does seem to lurk in the background: a system that fails soon is not robust whereas a system that lasts a long time is robust.

Robust design is a process that focuses on quality in order to reduce the vulnerability of the system as a whole to problems that it may encounter. There are three components of robust design: system, parameter, and tolerance, with a focus on increasing quality during manufacturing rather than trying to “inspect in quality” after manufacturing. (Wysk, Niebel, Cohen, & Simpson, 2000) (Maurer & Lau, 2000)

The aqueduct design and build process used by the Romans focuses on product improvement at every step, including research and development of better materials to increase the effectiveness of the system. Continual maintenance was performed regularly until the organizing structure of the Roman Empire collapsed. The aqueducts continued to exist for a long time after the end of regular maintenance. (World Monuments Fund, 2016) They were highly resistant to variations and, as a result, very robust.

The aspen is a wonder of nature: most of it is underground and hence able to withstand the insults and challenges associated with environment and technical changes. The oldest aspen stand is estimated to be more than 80,000 years old (Featherman, 2014). It is highly resistant to variations, has great lasting power, and is, as a result, very robust.

Comparing Resiliency and Robustness

The following Table 4-1 summarizes the above discussed differences between resiliency and robustness:

Table 4-1: Summary of Resiliency and Robustness

	Attributes	**Time Component**
Resiliency	Ability to respond to undesired changes Ability to monitor current state Ability to learn from experiences Ability to anticipate challenges	Quick to recover to desired state $\partial t \sim 0$
Robustness	Insensitive to component variation Insensitive to parameter variation Tolerant of environmental variation	Lasts a relatively long time $T \gg 0$

Source: Ryan, J.J.C.H Notes (2020)

Operational Aspects of Resiliency and Robustness

Resiliency and robustness aspects are important considerations in system design and operations. Integrating the components into a system that enhance these two attributes can be costly, which means that design trade-offs may have to be made. On the other hand, sometimes neither resiliency nor robustness are desirable attributes. For example, single use plastic kitchen waste bags are intended to be flimsy and easily degraded environmentally, although the nature of the material renders a level of robustness that is undesired (United Nations, 2018). On the other hand, material scientists have recently created a type of plastic that can self-destruct when exposed to sunlight:

Engineers at the Georgia Institute of Technology have developed a new type of plastic that can form flexible sheets and tough mechanical parts—then disappear in minutes to hours when hit by ultraviolet light or temperatures above 176 degrees Fahrenheit. … DARPA has already used the plastic to make light, strong gliders and parachutes. Last October the agency field-tested one of these vehicles: dropped from a high-altitude balloon at night, a glider successfully delivered a three-pound package to a spot 100 miles away. After four hours in the sun, it vanished, leaving behind nothing but an oily smudge on the ground. (Patel, 2019)

The example given in the story illustrates an obvious use for disappearing plastic: short term mission execution with very little forensics residue. Adversaries planning attacks on distant targets could use these types of materials to launch their attacks without leaving much behind for investigators to find. C-UAS planners might use this type of design feature as a focus for attack.

Deciding how much resiliency and how much robustness is needed for a given system is a design choice and must be made in consideration of the overall mission goals.

Measuring Resiliency and Robustness

As noted in the discussion regarding the definitions of robustness and resiliency, measurement of such attributes is only possible in relation to the system mission goals. If a system is designed for preplanned product obsolescence (Buck, 2017) (Patel, 2019), then it is right and appropriate to design it with a planned lifetime. In fact, the robustness of that product is appropriately measured in its ability to last the planned lifetime. If it does, reliably, then it can be considered robust. If there is a non-trivial chance of it failing prior to planned end of life, then it can be considered not robust. Similarly, resilience must be measured relative to the mission goals. If the mission has a goal to linger over a territory for a period of time, then resiliency can be measured in the determination of the system to react to and recover from expected problems during that period of time. These attributes must be carefully considered and designed into the system from the beginning.

How Processes can Boost Resiliency and Robustness

Resiliency and robustness do not need to be cares borne solely by single components or even single systems. Having redundant systems can boost both resiliency and robustness, if those redundant are integrated appropriately. It does no good to have redundant systems or elements if such components are equally vulnerable to expected attacks or insults. Redundant processes can additionally assist in delivering resiliency through the augmentation of learning and detection capabilities. Having redundant processing channels that double check the precision and appropriateness of the primary processing channel is a very valuable method of monitoring the state of the system and ensuring that it is operating correctly.

When Resiliency and Robustness is More Costly than Optimal

Engineering for increased resiliency and/or robustness costs resources: money, labor, energy, and space. As such, the decisions must be carefully made. In some cases, it is not possible to have precise data on the operational environment, in which case guesses must be made. For example, the scientists and engineers developing the first-generation space systems had little empirical data to work with when trying to design the desired resiliency and robustness. One thing they did know is that once the system was launched, it was going to very difficult indeed to send a repair person after it. As a result, the early systems lasted much longer than expected (Gruss, 2014).

Those satellites were very expensive, but data to inform the decision space was for all practical purposes non-existent. For most of the systems that are being designed for terrestrial purposes, ample data exists, and significantly more computing power exists to support modeling and simulation. Costs can be extrapolated for both design improvements and marginal returns on investment, giving the product manager the ability to make rational decisions on how to make the hard decisions about expenditures for resiliency and robustness. But these decisions can not be made as cookie cutter decisions: just as robustness and resiliency are only measurable relative to mission goals, so are the costs associated with providing these attributes.

When Resiliency and Robustness are Attacked

Both the presence and absence of robustness and resiliency can be used as vectors for attack. When robustness or resiliency is absent, the attacks are much more obvious. It is when the systems have been designed with robustness or resiliency in mind that the attack challenge becomes interesting.

Candidate targets to be considered include (Ryan J. J., Information Warfare: A Conceptual Framework, 1997):

- Autonomous Sensor Systems, which can be exploited to send false data back to the controlling system or used as conduits for other weapons such as viruses, logic torpedoes, and worms
- The C2 Infrastructure, which includes Civilian and Strategic Leadership, the Decision Process, Societal Support Structures such as the police, and other governmental entities like the Bureau of Land Management and the Strategic Oil Reserves. Attacking these targets can sow discord in an opponent's society, thereby fracturing the decision-making process or any consensus, deny an opponent the ability to marshal needed resources to rebuff an attack, or divert attention from other activities.

- The Communications Infrastructure, including the physical part of a communications infrastructure which includes microwave antenna towers, switching stations, telephones, radios, computers, and modems. Non-physical portions include the data, electrical systems, and management support systems.
- Logistics, including the computerized backbone that identifies supply requirements, positions materials, tracks deliveries, and schedules resources. Attacks on that backbone can severely impact the ability of the dependent forces to deploy or maintain a deployment.

There are many other targets, including the sensors and individual UAS systems, but it pays to think broadly about targets.

Types of Attacks

A system that is designed to be very robust is one that is expected to last for a long period of time, relative to its mission. The designers made the decision that it was necessary for the mission to engineer the components for enhanced robustness, which was a resource decision: simply stated, they decided it was worth the extra money, energy expenditures, labor, and time to make the system more robust. The mission needs are for it to last, to persist. Destroying or damaging such a system, then, is an obvious priority for an adversary. Discovering the relative robustness of each system is also an adversary priority, since it informs targeting decisions.

Similarly, a system that is designed to be resilient is one that has been imbued with the ability to recover quickly from challenges. For such a system, a single attack is not likely to be (very) effective. Instead, a series of attacks in intervals at a rate that overwhelms the recovery process may be appropriate. For example, the distributed denial at service (DDOS) attack concept was developed when targets began designing interfaces that were resilient to normal denial of service (DOS) attacks (Cloudflare, 2020).

Revisiting the definitions of resiliency and robustness, the very attributes provide clues as to how to craft effective attacks (see Table 4-2):

Table 4-2 Attributes v Time

	Attributes	**Time Component**
Resiliency	Ability to respond to undesired changes Ability to monitor current state Ability to learn from experiences Ability to anticipate challenges	Quick to recover to desired state ∂t ~ 0
Robustness	Insensitive to component variation Insensitive to parameter variation Tolerant of environmental variation	Lasts a relatively long time T >> 0

Source: Ryan, J.J.C.H (2020)

Attacking resiliency should focus on slowing down or compromising entirely the ability to recognize and recover from state changes. Attacking robustness may be best accomplished through sabotage in the manufacturing process. Focusing on each of these attributes provides the C-UAS planner options for consideration.

In designing appropriate attacks, the C-UAS planner needs to consider system design and system operation. Individual components of systems can prove to be the Achilles' heels of larger systems. Getting to this level of knowledge requires significant intelligence data support and analytical capability.

Cascading Effect Potential

One of the challenges associated with automated systems, such as

UASs, is that there is a huge potential for them to be used in multiple system configurations, including swarms. While the offensive potential of such swarms is large, it also provides a potential for cascading C-UAS effects. For example, if a swarm has a single controlling entity, the jamming or destruction of that single entity makes the entire swarm vulnerable. Analysis of the C-UAS potential should always consider the potential for creating effects that cascade from one system to another (Ryan, Woloschek, & Leven, Complexities in Conducting Information Warfare, 1996).

The Role of Secrecy

Because of the obvious implications of the preceding discussion, secrecy associated with all aspects of UAS operations can be a paramount consideration. UAS operators should be mindful of adversaries attempting to discover information useful to the adversaries C-UAS activities. C-UAS planners should be careful of adversaries trying to discover intent and capabilities of the C-UAS efforts. The types of secrecy considerations span operations, capability and resiliency/robustness attributes.

Operational Secrecy

Normal operations can provide hints to how resiliency and robustness are engineered into a system. When conducting UAS operations, caution might be warranted to disguise or hide operational patterns or capabilities. Obviously, the longer a system is in use, the harder this becomes and the potential for secrecy dwindles to simply secrecy regarding current operations. But even this can be valuable.

From a C-UAS perspective, observing adversary training and operational patterns can provide a great deal of information regarding capabilities and intentions. Even such apparently minor things as the types of personnel expertise being acquired or the amount of energy being used can provide clues. Clues provide lines of inquiry for potential targeting and C-UAS mission planning. Granted a huge part of the C-UAS problem is when the adversary fleet is inbound, but don’t overlook the opportunity to subvert it before it is launched.

Capability Secrecy

Hiding or disguising capabilities is always a popular choice. For C-UAS planners, care should be taken to test hypotheses thoroughly to ensure that the adversary has not managed to confound the intelligence gathering and analysis process regarding the UAS missions and capabilities.

Resiliency and Robustness Secrecy

Adversaries may go to some lengths to hide the actual nature of how robust or resilient their systems might be. In some cases, the systems may be quite frail, contrary to the data revealed by the adversary. In other cases, the systems may be much more capable and resilient than expected. In either case, the potential for a target-weapon-effects match might be affected, to the detriment of both the nature of the conflict and the geo-political stability. Getting it right is important and no information should be taken at face value.

Questions for Reflection

1. You are planning a C-UAS operation against an adversary that has very robust UASs. Your intelligence support activity has verified this level of robustness. Is your best option to try to sabotage the systems while they are in production, in the field awaiting launch, or while in flight? What are the trade-offs associated with each choice?
2. A spy has revealed that an adversary has been outfitting recreational UASs with secret surveillance capabilities. These UAS systems have been advertised during the recent holiday season at deep discounts and, as a result, the sales of the systems have sky rocketed. Part of the secret surveillance system is an AI system that detects unauthorized activity and self-destructs to avoid any information being extracted. You have been charged with coming up with a way to subvert these capabilities. What are your alternatives?
3. You are on guard duty and the alarm has just been raised that a swarm of very resilient UASs are inbound on an intelligence

collection mission. What are your options?

References

AirForceTechnology.com. (2019, June 19). *The 10 longest range unmanned aerial vehicles* (UAVs). Retrieved January 7, 2020, from AirForceTechnology.com: https://www.airforce-technology.com/features/featurethe-top-10-longest-range-unmanned-aerial-vehicles-uavs/

Bolander (ed.), D. O., & Stodden, V. L. (1986). *The New Webster's Dictionary*. New York, New York, USA: Lexicon Publications, Inc.

Buck, S. (2017, March 3). GM *invented planned obsolescence during the Great Depression, and we've been buying it ever since* . Retrieved January 30, 2020, from TimeLine: https://timeline.com/gm-invented-planned-obsolescence-cc19f207e842

Bursztein, E. (2018, May 1). *Attacks against machine learning – an overview.* Retrieved January 29, 2020, from Blog: AI: https://elie.net/blog/ai/attacks-against-machine-learning-an-overview/

Cloudflare. (2020, January 1). *What is a DDOS Attack?* Retrieved January 30, 2020, from Cloudflare Learning: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

Coram, R. (2010). *Boyd: The Fighter Pilot Who Changed the Art of War.* New York: Hatchette Book Group.

Featherman, H. (2014, March 21). *Tree Profile: Aspen – So Much More Than a Tree.* Retrieved January 30, 2020, from Blog: Trees: https://www.nationalforests.org/blog/tree-profile-aspen-so-much-more-than-a-tree

Fisher, J. (2020, January 27). *The Best Drones for 2020.* Retrieved January 29, 202, from PC Magazine: https://www.pcmag.com/picks/the-best-drones

Forsling, C. (2018, July 30). *I'm So Sick of the* OODA *Loop.* Retrieved November 6, 2019, from Task and Purpose: https://taskandpurpose.com/case-against-ooda-loop

Gambrell, J. (2020, January 11). Crash may be grim echo of US downing of Iran flight in 1988. *Minnesota Star Tribune*, p. 1.

Goel, A. (2018, February 2). *How Does Siri Work? The Science Behind Siri.* Retrieved January 29, 2020, from Magoosh Data Science Blog: https://magoosh.com/data-science/siri-work-science-behind-siri/

Gray, R. (2017, March 1). *Lies, propaganda and fake news: A challenge for our age.* Retrieved January 29, 2020, from BBC Future: https://www.bbc.com/future/article/20170301-lies-propaganda-and-fake-news-a-grand-challenge-of-our-age

Green, M. (2013, January 1). *Driver Reaction Time.* Retrieved January 29, 2020, from Visual Expert: https://www.visualexpert.com/Resources/reactiontime.html

Gruss, M. (2014, February 24). *Long-lasting Milsats Give U.S. Time to Consider Next Steps.* Retrieved January 30, 2020, from Space News: Military Space Quarterly: https://spacenews.com/39608military-space-quarterly-long-lasting-milsats-give-us-time-to-consider/

Halloran, R. (1988, July 4). The Downing of Fliight 655. *New York Times*, p. 1.

Hollnagel, E. (2016, January 1). *Resilience Engineering.* Retrieved January 30, 2020, from Erik Hollnagel Ideas: https://erikhollnagel.com/ideas/resilience-engineering.html

Huang, A. (2006, January 1). *A Holistic Approach to AI.* Retrieved January 29, 2020, from Ari Huang Research: https://www.ocf.berkeley.edu/~arihuang/academic/research/strongai3.html

James, R. (2019, October 30). *Understanding Strong vs. Weak AI in a New Light.* Retrieved January 4, 2020, from Becoming Human AI: https://becominghuman.ai/understanding-strong-vs-weak-ai-in-a-new-light-890e4b09da02

Kenton, W. (2019, February 12). *Stock Market Crash of 1987.* Retrieved January 29, 202, from Investopedia: https://www.investopedia.com/terms/s/stock-market-crash-1987.asp

Loon LLC. (2020, January 1). *Loon.com*. Retrieved January 29, 2020, from Loon.com: https://loon.com

Maurer, K., & Lau, S. (2000, February 11). *Robust Design*. Retrieved January 30, 2020, from IE 361: https://vardeman.public.iastate.edu/IE361/s00mini/maurer.htm

McCausland, P. (2019, November 9). *Self-driving Uber car that hit and killed woman did not recognize that pedestrians jaywalk*. Retrieved January 29, 2020, from NBC News: https://www.nbcnews.com/tech/tech-news/self-driving-uber-car-hit-killed-woman-did-not-recognize-n1079281

Miller, E. K. (2017, April 11). *Multitasking: Why Your Brain Can't Do It and What You Should Do About It*. Retrieved January 4, 2020, from Miller Files: https://radius.mit.edu/sites/default/files/images/Miller%20Multitasking%202017.pdf

Moisejevs, I. (2019, July 14). *Poisoning attacks on Machine Learning* . Retrieved January 29, 2020, from Towards Data Science: https://towardsdatascience.com/poisoning-attacks-on-machine-learning-1ff247c254db

Morgan, T. P. (2019, November 13). *INTEL THROWS DOWN AI GAUNTLET WITH NEURAL NETWORK CHIPS*. Retrieved January 29, 2020, from The Next Platform: https://www.nextplatform.com/2019/11/13/intel-throws-down-ai-gauntlet-with-neural-network-chips/

National Academy of Engineering. (1996). Engineering Resilience versus Ecological Resilience. In N. A. Engineering, *Engineering Within Ecological Constraints*. Washington, DC, USA: The National Academies Press.

Nichols, R. K., Ryan, J. J., & Ryan, D. J. (2000). *Defending Your Digital Assets Against Hackers, Crackers, Spies, and Thieves*. New York: McGraw Hill.

Nuance. (2020, January 1). *Dragon Speech Recognition Solutions*. Retrieved January 29, 2020, from Nuance Products: https://www.nuance.com/dragon.html

Patel, P. (2019, August 26). *Disappearing Plastics Stay Strong in the Shadows and Melt Away in the Sun*. Retrieved January 30, 2020, from Scientific American: Chemistry: https://www.scientificamerican.com/article/disappearing-plastics-stay-strong-in-the-shadows-and-melt-away-in-the-sun1/

Richards, C. (2012, March 21). *Boyd's OODA Loop: It's Not What You Think*. Retrieved July 27, 2019, from Fast Transients Files: https://fasttransients.files.wordpress.com/2012/03/boydsrealooda_loop.pdf

Ryan, J. J. (1997, January 1). *Information Warfare: A Conceptual Framework*. Retrieved January 30, 2020, from Proceedings of the 1996 Seminar on Intelligence, Command, and Control : http://www.pirp.harvard.edu/pubs_pdf/ryan/ryan-i97-1.pdf

Ryan, J. J. (1997, September 80). *Lecture Notes, EMSE 218/6540/6537*. (J. J. Ryan, Performer) George Washington University, Washington, DC, USA.

Ryan, J. J. (2001, November 12). *Security Challenges in Network-Centric Warfare*. (J. J. Ryan, Performer) George Washington University, Washington, DC, USA.

Ryan, J. J., Woloschek, J., & Leven, B. (1996, April 1). Complexities in Conducting Information Warfare. *Defense Intelligence Journal*, 5(1), 69-75.

Sampson, B. (2019, February 20). *Stratospheric drone reaches new heights*. Retrieved January 5, 2020, from Aerospace Testing International: https://www.aerospacetestinginternational.com/features/stratospheric-drone-reaches-new-heights-with-operation-beyond-visual-line-of-sight.html

Tarm, M. (2010, January 8). *Mind-reading Systems Could Change Air Security* . Retrieved March 1, 2011, from The Aurora Sentinel: http://www.aurorasentinel.com/news/national/article_c618daa2-06df- 5391-8702-472af15e8b3e.html

Tozzi, C. (2019, October 16). *Is Cloud AI a Fad?* . Retrieved January 29, 2020, from ITPro Today: https://www.itprotoday.com/cloud-computing/cloud-ai-fad-shortcomings-cloud-artificial-intelligence

United Nations. (2018, January 1). *Plastic Pollution*. Retrieved

January 30, 2020, from UN Environment: https://www.unenvironment.org/interactive/beat-plastic-pollution/

Vincent, J. (2017, April 12). *MAGIC AI: THESE ARE THE OPTICAL ILLUSIONS THAT TRICK, FOOL, AND FLUMMOX COMPUTERS.* Retrieved January 29, 2020, from The Verge: https://www.theverge.com/2017/4/12/15271874/ai-adversarial-images-fooling-attacks-artificial-intelligence

Wakabayashi, D. (2018, March 19). *Self-Driving Uber Car Kills Pedestrian in Arizona, Where Robots Roam.* Retrieved January 29, 2020, from New York Times: https://www.nytimes.com/2018/03/19/technology/uber-driverless-fatality.html

Wikipedia. (2019, December 29). *Loon LLC.* Retrieved January 14, 2020, from Wikipedia: https://en.wikipedia.org/wiki/Loon_LLC

World Monuments Fund. (2016, January 1). *The Quest to Save Segovia Aqueduct.* Retrieved January 30, 2020, from World Monuments Fund Articles: https://www.wmf.org/sites/default/files/article/pdfs/the_quest_to_save_segovia_aqueduct.pdf

Wysk, R. A., Niebel, B. W., Cohen, P. H., & Simpson, T. W. (2000, January 1). *Taguchi's Robust Design Method.* Retrieved January 30, 2020, from IE 466: Concurrent Engineering: https://www.mne.psu.edu/simpson/courses/ie466/ie466.robust.handout.PDF

PART II

SECTION 2: C-UAS TECHNOLOGIES AND PROCESSES

Chapter 5: Surveillance and Reconnaissance

H.C. MUMM

Student Learning Objectives – The student will gain knowledge of the concepts and framework as it relates to the surveillance and reconnaissance aspects of C-UAS (Counter-unmanned aerial systems). The student will be able to:

- Describe the importance of surveillance to C-UAS activities, differentiating it from reconnaissance
- Describe the importance of reconnaissance to C-UAS activities, differentiating it from surveillance
- Develop a surveillance plan for a notional C-UAS scenario, identifying processes, systems, and technologies needed, as well as mission goals and metrics
- Explain how detection of UAS is different from detection and interpretation of adversarial intent
- Explain the need for operational secrecy for C-UAS surveillance and reconnaissance activities

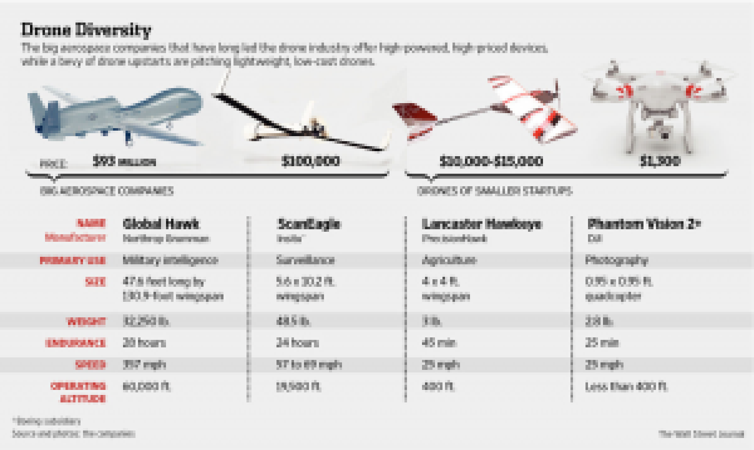
History-What is it, and Why Does it Matter?

This chapter explores the differences and similarities of how technology is used to find manned and unmanned aircraft in the sky. The history of surveillance and reconnaissance has its roots in military uses with only a small operation with its civilian counterparts. “The tactics and techniques that are applied to today’s technology stem from the field of remote sensing. Remote sensing has a long history as it began with humans attempting to see and sense phenomena from a distance and (we have now) taken a long journey from using pigeons to balloons to aircraft, then to satellites, to UAS [unmanned aerial systems]” (Nichols & Mumm, 2018)

The use of UAS or unmanned aerial vehicles (UAVs) for intelligence, surveillance, and reconnaissance is one of the most well-known applications of the technology. “The vast majority of UAVs are used purely for intelligence, surveillance, and reconnaissance (ISR) missions. In current military usage, they range from the Global Hawk, with a wingspan greater than a Boeing 737 airliner, to nano-helicopters that weigh a few grams, and all points in between” (Lambeth, 2006). This field of study has allowed advances in military movement, attack, and defend, as well as civilian surveying and developing, freedom of movement throughout our world. (Nichols & Mumm, 2018)

However, the tactics this chapter will discuss are almost 180 degrees from the normal thought process in surveillance and reconnaissance, as the “target” is up in the expansive sky and is not always bound by the rules of conventional manned aircraft, and sometimes UAS technologies evolve so quickly that counter-UAS (C-UAS) systems just cannot adapt quickly enough. “The proliferation of C-UAS technology might even accelerate the development of technologies that will render C-UAS systems ineffective, particularly in military environments” (“The new world of counter-drone technology,” 2018). C-UAS technology has two primary functions “the first is to identify or **detect** drone activity. The second function is to intercept the airspace threat or **defeat** the drone” (Friedberg, 2019)

Figure 5-1: Drone Capability Diversity



Drone Diversity

The big aerospace companies that have long led the drone industry offer high-powered, high-priced devices, while a bevy of drone upstarts are pitching lightweight, low-cost drones.

	BIG AEROSPACE COMPANIES		DRONES OF SMALLER STARTUPS	
PRICE:	$93 MILLION	$100,000	$10,000-$15,000	$1,300
NAME Manufacturer	Global Hawk Northrop Grumman	ScanEagle Insitu*	Lancaster Hawkeye PrecisionHawk	Phantom Vision 2+ DJI
PRIMARY USE	Military intelligence	Surveillance	Agriculture	Photography
SIZE	47.6 feet long by 130.9-foot wingspan	5.6 x 10.2 ft. wingspan	4 x 4 ft. wingspan	0.95 x 0.95 ft. quadcopter
WEIGHT	32,250 lb.	48.5 lb.	3 lb.	2.8 lb.
ENDURANCE	28 hours	24 hours	45 min	25 min
SPEED	357 mph	57 to 69 mph	25 mph	25 mph
OPERATING ALTITUDE	60,000 ft.	19,500 ft.	400 ft.	Less than 400 ft.

*Boeing subsidiary
Source and photos: the companies

The Wall Street Journal

Source: (Snow, 2014)

According to Merriam-Webster, the definition of reconnaissance is “a preliminary survey to gain information; *especially* an exploratory military survey of enemy territory. (Dictionary, 2019) In historical terms, it is French and means “recognition” or from Old French *reconoistre* or to “recognize” (Surveillance, 2019). This idea of a quick look or survey is in contrast with the meaning of surveillance which is “continuous observation of a place, person, group, or ongoing activity in order to gather information: attentive observation, as to oversee and direct someone or something” (Surveillance, 2019). This continuous observation does not always need to be carried out with the knowledge or consent of the surveilled as we can use electronic surveillance methods which allow for “surveillance or the gathering of information by surreptitious use of electronic devices, as in crime detection or espionage” (Surveillance, 2019)

.Furthering this idea in the C-UAS arena, one must look at not only finding an object in the vastness of the open sky but the ability to detect, classify, identify and dispatch countermeasures for not only the flying vehicle but also for the operator or base station on the ground. *Detection* means the technology can discover UAS in a given area. *Classification* of UAS will usually be able to separate UAS (drones) from other types of objects – such as manned aircraft.

"One step further is *identification.* Some equipment can identify a particular model of drone or even identify the drone's or controller's digital fingerprint, like a MAC address for example. This level of identification can be handy for (tracking and) prosecution purposes. Being *alerted* that a drone is present…is already useful. But your situational awareness, and ability to deploy countermeasures is greatly enhanced if you know the drone's (and/or the controller's) exact *location.* Some equipment will even allow you to *track* the drone location in real-time" (9 Counter-Drone Technologies To Detect And Stop Drones Today, 2019).

Table 5-2: Threat Detection Tools

Technology	Method
Radar	Detects the presence of small unmanned aircraft by their radar signatur encounters RF pulses emitted by the detection element. These systems between drones and other small, low-flying objects, such as birds.
Radio Frequency (RF)	Identifies the presence of drones by scanning for the frequencies on wh Algorithms pick out and geo-locate RF-emitting devices in the area that
Electro-Optical (EO)	Detects drones based on their visual signature.
Infrared (IR)	Detects drones based on their heat signature.
Acoustic	Detects drones by recognizing the unique sounds produced by their mo of sounds produced by known drones, which are then matched to soun environment.
Combined Sensors	Many systems integrate a variety of different sensor types in order to pr capability. For example, a system might include an acoustic sensor that a potential drone in the vicinity. The use of multiple detection elements probability of successful detection, given that no individual detection m

Source: (Michel, 2018)

Threat Identification-How and Why

The traditional ways of looking for human-made objects in the sky are radar signatures, heat signatures, visually seeing the object with the human eye, or through an optical assist mechanism. There are also acoustic signatures as well as an array of electronic signals sweeping technologies used for detection as "C-UAS systems can be ground- or air-based or even handheld. Most systems on the market today are designed only for detection or for interdiction, and the clear majority are ground-based, although a few comprise air and ground components" (Wilson, 2018). Table 5 -1 lists the main techniques for the detection and tracking of UAS.

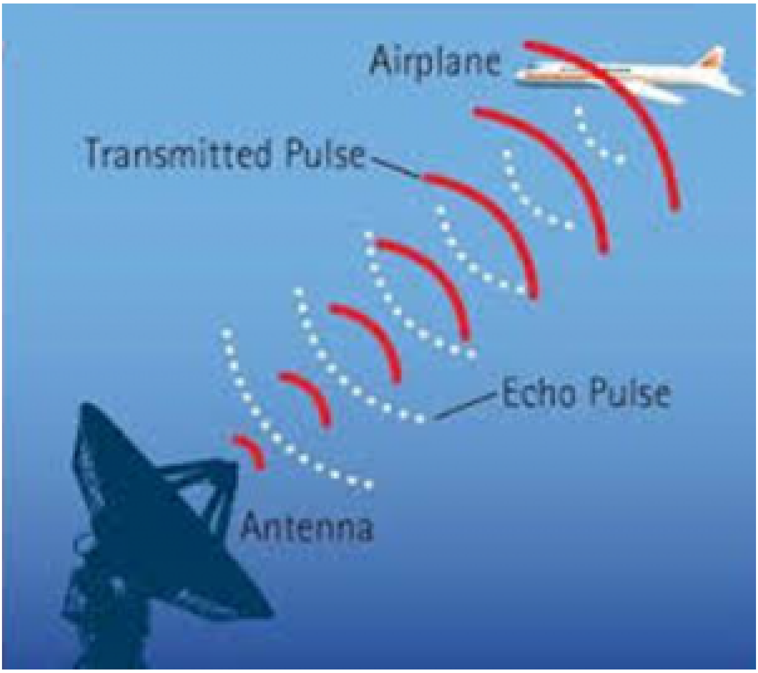
The ability to find an object in the sky is a combination of the mechanism chosen as well as the size, speed, trajectory, weather conditions and possible stealth capabilities the object may employ to avoid detection. Surveillance and reconnaissance in the C-UAS arena

includes radar, radio frequency (RF), electro-optical (EO), infrared (IR), acoustic, and combined sensors. There are no perfect detection methods. Many affordable electro-optical sensors are limited to daylight operations and a direct line-of-sight to the target (also true for IR and many RF systems). RF and acoustic sensors use a library of known sounds and frequencies to detect UAVs, but the rapid development of new platforms makes it impossible for those to be fully up to date. Sensor sensitivity also is an issue; too sensitive generates many false positives, while reduced sensitivity leads to false negatives (Wilson, 2018).

Adding to this equation is the atmospheric effects of temperature, weather conditions, and location of the object be it over an open desert, the vastness of the ocean, or mixed within the many buildings and signals within a city or urban terrain. Tracking an object in the sky is more difficult than tracking an object on land as the vastness of the sky creates the difficulty of a three dimensional environment where the object could move up, down, laterally side to side or a combination of all three dimensions as individuals and sensors attempt to find and track the object. The most common way to find and track an aircraft is through the use of radar. RADAR is an acronym for Radio Detection and Ranging. A simple explanation how radar works is:

A beam of energy, called radio waves, is emitted from an antenna. As they strike objects in the atmosphere, the energy is scattered in all directions, with some of the energy reflected directly back to the radar. The larger the object, the greater the amount of energy that is returned to the radar. In addition, the time it takes for the beam of energy to be transmitted and returned to the radar also provides is with the distance to that object. (How Radar Works., 2019)

Figure 5-2: Example of RADAR Signal



Source: (Goyal, 2019)

A radar signal has a pulse width (pulse duration), which can be increased or decreased to "see" further out or to get a better image of the object in question. The "Pulse width determines the spatial resolution of the radar… decreasing the pulse width increases signal bandwidth. A wider system bandwidth results in higher receiver noise for a given amount of power, which reduces sensitivity" (Encyclopedia Britannica, 2019). As we are working with the position of time and space of an aircraft a "Doppler radar systems can provide information regarding the movement of targets as well as their position by measuring the shift (or change) in phase between a transmitted pulse and a received echo, the target's movement directly toward or away from the radar is calculated" (How Radar Works., 2019).

Several factors affect the performance of a given radar system, these factors include

- (1) the maximum range at which it can see a target of a specified size, (2) the accuracy of its measurement of target location in range and angle, (3) its ability to distinguish one target from another, (4) its ability to detect the desired target echo when masked by large clutter echoes, unintentional interfering signals from other "friendly" transmitters, or intentional radiation from hostile jamming (if a military radar), (5) its ability to recognize the type of target, and (6) its availability (ability to operate when needed), reliability, and maintainability (Encyclopedia Britannica, 2019).

These and many other factors create issues when attempting to use radar to find and track UAS as "Echoes from land, sea, rain, snow, hail, birds, …but they are a nuisance to those who want to detect aircraft, ships, missiles, or other similar targets. Clutter echoes can seriously limit the capability of a radar system… (we must) minimizing the effects of clutter without reducing the echoes from desired targets" (Encyclopedia Britannica, 2019)

UAS tend to be small in size and have a low electromagnetic signature, which can be missed by most traditional detection measures such as an airport radar system; however, a micro-doppler radar "is able to detect movement – specifically, speed differences – within moving objects. And drones tend to have propellers that create a large spectrum of speed differences. Part of the propeller is moving towards you, and part is moving away (9 Counter-Drone Technologies To Detect And Stop Drones Today, 2019). This micro-doppler technique can identify drones and even distinguish drones from birds. UAS can also be detected by using the millimeter-wave range as this range is “ideal for surveillance tasks in the immediate environment, particularly when visibility is poor. In comparison to the optical and IR spectrum, millimeter waves have good penetration characteristics in the presence of fog, smoke, or dust.” (Caris, 2019)

Radio Frequency (RF)

Radio Frequency (RF) sensors can detect the UAS and the operator or ground station location from which the control signal or payload exploitation signal is being sent and received. Commercial drones are usually operated via a radio control signal and often have onboard data link transmitters for real-time sensor download (typically in the 2.4 GHz ISM band). These upload and download frequency signals can be detected and geolocated (Drone Detection , 2019). RF sensors are passive and do not require legal authorization for use, so they will not emit signals that can cause issues with other signal emitters in a given area. RF sensors are one of the first lines of defense in C-UAS as they can “detect commercial, consumer, and DIY or prototype drones, flight paths, and the location of drones. RF sensors are capable of identifying a drone’s type and model based on the protocol or frequency the drone is operating” (Friedberg, 2019).

Electro-Optical (EO) Sensors-Full Motion Video Cameras

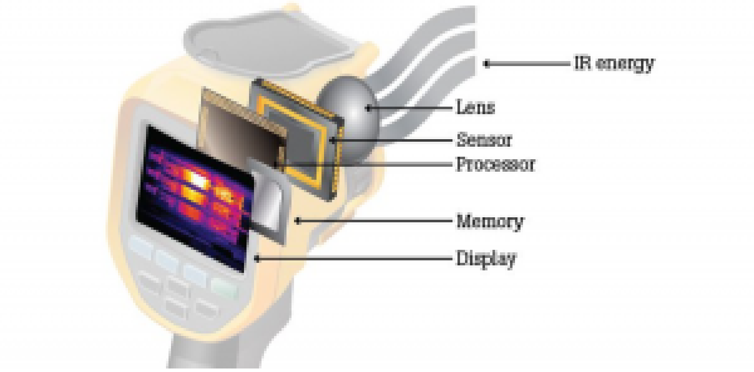
Full motion video or digitally enhanced cameras can “provide vital visual confirmation of a drone, help identify payloads, and record forensic evidence of drone intrusions. This sensor is important for times when human verification is necessary, or when security teams need visual evidence of an intrusion” (Friedberg, 2019).

Video and camera sensors are limited in their ability to find a UAS and generally need to be cued to a UAS through other sensors. Cameras are limited in a C-UAS system due to limitations of weather conditions, low visibility environments, line of sight, range, smoke environments, and nighttime operations. EO sensors are normally combined with an infrared sensor (IR) device and sold as one unit, as an EO/IR sensor.

Infrared Sensors (IR)

Infrared sensors are based on the science that “all objects emit infrared energy, known as a heat signature. An infrared camera (thermal imager) detects and measures the infrared energy of objects. The camera converts that infrared data into an electronic image that shows the apparent surface temperature of the object being measured” (Thermography Fundamentals, 2016).

Figure 5-3: Infrared Heat Signature



Source: (Thermography Fundamentals, 2016)

This temperature difference offers the ability for the sensors to surveil the aircraft in the sky as the “camera processor takes the signal from each pixel and applies a mathematical calculation to it to create a color map of the apparent temperature of the object (Thermography Fundamentals, 2016).

Acoustic Sensors for C-UAS

The concept behind acoustic sensors is based on the idea that the distinct sounds created by different aircraft can be identified and distinguished from all other sounds in a given area as “acoustic sensors use a library of known sounds and frequencies to detect UAVs, but the rapid development of new platforms makes it impossible for those to be fully up-to-date. Sensor sensitivity also is an issue; too sensitive generates many false positives” (The new world of counter-drone technology).

It’s a Big Sky-How Can We Discern the Clutter from the UAS?

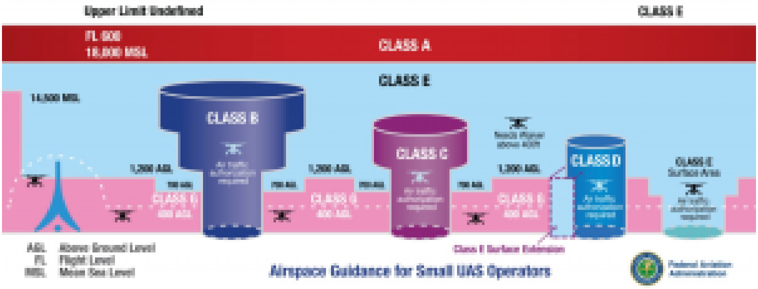
Another issue of tracking airborne objects is one or more of the objects in the sky making contact or colliding into each other; however, this is rare and is known as the Big Sky Theory. The Big Sky theory states “that two randomly flying bodies are very unlikely to collide, as the three-dimensional space is so large relative to the bodies. Some aviation safety rules involving altimetry and navigation standards are based on this concept” (Big Sky Theory, 2019).

With the “advent of radar, two aircraft could be “seen” and maneuvered clear of each other’s flight paths. The advent of Traffic Collision Avoidance System (TCAS) equipment allowed equipped aircraft to resolve conflicts. Now we have technology that allows space-based positioning of two aircraft” (Big Sky Theory, 2019).

One of the techniques to control the Big Sky Theory is assigning different types of airspace rules to control certain areas of time and space. This use of airspace allows different rules to be assigned to different environments. As an example, if an aircraft, manned or unmanned is not following the agreed-upon rules it is considered to be hazardous. Predetermined responses are employed depending on which airspace the vehicle is operating in and to what degree the vehicle is not following the agreed-upon rules.

Figure 5-4 depicts the different types of airspace and control within each of these airspace corridors. Depending upon which airspace corridor a vehicle is operating in, a series of positive controls are in place including radar tracking, mode “C” altitude encoders (allows for a unique code to be assigned to each aircraft in an area), self-reporting by operators, visual indicators and radio call signs. This concept has worked well in the manned aircraft arena as all aircraft in controlled airspace must have an altitude encoder, and “up until now means planes moving between Europe and North America have had to use regimented tracks in the sky. The rigid structure maintains large areas of clear space around planes to remove the possibility of a collision” (Amos, 2019). This concept must now become more flexible as unmanned and optionally manned technology proliferates around the world. The system is slowly evolving with the invention of Automatic Dependent Surveillance-Broadcast (ADS-B) transponders. These transponders push out information from a particular aircraft – including its identity, GPS-determined altitude, and ground speed. ADS-B was introduced to enhance surveillance and safety over land, but the messages can also be picked up by satellites (Amos, 2019).

Figure 5-4: Air Space Classification



Source: (FAA, 2019).

Table 5-3: Airspace and Altitude Definitions

Airspace	Altitude Definition
Class A	Generally, airspace from 18,000 feet mean sea level (MSL) up to and including FL600. Includes airspace overlying the waters within 12 nautical miles (NM) off the coast of the 48 contiguous United States and Alaska.
Class B	Generally, from the surface to 10,000 feet MSL including the airspace from portions of Class Bravo that extends beyond the Mode C Veil up to 10,000 feet MSL (e.g. SEA, CLE, PHX).
Class C	Generally, from the surface up to 4,000 feet MSL including the airspace above the horizontal boundary up to 10,000 feet MSL.
Class D	Generally, airspace from the surface up to 2,500 feet above the airport elevation. The configuration of each Class D airspace is individually tailored.
Class E	Above 14,500 feet MSL over the 48 United States and Alaska, excluding airspace at and below 2,500 feet AGL and excludes airspace 18,000 MSL or above. Includes airspace overlying the waters within 12 nautical miles (NM) off the coast of the 48 contiguous United States and Alaska.
Class G	Uncontrolled airspace – not designated as Class A, B, C, D, or E.

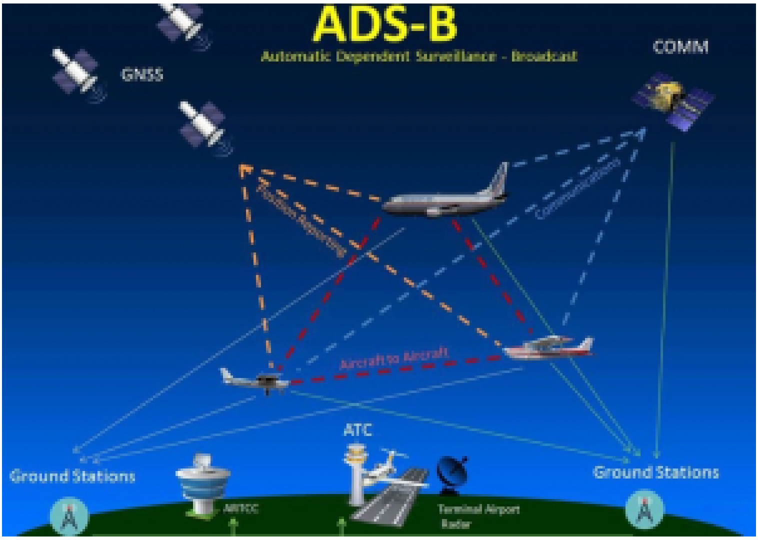
Source: (-Handbooks, 2019) [1]

Automatic Dependent Surveillance-Broadcast (ADS-B)-Helping to Eliminate the "Good Guy" from C-UAS Surveillance and Reconnaissance Challenge

The introduction of the Automatic Dependent Surveillance-Broadcast (ADS-B) will help transform surveillance and reconnaissance of manned aircraft, yet how this new technology can fit into the unmanned arena and possibly assist C-UAS is still being determined. The U.S. firm, Aireon, says "its new satellite surveillance network is now fully live and being trialed over the North Atlantic. The system employs a constellation of 66 spacecraft, which monitors the situational messages pumped out by aircraft transponders. These report a plane's position, altitude, direction and speed every eight seconds. The more detailed information they now have about the behavior of airplanes means more efficient routing can be introduced" (Amos, 2019).

ADS-B is a system of systems and rides "piggyback on all 66 spacecraft of the Iridium sat-phone service provider. These sensors make it possible now to track planes even out over the ocean, beyond the visibility of radar – and ocean waters cover 70% of the globe" (Amos, 2019). If we know where the manned "friendly" aircraft are in time and space, this may assist in the surveillance and reconnaissance of potentially harmful UAS and allow for the tracking and neutralizing of this threat. Figure 5-5 illustrates how ADS-B will operate in the next few months as the FAA (Federal Aviation Administration) has mandated that all aircraft are required to comply by January 1, 2020. This includes any aircraft operating in Class A, B, or C airspaces. Additionally, any aircraft operating in Class E airspace (above FL100 MSL but not below 2,500 ft AGL) must also comply ("The "No-BS" PDQ ABC's of ADS-B," 2019).

Figure 5-5: ADS-B Signal Broadcast



Source: (The “No-BS” PDQ ABC’s of ADS-B, 2019)

With ADS-B technology offering near-real-time surveillance from satellites, the ability to “introduce greater flexibility into the management of the airspace (become[s] possible). For example, in the North Atlantic, traditional in-line safe separation distances will eventually be reduced from 40 nautical miles (80km) down to as little as 14 nautical miles (25km)” (Amos, 2019). This flexibility offers great promise for the airline industry; however, it also complicates C-UAS, as aircraft are no longer on a known, predictable flight path. Attempting to mandate that all UAS incorporate ADS-B transponders may prove to be difficult as the technology can cost thousands of dollars, and integration into current UAS designs may not be completely successful.

The Difficulty of Differentiating Harmless Aircraft from Threat Aircraft in the C-UAS Space

How do you determine what is flying in the area-is it a bird, small plane, UAS, and is it a threat? The standard airport radar does not work well for finding and tracking most UAS. There are several reasons for this, including the size of the aircraft, the material it is made from, and the general lack of a heat signature in most of the Group 1 and Group 2 weight classes. (See also Figures 5-6, and 5-7)

Table 5-4: UAVs Classification According to U.S. DoD

UAVs Classification According to the U.S. Department of Defense (DoD)

Category	Size	Maximum Gross Ta Weight (MGTW) (lb
Group 1	Small	0-20
Group 2	Medium	21-55
Group 3	Large	<1320
Group 4	Larger	>1320
Group 5	Largest	>1320

*AGL = Above Ground Level **MSL = Mean Sea Level
Note: If the UAS has even one characteristic of the next level, it is classified at that level.

Sources: (U.S. Army Unmanned Aircraft Systems Roadmap 2010-2035, 2010)

Complicating the matter of discerning manned from unmanned systems is a multitude of ontologies and taxonomies used to discuss different sizes, weight, and mission classes of aircraft as illustrated in Tables 5-3 and 5-4. The fact that most UAS blur the line between civilian and military use (dual-use technology) compound these issues. Cohesive agreed to classifications for UAS, and manned aircraft is a worldwide issue. There is a real challenge in verifying if an aircraft is manned, definitely unmanned, or maybe optionally manned when a human must make a judgment call of life or death when determining if a UAS has nefarious intent or is simply an innocent aircraft flying in a given airspace.

Table 5-5: NATO UAS Classification

NATO UAS Classification			
Class	**Category**	**Normal Employment**	**Normal Operat Altitude**
Class III (> 600 kg)	Strike/ Combat*	Strategic/ National	Up to 65,000 ft
HALE	Strategic/ National	Up to 65,000 ft	Unlimited (BLO
MALE	Operational/ Theatre	Up to 45,000 ft MSL	Unlimited (BLO
Class II	Tactical	Tactical Formation	Up to 18,000 ft AGL
Class I	Small (>15 kg)	Tactical Unit	Up to 5,000 ft A
Mini (<15 kg)	Tactical Subunit (Manual or hand launch)	Up to 3,000 ft AGL	Up to 25 km (LO
Micro** (<66 J)	Tactical Subunit (manual or hand launch)	Up to 200 ft AGL	Up to 5 km (LO

Source: (Szabolcsi, 2016)

An airport radar normally detects aircraft as small as helicopters and single-engine land aircraft, and as large as jumbo jets, however, these all of these aircraft are generally made out of metal, have a recognizable heat signature, and a pilot that can communicate location and intent. UAS tend to have none of these attributes. Additionally, most UAS are made from plastics, balsa wood, composite materials, or combinations of all of these materials, with metal tending to be used less than any other material. Group 1 and 2 UAS tend to be battery-powered and therefore offer no discernable or trackable heat source. UAS that uses a combustible fuel engine will still not have enough of a heat signature or radar return signature to make surveillance and reconnaissance an easy task.

Figure 5-6: Size Comparison Drone to Commercial Aircraft -A

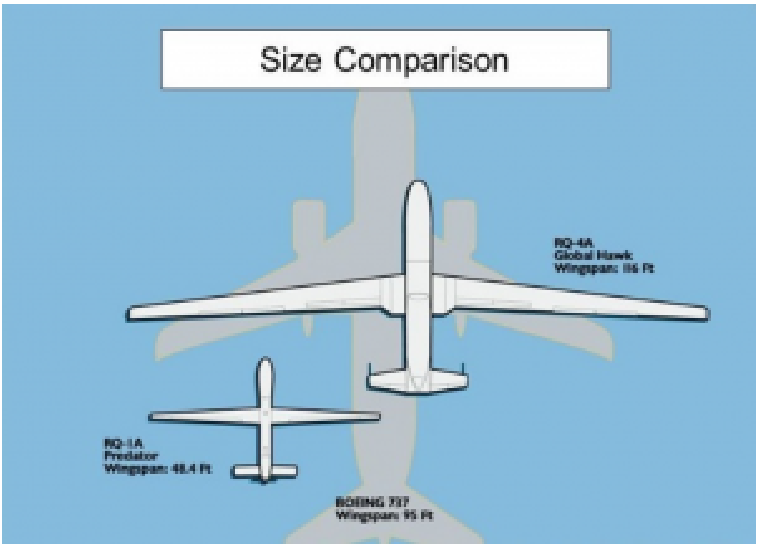
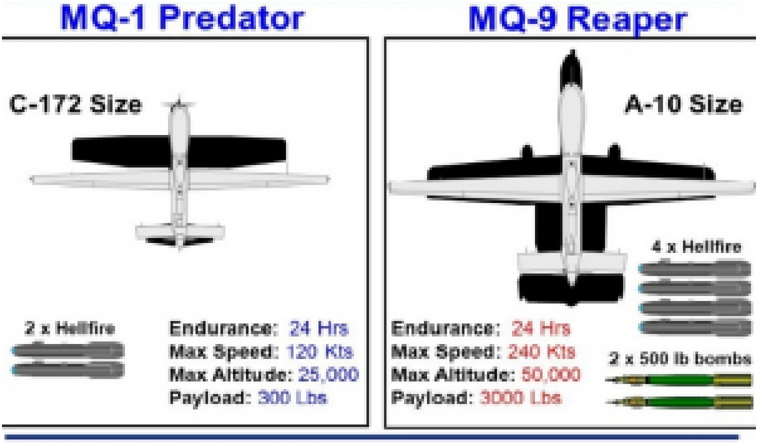


Figure 5-7: Size Comparison Drone to Commercial Aircraft -B



Sources: (Aviation-Design of UAV Systems, 2014) (Eggers)

These composite built UASs do not reflect radar energy the way denser materials such as metal does. UAVs can further reduce any energy by using composites made with radar absorbing materials (RAM) or be constructed to include a radar-absorbing structure (RAS) into the superstructure using reinforced plastics or other unique non-traditional materials. Most UAS are small enough that finding a radar signature is sufficiently difficult; however there is now “a plethora of foams and coatings that can reduce radar signature now make up a highly active sector of the microwave materials market” (Marsh, 2010).

The use of composites is not unusual in UAS as reinforced plastic materials are known for their unique combination of low weight with high strength, stiffness and fatigue resistance, but their electromagnetic (EM) characteristics are important too; witness, for example, glass fiber reinforced plastic (GRP)-based printed circuit boards and carbon composite electromagnetic interference (EMI) shielding enclosures for sensitive electronic equipment. Low-weight RAS can be made from glass and carbon fiber composite lattices in which the voids are occupied by microwave absorbent foams. Absorption effectiveness would be related to the volume fraction of the grid cell structure and the distance between elements (Marsh, 2010).

New Challenges Require New Thinking-Combined Sensors

The most successful C-UAS initiatives incorporate a multi-sensor approach to ensure the accurate identification of a UAS as

relying on just one detection method; it can be possible for a drone to be missed. For example, when using conventional radar, it can be difficult to detect low-flying drones or distinguish drones from birds. Or if the drone is obscured by buildings or trees, an optical sensor will struggle to pick it up. By augmenting the radar and optical sensors with spectrum monitoring, the security team (will) have a much clearer picture of any potential drone activity (Drone Detection , 2019).

The discussion presented here is a sampling of the technical challenges of finding and tracking UAS. The tasks of identifying the specific UAS type, aircraft owner, what the UAS is generally used for (normal payloads) and the aircraft operator become an even greater challenge as "C-UAS systems, employing combined data from several sensors, also must be able to differentiate between legitimate and hostile, allied, and enemy UASs – something no known system can do. This is where a human operator must intervene to make what often is a split-second assessment" (Wilson, 2018).

Since the early years of the FAA, the agency has mandated that manned aircraft must be registered and assigned a tail number, which must be displayed permanently on the aircraft. Information on manned aircraft is easily found in databases around the world. As a newer technology that is evolving faster than policies, laws, and governance can keep pace with, there is no comprehensive database that offers an easy UAS identification look up and even if there were such databases, the varying laws for registering the UAS (along with limited compliance) would render most of the information incomplete and unusable. New UAS are evolving at a rapid pace, and their missions are far beyond the once normal camera sensor work as UAS are taking over many traditional manned aircraft missions. This is illustrated with Boeing's aircraft refueling drone which is an "advanced unmanned aircraft designed to refuel the US Navy's fighter jets in mid-air has taken to the skies operating under the name T1, the prototype MQ-25 performed an autonomous flight over the course of two hours at MidAmerica St. Louis Airport" (Lavars, 2019). The FAA is continuing to struggle with these issues. In July 2019, many US lawmakers sent a letter to the Secretary of Transportation stating that

"We write to register our ongoing concerns regarding the continuing delay in the issuing of the Federal Aviation Administration's (FAA) rule requiring remote identification for unmanned aircraft systems (UAS) and urge you to dedicate the necessary staff and resources for the rapid publication of a notice of proposed rulemaking (NPRM) on this subject…the failure to complete Remote ID poses "serious risks" to the airspace and also "stifle innovation" in the drone industry. There are many reasons for this – the technology isn't simple, there are multiple methods and discussions over which is best, and many stakeholders in the mix" (McNabb, 2019).

This section of the chapter offers a glimpse of new technologies, tactics, techniques, and policies that are being explored to assist the difficulties in the C-UAS surveillance and reconnaissance mission areas. Technologies that were originally designed to protect military installation are being modified for C-UAS missions. The Scanning Surveillance Radar System (SSRS) is an example and is "ideally suitable for the detection and precise location of several drones of both classes (micro and mini UAS) at close range. In addition, the SSRS system offers live tracking for up to four UAS in a measurement range of 50 to 150 meters"(Caris, 2019). This technology is effective for smaller UAS; additional combined sensor technology must be used to create a full C-UAS spectrum of protection.

Many C-UAS directories exist; however, a good amount of the information is not vetted correctly or is more in an advertising format than an informative format. The Counter UAS Directory from www.unmannedairspace.info is one of the more comprehensive lists. The latest edition had 83 technologies discussed within a 54-page document. The directory is free to the public and tends to be vetted with only verifiable information listing "available counter-UAS systems, networks, and components and is supplied free of charge…Information is supplied directly by suppliers, with data edited to remove unverifiable claims" (FAA, 2019).

One of the issues that have proven to be difficult in the C-UAS arena is attempting to not only find and track a vehicle; it is attempting to find where the vehicle is being controlled from and who is controlling the vehicle. New technology is being developed to cope with this issue as “CACI’s SkyTracker® Technology Suite is a counter-small unmanned aircraft system (C-sUAS) capability comprised of different form factors designed to exploit the radio communication between small unmanned aircraft systems (sUAS) and their controller” (CACI, 2019).

The SkyTracker® has three different form factors depending on C-UAS requirements; they include the:

CORIAN system provides fixed facility protection against unmanned aircraft systems (UAS) threats to warfighters and critical infrastructure. CORIAN detects, identifies, tracks, and mitigates sUAS threats using precision neutralization techniques to ensure little to no collateral damage to the surrounding radio frequency (RF) spectrum and existing communications.

AWAIR® system provides on-the-move force or facility protection against hostile sUAS. The ruggedized mobile platform leverages the CORIAN software baseline to precisely detect, identify, and mitigate sUAS threats. The system can be easily deployed on a vehicle or marine vessel, providing both ground and maritime convoy protection.

CACI’s man-packable advanced attack system can defeat small, complex UAS. The system surveys the environment to enable deployed units to counter sUAS and analog video signals. The system can operate autonomously to deliver precision distributed attacks and provide rapid, responsive force protection capability in hostile environments (CACI, 2019).

A U.S. applied research not-for-profit company known as SRC “is applying its extensive background in electronic warfare, air surveillance, and target detection, tracking and classification algorithms to help detect, track and defend against low, slow and small unmanned aircraft system (UAS) threats” (Counter-UAS Systems, 2016).

SRC has taken this knowledge and create C-UAS technology for both the military and civilian market places.

Silent Archer® counter-UAS technology detects, tracks, identifies, and defeats hostile UAS. The technology comprises proven, radar and electronic warfare systems, a camera for visual identification of targets, and a 3-D user display to provide the warfighter with advanced situational awareness.

Small, slow, low-flying drones can easily slip through current security measures, posing an undetected threat to personnel and property. SRC's Gryphon *Skylight*® drone security solution relies on radar and spectrum sensing to detect and identify UAS, commercial aircraft, and even birds to give you a clear picture of your secure airspace (Counter-UAS Systems, 2016).

Mission Planning Secrecy – Protecting the Data

The first question in protecting the data is, does it matter if the data is seen by others? This may seem counterintuitive to this conversation; however, encrypting data carries costs that may not be needed in most C-UAS scenarios. The art of surveillance and reconnaissance tends to be done in the shadows. In the C-UAS arena it might be more advantageous to allow the information to be known by all who have access, allowing for additional informational inputs and more "eyes" on the subject aircraft. Now, the response to the subject aircraft is another matter, as individual companies and governments may not want to disclose the exact methods being employed and the effect these methods will have on the subject aircraft. Information such as acoustics signatures is important to mask and not be disclosed as today's sensor includes

a range of tracking and data collection capabilities and visualizations, including early warning alerts with target bearings, multiple simultaneous threat detection, and tracking, and 3D-track of targets. The system can be configured with multiple networked sensors to support a wide area of coverage, from remote field operations to congested urban environments. Captured data can be integrated into existing command and control software programs to support Intelligence, surveillance and reconnaissance, operations, and decision-support applications (General Atomics demonstrates acoustic drone-detector to US Army, 2019).

The nature of most UAS platforms are inexpensive and openly available components, yet these components are often:

built independently without cyber protection standards built-in leaving the systems vulnerable, and the very nature of “plug and play” tends to create incompatibility in cyber protection with very few if any true data standards.

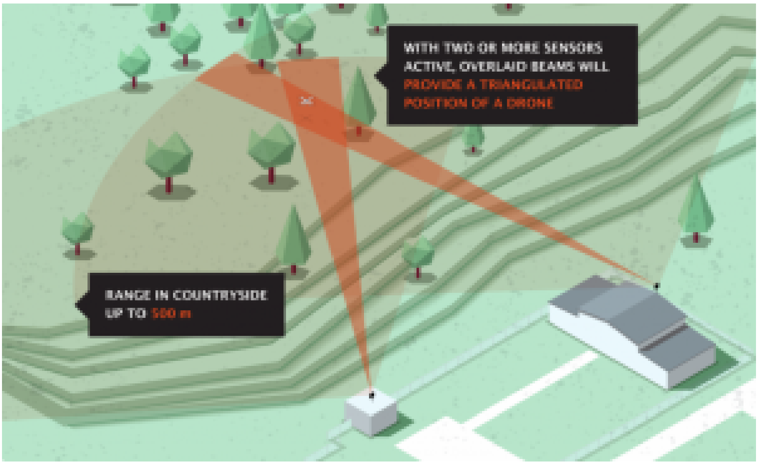
Analysis of the configuration and flight controllers/ microprocessors of several popular UAV models having multiple rotors revealed weaknesses associated with both the telemetry links streaming data to and from a drone via serial port connections (in which information could be captured, modified, or injected), and the UAVs’ connections to their ground station interface (whose data link could be spoofed, enabling hackers to assume complete control of the vehicle).” (Nichols & et.al, 2019)

Sensor data security and the threat of attacks within the cyber domain must be a part of all aspects of mission planning. Mission planning will require tradeoffs between target area access, sensor capability and availability, information time dominance, and cyber/ data security requirements.

Mission Planning for C-UAS for Perimeter Protection

Now that the foundation of combined for C-UAS has been discussed, the placement and interconnection of these sensors systems are required for triangulation of the UAS. As seen in Figure 5-8, the interlocking nature and overlap of sensors will create a triangulation of the UAS target.

Figure 5-8: Overlapping Sensor Example


WITH TWO OR MORE SENSORS ACTIVE, OVERLAID BEAMS WILL PROVIDE A TRIANGULATED POSITION OF A DRONE
RANGE IN COUNTRYSIDE UP TO 500 m

Source: (Perimeter Protection & Defense, 2019).

In protecting the perimeter of a given facility, an in-depth analysis must take place to understand the ability to obtain the security level required before surveillance and renaissance of the area can begin. Once the reconnaissance of the area is complete the surveillance of any unauthorized UAS can occur and will be digitally documented and the appropriate countermeasures taken against the offending UAS.

Combining the correct sensors (discussed earlier) will depend on many factors including:

- Topography (line of sight)
- Amount and height of buildings and human-made objects in the area
- Protection level- Provide for 24/7 operations, all-weather (or just during occupied times)
- Frequency noise level-electromagnetic interference
- Applicable laws for the area/country
- Threat level-is there known threats in the area-critical infrastructure or protecting the family business

- Most likely type of threat (quad-rotor with EO/IR sensor or fixed-wing suicide UAS)
- What are the likely responses to the threat? How does the combined sensors system verify the threat has been neutralized or has left the area and is no longer a threat?
- What is the budget for C-UAS? How much of this budget can be allocated to surveillance and reconnaissance?
- Can the sensors cover hidden areas or pockets without overlapping coverage?

Each of these factors will affect the type and number of sensors placed and how these sensors report back, store information, and are utilized during the normal course of time, or during a C-UAS threat event and the threat de-escalation and neutralization phase. Additionally, technology refresh schedules should be considered as the UAS market continues to evolve, and the tactics and techniques from threat actors get more sophisticated. The planning for C-UAS perimeter protection must be updated to match the new threats.

Conclusions

Reviewing the difference between surveillance and reconnaissance in the context of C-UAS offers distinctions between the typical thought process of sensors looking down on a target and the reality of the difficulty in attempting to find UAS targets in the vastness of the sky. The sensors that track manned aircraft are often not good at finding and tracking UAS as the size, materials, heat signatures, and overall UAS radar profiles are vastly different than of manned aircraft. The ability to discern this difference, catalog it and maintain the accuracy of the database information is imperative to avoid loss of life from an accidental mischaracterization of manned aircraft versus from a hostile UAS. The introduction of ADS-B will assist in identifying manned aircraft in controlled airspace. The transponder will also make the task of determining a threatening UAS in this airspace easier to detect and mitigate. The use of multiple sensor suites and continued innovation in this space is required to have the best chance of allowing surveillance and reconnaissance to occur in this ever-changing and growing field of UAS. The overall identification mechanisms, be it administrative or technical for UAS are issues that are still being developed through the creation or adaptation of policies, laws, and governances by aviation authorities across the globe. The ability for all aviation authorities to agree upon identification mechanisms, ontologies and taxonomies of the UAS arena along with national and international cooperation agreements offers an opportunity to positively impact the safety of the aviation community.

Questions

1. What is the difference between reconnaissance and surveillance in the context of C-UAS?
2. What airspace can UAS operate in? (Hint below 400AGL)
3. For C-UAS surveillance and reconnaissance, does the UAS size and composition matter? Why or why not?
4. How would you position multiple sensors to surveil a given area for C-UAS?
5. What is the correct sensor placement for triangulating UAS?

References

9 Counter-Drone Technologies To Detect And Stop Drones Today. (2019). Retrieved from www.robinradar.com: https://www.robinradar.com/9-counter-drone-technologies-to-detect-and-stop-drones-today

Amos, J. (2019). *Satellite plane-tracking goes global.* . Retrieved from www.bbc.com/news/: https://www.bbc.com/news/science-environment-47793983

Aviation-Design of UAV Systems. (2014). Retrieved from aviation.stackexchange.com: https://aviation.stackexchange.com/questions/43780/why-arent-there-any-single-turbofan-airliner

Big Sky Theory. (2019). Retrieved from www.apstraining.com:

https://www.apstraining.com/resource/the-big-sky-theory-luck-and-loss-of-control-in-flight/

CACI. (2019). *SkyTracker® Technology Suite.* Retrieved from www.caci.com/skytracker/: http://www.caci.com/skytracker/

Caris, M. (2019). *Detection of Small Drones With Millimeter Wave Radar* . Retrieved from www.fhr.fraunhofer.de/en/businessunits/security/: https://www.fhr.fraunhofer.de/en/businessunits/security/Detection-of-small-drones-with-millimeter-wave-radar.html

Counter-UAS Systems. (2016). Retrieved from www.srcinc.com: https://www.srcinc.com/about/index.html

Dictionary, M.-W. (2019). *Definition of Reconnaissance.* Springfield, MA: Merriam-Webster, Inc.

Drone Detection . (2019). Retrieved from www.crfs.com/drone-detection/: https://www.crfs.com/drone-detection/

Eggers, J. (n.d.). *MQ-1 Predator/MQ-9 Reaper Unmanned Aircraft Systems.* Retrieved from slideplayer.com/: https://slideplayer.com/slide/5070244/

Encyclopedia Britannica. (2019). *Factors Affecting Radar Performance.* Chicago IL: Britannica Group.

FAA. (2019). *Airspace 101 – Rules of the Sky.* Retrieved from www.faa.gov/uas/: https://www.faa.gov/uas/recreational_fliers/where_can_i_fly/airspace_101/

Friedberg, S. (2019). *CUAS Technology Series: Detection Hardware.* . Retrieved from www.dedrone.com/blog/: https://www.dedrone.com/blog/cuas-technology-series-detection-hardware

General Atomics demonstrates acoustic drone-detector to US Army. (2019). Retrieved from www.unmannedairspace.info/: https://www.unmannedairspace.info/counter-uas-systems-and-policies/general-atomics-demonstrates-acoustic-drone-detector-us-army/

Goyal, S. (2019). *airport-surveillance-radar.* Retrieved from www.jagranjosh.com/: https://www.jagranjosh.com/general-knowledge/airport-surveillance-radar-1551178752-1

-Handbooks, F. (2019). *Airspace.* Retrieved from www.faa.gov/regulations_policies/handbooks_manuals/aviation: https://www.faa.gov/regulations_policies/handbooks_manuals/aviation/phak/media/17_phak_ch15.pdf

How Radar Works. (2019). Retrieved from www.weather.gov/jetstream/how: https://www.weather.gov/jetstream/how

Lambeth, B. S. (2006). *Air Power Against Terror: America's Conduct of Operation Enduring Freedom.* Santa Monica, CA: RAND Corporation.

Lavars, N. (2019). *Boeing's aircraft refueling drone flies for the first time.* Retrieved from newatlas.com/military/: https://newatlas.com/military/boeings-aircraft-refueling-drone-first-flight/

Marsh, G. (2010, Volume 54, Issue 6, November–December). Going Stealthy with Composities. *Reinforced Plastics*, pp. Pages 30-33.

McNabb, M. (2019, July 10). U.S. *Lawmakers Express Frustration With Drone Remote ID Delay, "This Summer" Says Standards Committee Chair.* Retrieved from dronelife.com: https://dronelife.com/2019/07/10/u-s-lawmakers-express-frustration-with-drone-remote-id-delay-this-summer-says-s

Michel, A. (2018, February). *CSD-Counter-Drone-Systems-Report.* Retrieved from dronecenter.bard.edu/: https://dronecenter.bard.edu/files/2018/02/CSD-Counter-Drone-Systems-Report.pdf

Nichols, R. K., & Mumm, H. C. (2018). *Unmanned Aircraft Systems (UAS) in the Cyber Domain: Protecting* USA's *Advanced Air Assets.* Manhattan, KS: New Prairie Press /21/.

Nichols, R., & et.al. (2019). *Unmanned Aircraft Systems in Cyber Domain: Protecting USA's Advanced Air Assets, 2nd Edition.* Manhattan, KS: NPP Press /27.

Perimeter Protection & Defense. (2019). Retrieved from www.sqhead.com/drone-detection/: https://www.sqhead.com/drone-detection/#1533491859389-4d070f8f-97fb

Snow, C. (2014, February 6). *Making Sense of Drones.* Retrieved from droneanalyst.com: http://droneanalyst.com/2014/02/06/making-sense-of-drones

Surveillance, D. o. (2019). *Definition of Electronic Surveillance.* Detroit, MI: Rock Holdings, Inc.

Szabolcsi, R. (2016). Beyond Training Minimums – A New Concept of the UAV Operator Training Program. *International conference* KNOWLEDGE-BASED ORGANIZATION, 22. doi:doi:10.1515/kbo-2016-0096

The "No-BS" PDQ ABC's *of* ADS-B. (2019). Retrieved from murfreesboroaviation.com/: https://murfreesboroaviation.com/no-bs-pdq-abcs-ads-b/

The new world of counter-drone technology. (n.d.). Retrieved from www.militaryaerospace.com/unmanned/: https://www.militaryaerospace.com/unmanned/article/16707131/the-new-world-of-counterdrone-technology

Thermography Fundamentals. (2016). Retrieved from www.fluke.com/en-us/: https://www.fluke.com/en-us/learn/best-practices/measurement-basics/thermography

U.S. Army Unmanned Aircraft Systems Roadmap 2010-2035. (2010). Fort Rucker, AL: US : U.S. Army.

Wilson, J. (2018, November 1). *the-new-world-of-counterdrone-technology.* Retrieved from www.militaryaerospace.com: https://www.militaryaerospace.com/unmanned/article/16707131/the-new-world-of-counterdrone-technology

[1] ** Starting January 1, 2020, aircraft must be equipped with ADS-B Out to fly in most controlled airspace. ("Airspace," 2019) See http://www.asy.faa.gov/safety_products/airspaceclass.htm for additional information.

Chapter 6: C-UAS Evolving Methods of Interdiction

CANDICE CARTER

Student Learning Objectives

There are several goals for student learning in this chapter:

1. To understand the need for Interdiction in C-UAS,
2. To see the need to increase security UAS Supply chain management potentially using Blockchain,
3. To dig into the Blockchain process and understand its strengths and vulnerabilities and its relationship to aircraft communications,
4. To recognize the hurdles that Blockchain may face like 5G and public acceptance.

Why is Interdiction Needed?[1]

Unmanned aircraft receives external communication through radar. There are four different types of radar: active (using the drone's transmitter or illuminator), passive (using another drone's transmitter), basic (from one location) and multistatic (when the radar transmitter and receiver are at different locations) (Chantz, 2016). In addition, radar is used with a measure of signals and patterns to direct the drone out of harm's way. This communication process is based on a network of trust. GNSS/GPS jamming, and spoofing are methods that compromise the blind aviation trust of the external communications the unmanned aircraft receives. Other methods of electronic compromise have created a challenge when addressing C-UAS.

Methods of interdiction should be one step ahead of the unmanned aircraft industry to become an effective offensive security measure.

What is a Blockchain?

Most people associate blockchain with cryptocurrency, not all blockchains are created with the same product in mind. At the most basic level, every blockchain is a digital ledger of transactions that take place on a peer-to-peer network with the ability to control visibility – who has permission to see which data (Marx, Sealy, & Thompson, 2019). Each step the transaction makes through the supply chain it is assigned an encrypted block. Each block contains information about a certain number of transactions, a reference to the preceding block in the blockchain, and an answer to a complex mathematical challenge known as the "proof of work". The concept of proof of work is used to validate the data associated with that particular block as well as to make the creation of blocks computationally "hard", thereby preventing attackers from altering the blockchain in their favor (Ferrer, 2017)

The blockchain network has four main components viz, asymmetric cryptography and node applications, transactions and blocks, the distributed ledger, and the consensus mechanism

Blockchain is can be considered trustless, since the transaction participates do not require trust. Inversely to digital certificates, which a client trusts the certificate presented by a certificate authority on behalf of a website, to conduct secure transactions.

Figure 6-1: Blockchain in Supply Chain Management

Blockchain in Supply Chain Management
Transaction Settlement
Audit Transparency
Tracking Social Responsibility
Accurate Costing Information
Better Shipping Data
Preventing Compliance Violations
Provenance
Reducing Human Error
Automated Purchasing & Planning
Automation
Enforcing Tariffs & Trade Policies
Food Safety
Reducing Counterfeit Goods

Source: (3i Infotech, 2019)

The Process of Blockchain Synchronization

The advantage of decentralization and the distribution of information in the blockchain is also a vulnerability. Depending on the implemented framework of blockchain, the scalability and consensus becomes more challenging to guarantee performance of the blockchain process. Below is a list of parameters that determine synchronization mechanism between nodes in a distributed system (consensus mechanism) (Bogdanov, et al., 2018):

- **Decentralized governance:** a single central authority cannot ensure the completion of a transaction.
- **Quorum structure:** Nodes exchange messages in predestination (paths that may include steps or levels).
- **Authentication:** this process provides the means to verify the identity of participants.

- Integrity: it provides verification of the integrity of a transaction (for example, mathematically by means of cryptography).
- **Non-repudiation:** provides a means to verify that the intended sender actually sent the message.
- **Privacy:** this helps ensure that only the intended recipient can read the message.
- **Fault tolerance:** The network works efficiently and quickly, even if some nodes or servers do not work or are slow.
- **Performance:** considers bandwidth, survivability, scalability and latency.

The blockchain is not full proof from attacks. Established chains of reliable users can be used to carry out a third-party attack (Bogdanov, et al., 2018). Also, there is the possibility of including third parties as an additional node of the Blockchain system with the participation of an unscrupulous partner of a streamlined chain (Bogdanov, et al., 2018).

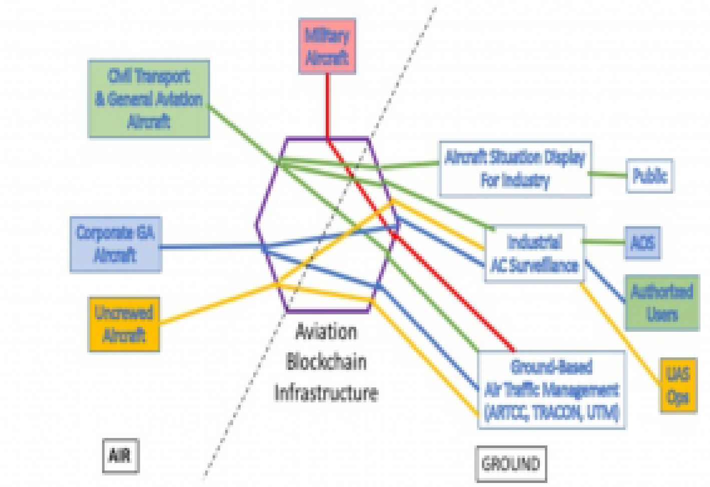
Blockchain Aircraft Communication

Announced in 2018, as of January 1, 2020, the FAA will now enforce the mandatory installation of Version 2 ADS-B Out system to fly in most controlled U.S. airspace. The ADS-B system uses GPS satellites verses the traditional ground-based radar. The advantage of GPS based system, FAA will be able to see information such as registration number, precise location, aircraft dimensions, etc. However, the rules were published May 27, 2010 and the DOD submitted comments to the FAA of ADS-B compromising the safety of special flights and missions. This lag in time is significant in understanding the threat that emerged over the past ten years, before implementation the ADS-B out system can be considered already out of date.

On January 12, 2020, Ronald J. Reisman (NASA Ames Research

Center) published research entitled,” Air Traffic Management Blockchain Infrastructure for Security, Authentication, and Privacy “. Mr. Reisman outlines the vulnerabilities of ADS-B for civil and military aviation and provides the solution of blockchain. “The design innovation is the use of an open source permissioned blockchain framework to enable aircraft privacy and anonymity while providing a secure and efficient method for communication with air traffic services, operations support, or other authorized entities,” Notes Mr. Reisman (Global Business Outlook, 2020). Mr. Reisman’s scalable framework will include certificate authority, smart contract support, and higher-bandwidth communication channels for private information that may be used for secure communication between any specific aircraft and any particular authorized member (Global Business Outlook, 2020) The blockchain would essential provide a method to encrypting the ADS-B transmissions. Aviation Blockchain Infrastructure (ABI) design that enables aircraft to communicate effectively, securely, and privately with air traffic management and other properly authorized entities (Reisman, 2019). In the case of unmanned aircrafts, blockchain brings security to Radio Frequency by keeping a high-speed, assured ledger of airspace activity and information regarding the drone and its operator, and distributing it to all appropriate parties (Chantz, 2016).

Figure 6-2: Notional Design of Blockchain-Mitigated Channels of Communication


Military Aircraft
Civil Transport & General Aviation Aircraft
Aircraft Situation Display For Industry
Public
Corporate GA Aircraft
Industrial AC Surveillance
AOS
Authorized Users
Uncrewed Aircraft
Aviation Blockchain Infrastructure
Ground-Based Air Traffic Management (ARTCC, TRACON, UTM)
UAS Ops
AIR
GROUND

Source: (Reisman, 2019)

Figure 6-2 shows the Notional design of blockchain-mitigated channels of communication. Chain code (aka 'Smart Contracts') routes the information appropriately between aircraft and the ground-based ATM and other support services (Reisman, 2019).

ABI proposed by Mr. Reisman is based on Hyperledger Fabric, a Linux based opensource tools and blockchains with contributions from Intel, IBM, and SAP. Hyperledger Fabric allows for the creation of a private and permissioned blockchain. Through services called "private channels" as a means to communicate private information at a comparatively high bandwidth. These private channels may be used to pass a private key (or time-key data structure) suitable for encrypting ADS-B Out transmissions between any specific aircraft and any particular authorized member in accordance with the terms of the smart contracts associated with the particular private channel (and subnet). The use of ciphertext enables ADS-B users to maintain privacy and anonymity from general public while also providing a secure and efficient method for communication with authorized entities, such as Air Traffic Services or Airline Operations Services (Reisman, 2019).

Blockchain to encrypt ADS-B transmissions is in the testing phases. While this is a solution for right now, we need to look ahead to understand how blockchain, as ADS-B could become present new risks verses a solution in particular verticals of aviation.

Blockchain Vulnerabilities

First document blockchain successful hack occurred in 2011. A simple case of compromised credentials. Victorious hacks of blockchains have continued along with the sophistication of attacks. Manipulation of signatures, overwriting transactions, etc. Prominently the attacks on blockchains come back to one of the basic security issues that no vertical has solved, compromise of the company employees and systems. It is amazing to see social engineering techniques that can date back to the days of Frank Abagnale Jr. are still just as effective as they were in 1960's. A simple act of piggybacking through a secure door, picking up items that were left on the printer, and photographic diagrams with IP addresses can lead to a system's compromise. Below are additional blockchain attacks that could lead to breaking the blockchain:

Blockchain Attack Scenarios (Anwar, 2019)

- A 51% Attack

> The majority of Blockchains use the prove of work to communicate the verified transactions in the block. The mining for the prove of work entails the nodes spend large amounts of computing power to prove themselves trustworthy enough to add information about new transactions to the database (Orcutt, February)

- Blockchain Protocol Code Bugs

  Bad actors exploit those loopholes

- Routing Attacks

  Bad Actors can intercept communication channels with a compromise of ISP

- Smart Contract Bugs/Compromise

  If a smart contract is changed it the blockchain is gravely impacted. Since transactions cannot be undone, a “fork” in the blockchain (a new branch of the blockchain) will need to occur to bring the process back up.

- Sybil Attack

  The attacker is running multiple fake nodes on a blockchain network that can block receiving and transmission of blocks.

- Direct Denial of Service (DDoS)

  Flooding the network with requests to stop all functions. There are critics that claim the decentralization of the blockchain reduces the risk of DDoS. However, several successful attacks DD0S on blockchains have taken place.

Blockchain Unmanned Aircrafts

Blockchain brings new functionality to the unmanned aircraft industry. The UAS vertical has struggled with air traffic control, identity management, insurance, and security. In march 2017, IBM patent filing outlines using distributed ledger technology (blockchain) can provide effective techniques for managing data related to commercial and recreational drones, particularly when a security risk level is considered to be relatively high (Cant, 2019).

IBM was not alone, Intel, Accenture, and numerous individuals applied for unmanned aircraft technology patents. Walmart out applied all organizations with their unmanned aircraft technology patents. From pizza cooking delivery to compromise of communication while delivery is in progress.

U.S. Unmanned Aircraft Patents

The patents filed over the past seven years referencing unmanned aircrafts and blockchain give an indication of the direction of the technology. China globally leads the way with 62% of the blockchain patents applications (IAM, 2019). The United States is at a mere 22% globally with blockchain patents applications (IAM, 2019). However, Korea grants 54 % of the blockchain patents filed (IAM, 2019). These numbers are concerning for the United States, blockchain security and process will be the future of all verticals not just in the drone industry. Highlighted below are a few of the newsworthy United States patents.

IBM patent application for *Unmanned Aerial Vehicle Date Management* highlights the use of blockchain securing the unmanned aerial data. "The chain can be considered a chronicle of a UAV's path through time. When a transaction is conducted, the corresponding UAV parameters are sent to one or more of the computing nodes in the system for validation. The one or more computing nodes establish a validity of the transaction and generate a new block. Once the new block has been calculated, it can be appended to the stakeholder's UAV blockchain. Among many other advantages, the use of a blockchain infrastructure helps in identifying misbehaving UAVs by multiple parties and such activities are recorded in an immutable ledger." (United States of America Patent No. US2018/027024A, 2019)

One of Walmart's patents outlines security for electronic communications in connection with a package delivery. "Authentication can be performed at the delivery communication and control system and/or other security systems by visual recognition such as facial recognition, biometric fingerprint analysis, and so on, audio recognition such as voice signatures, biometric recognition via a fingerprint or retinal scanning device (not shown) at the unmanned vehicle, blockchain recognition for scanning a blockchain signature or key for authentication, and so on." (United States of America Patent No. US2018/0205682A, 2018). In 2019, Walmart filed a patent application for Cloning Drones Using Blockchain. This Walmart patent application focuses on data integrity, "A blockchain ledger may store any kind of information that may be stored in any other format or medium, for example, a large list of instructions of different types, navigational information, and maps. In such a way, a same software profile may be deployed across the cloned drone" (Foxley, 2019)

Countering a Blockchain Unmanned Aircraft Attack

Published research of countering a blockchain unmanned aircraft attack is a sparse. However, a counter technique can be developed by applying known flaws of blockchain technology. A successful attack involves multiply vectors. Using the following vectors an affective counterattack can be formulated:

- If blockchain is used for synchronized unmanned aircraft attack by a bad actor, it can be determined the decentralized algorithm requires will require significantly lower communications bandwidth. Therefore, sharing intel on obstacle-free regions in their immediate vicinity (Ferrer, 2017).

- As referenced in the beginning of the chapter, SSL certificates are used encrypt the blockchain. When a flaw in the encryption algorithm arises, or as computing power continues to become stronger, the encrypted data may then be decrypted to reveal private details (Fitzpatrick, 2019). In 2017, industry drone manufacture DJI had an incident of SSL certificate leak. Leading cloud security systems, for example Imperva's Incapsula, compromised undisclosed amount of customer SSL certificates. Imperva has seven out of 10 global telecom providers, half of the top ten United States commercial banks, along with other prominent industries (Imperva, 2018).

- The UAV sensor system consists of the sensory equipment of the UAV together with integrated pre-processing functionalities. For common military UAVs these sensors are often cameras with different capabilities. UAVs may be equipped with further sensors, such as INS, GPS and radar (Hartmann & Steup, 2018). Sensors with external references are more susceptible to jamming and spoofing than sensors with internal references. External references generally impose a risk to the integrity of the system (Hartmann & Steup, 2018).

Taking these vulnerabilities into consideration the following steps can be used to counter a blockchain unmanned aircraft attack. The methods below are homegrown hacking methods and purchased commercial solutions.

- Skyjack Drone Hack, developed by hacker and researcher Samy Kamkar. Drone that flies around seeking Seeks wireless signal of any other drone in area. Forcefully disconnects wireless connection of true owner of target drone. Authenticates with target drone pretending to be its owner (O'Malley, 2019)
- SSL interception proxy using Burp Suite, using the steps below (Vanunu, Barda, & Zaikin, 2018):

1. Open our Burp Suit Certificate and cast it to X509Certificate.
2. Load a KeyStore and put the certificate inside.
3. Create TrustManagerFactory and initialize it with the KeyStore we just created that contains our Burp Suit certificate.
4. Overload the SSLContext and hook the TrustManager with our TrustManager.

- Sensor Jamming: disruption to inter–drone communications by manipulating UAS onboard sensors can be archived by Sensor Jamming. Jamming sensors can impact GPS signals by giving false GPS information (camera/gimbal dislocation, heading sensor demagnetization, etc.). "High intensity light directed at an optical sensor can blind it. GPS receivers can be cyber-spoofed, which consists of transmitting a stronger, but false, GPS signal to a receiver, resulting in inaccurate navigation. Influencing the local magnetic field can have adverse effects on both onboard hard drives and sensors that require magnetic orientation to operate correctly." (Boutros, 2015)(Humphreys, 2012)

Using proven techniques of signal jamming, SSL interception proxy, and sensor jamming potentially counter a blockchain unmanned aircraft attack. Evolving technology will continue to change the characteristics of blockchain but the basic concept gives the layout of the process.

Next Counter-UAS Hurdle – 5G Communication, Blockchain, Unmanned Aircrafts

What will the combination of 5G Communication and Blockchain bring to UAS? Counter-UAS? 5G is the fifth-generation mobile network (Qualcomm, 2020). 5G is a unified platform that will support a larger range of bands (1GHz to millimeter-wave) and 100% more traffic with latency of 1ms, along with other improvements.

The combination of 5G and blockchain will enable traffic management to geofence unmanned aircrafts. "…envision the use of the emerging 5G networking technology for that. 5G networking technology is the next generation of cellular networks. It is designed to provide much higher speed—larger bandwidth and smaller latency—higher reliability and the ability to serve a larger number of users, in comparison to 4G. To do that, the radio spectrum is partitioned into bands, with different frequencies—from low to extremely high." (Tasevski, 2018). Blockchain will be used to reach the consensus in the environment. 5G integrated at all levels of UAS (physical, network, and joint communication) and blockchain will bring greater control to air traffic management. China based studies have researched the creation of UAS-based antenna array system with high data rate and low service time can be created using 5G. The UAS-based antenna data will be protected by blockchain (Bin Li & Zhang, 2019). In the publication of *Unmanned Aircrafts in the Cyber Domain*, (by the authors of this publication) gives the use case of a cyber weapon deployed from a small UAS. The research points to the use of this UAS cyber weapon to cause the 2017 collusions of U.S. Navy Warships with commercial vessels. When reviewing the research of that incident combined with the creation of UAS-based antenna with 5G and blockchain, the threat level of advanced attack of vessels increases. Just this incident alone justifies the need for offensive security to be a priority for UAS commercial, military, and hobbyist.

Figure 6-3: 5g Communications/ Blockchain Geofence for the Financial District of Manhattan NYC

Source: (Tasevski, 2018)

Challenges Facing Interdiction Methods for C-UAS

Unmanned aircrafts hobby, military and commercial have their own unique attack methods, impacts, and risks. Geographic location, event, and intention can determine the method of prohibiting a drone attack. From a nation-state conflict to an outdoor concert, reviewing the scenarios and using a risk model can highlight the efficacy between C-UAS methods. With the addition of blockchain, 5G communication, and the evolution of UAS technology the risks/threats increase. Per contra, blockchain and 5G communication presents a substantial threat for the creation of an effective C-UAS.

Conclusions

Blockchain represents a disruptive security technology that may significantly improve the C-UAS supply chain management. It also faces some stiff challenges because of inherent vulnerabilities. Blockchain and 5 G communications are a mixed blessing and with increased UAS technology, comes increased threats.

References

3i Infotech. (2019, March 26). *Why you must Modernize your Supply Chain Management with Blockchain*. Retrieved from 3i Infotech Limitless Excellence: https://www.3i-infotech.com/must-modernize-supply-chain-management-blockchain/

Anwar, H. (2019, November 17). *101 Blockchains Reviews*. Retrieved from 101 Blockchains: https://101blockchains.com/blockchain-hacked/

Bin Li, Z. F., & Zhang, Y. (2019, January 20). *UAV Communications for 5G and Beyond: Recent Advances and Future Trends*. Retrieved from ARXIV: https://arxiv.org/pdf/1901.06637.pdf

Bogdanov, A., Degtyarev, A., Korkhov, V., Kamande, M., Iakushkin, O., & Khvatov, V. (2018). *ABOUT SOME OF THE BLOCKCHAIN PROBLEMS*. Saint Petersburg: Saint Petersburg State University.

Boutros, D. (2015, May 15). *Operational Protection from Unmanned Aerial Systems*. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a621067.pdf

Cant, J. (2019, November 29). *Cointelegraph News*. Retrieved from Cointelegraph: https://cointelegraph.com/news/ibm-files-a-blockchain-patent-for-fighting-package-theft-by-drone

Chantz, H. (2016, August 25). *Security Inteligence Manframe*. Retrieved from Security Inteligence : https://securityintelligence.com/using-blockchain-to-address-drone-cybersecurity/

De Wilde, W., Cuypers, G., Sleewaegen, J.-M., Deurloo, R., & Bougard, B. (2016). *GNSS Interference in Unmanned Aerial Systems*. Belgium: Septentrio Satellite Navigation.

Ferrer, E. C. (2017). *The blockchain: a new framework for robotic swarm systems*. Cambridge: MIT Media Lab.

Fitzpatrick, L. (2019, February 4). *Forbes A Haackers Take on Blockchain Security*. Retrieved from Forbes: https://www.forbes.com/sites/lukefitzpatrick/2019/02/04/a-hackers-take-on-blockchain-security/#2c788dbd4334

Foxley, W. (2019, August 14). *Coindesk Markets*. Retrieved from Coindesk: https://www.coindesk.com/walmart-files-patent-application-for-blockchain-backed-drone-communication

Global Business Outlook. (2020, January 20). *Global Business Outlook Technology Top Stories*. Retrieved from Global Business Outlook: https://www.globalbusinessoutlook.com/nasa-to-use-blockchain-technology-for-air-traffic-management/

Hartmann, K., & Steup, C. (2018, October 26). NATO CCD COE. Retrieved from The Vulnerability of UAVs to Cyber Attacks – An Approach to the Risk Assessment: https://ccdcoe.org/uploads/2018/10/26_d3r2s2_hartmann.pdf

Heue, R. (2018, June 2). *GNSS Jamming and Spoofing: Hazard or Hype?* Retrieved from Space of Innovation: https://www.space-of-innovation.com/gnss-jamming-and-spoofing-hazard-or-hype/

Humphreys, T. (2012). *STATEMENT ON THE VULNERABILITY OF CIVIL UNMANNED AERIAL VEHICLES AND OTHER SYSTEMS TO CIVIL GPS SPOOFING*. Austin: The University of Texas .

IAM. (2019, July 23). *IAM Patents*. Retrieved from IAM: https://www.iam-media.com/patents/revealed-countries-leading-race-blockchain-patents

Imperva. (2018, July 9). *Imperva Company Overview*. Retrieved from Imperva: https://www.imperva.com/resources/datasheets/Imperva_Company_Overview.pdf.pdf

Kumar, A., Kundu, A., Pickover, C., & Weldemariam, K. (2019). *United States of America Patent* No. *US2018/027024A*.

Ledger Insights. (2019, December 20). Retrieved from Ledger Insights Enterprise Blockchain News: https://www.ledgerinsights.com/us-air-force-blockchain-cybersecurity-xage/

Lufthansa Group. (2018, September 25). *Newsroom Lufthansa Group*. Retrieved from Lufthansa Group: https://newsroom.lufthansagroup.com/english/newsroom/news-releases/all/lufthansa-and-sap-select-the-nine-finalists-for-the-world-s-first-aviation-blockchain-challenge/s/b2a97099-b65b-46f6-94a3-1e6bacf5e62f

Marx, C., Sealy, R. P., & Thompson, S. (2019, July 7). *How blockchain can improve the aviation industry*. Retrieved from Strategy-Business: https://www.strategy-business.com/article/How-blockchain-can-improve-the-aviation-industry?gko=9e976

McCarthy, S., Zheng, W., & Tsang, D. (2018, October 29). *Hong Kong Society*. Retrieved from South China Morning Post: https://www.scmp.com/news/hong-kong/law-and-crime/article/2170669/hk13-million-damage-caused-gps-jamming-caused-46-drones

O'Brien, J., & High, D. (2018). *United States of America Patent No. US2018/0205682A*.

O'Malley, J. (2019, February 18). *E&T Engineering and Technology*. Retrieved from Take me out: creating 'No-Drone Zones' around airports: https://eandt.theiet.org/content/articles/2019/02/take-me-out-creating-no-drone-zones-around-airports/

Orcutt, M. (Feburary, 19 2019). *MIT Technology Review*. Retrieved from MS. Tech MIT Technology Review: https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/

Qualcomm. (2020). *Everything You Need to Know About* 5G. Retrieved from Qualcomm: https://www.qualcomm.com/invention/5g/what-is-5g

Reisman, R. J. (2019). *Page 1 1Air Traffic Management Blockchain Infrastructure forSecurity, Authentication, and Privacy.* Mountian View: NASA Ames Research Center.

Tasevski, S. (2018, December 3). *Herding Drones with Blockchains and* 5G. Retrieved from Drone Below: https://dronebelow.com/2018/12/03/herding-drones-with-blockchains-and-5g/

Vanunu, O., Barda, D., & Zaikin, R. (2018, November 8). *Check Point Research*. Retrieved from Check Point: https://research.checkpoint.com/2018/dji-drone-vulnerability/

Endnotes

[1] *prohibiting or forbidding intercepting and preventing the movement of something.*

Chapter 7: UAS Area / Airspace Denial

J.P. HOOD

Student Learning Objectives: The student will obtain an understanding of how state entities deny potential known and unknown adversaries from gaining access via UAS and air assets into a protected area, resource or installation. Through the use of real-world examples and case studies, the student will be able to visualize and understand the intricacies and planning required for state and local actors to adequately protect an area from possible intrusion, exploitation and attack.

Key Concepts:

A2 / AD (Anti-Access / Area Denial) is primarily designed to prevent or constrain the deployment of opposing forces into an area of operations

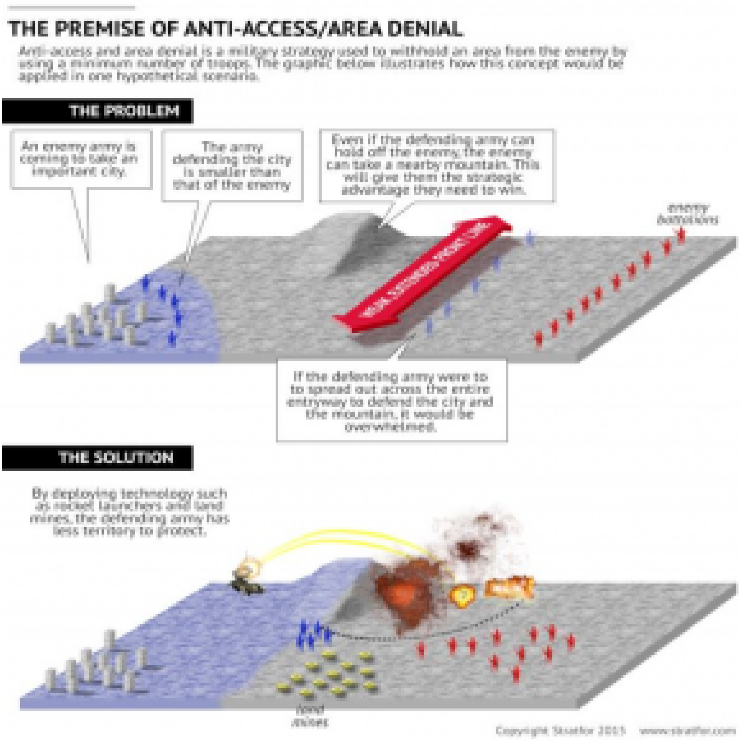
Anti-Access: Denying an adversary the ability to enter and operate military forces near, into or within a contested region.

Area-Denial: Used to reduce freedom of maneuver once an adversary is within an area of operations.

IADS (Integrated Air Defense Systems)

Simply put, the act of an adversary to work against the actions of another defines what anti-access or area denial environments are. More formally, the U.S Department of Defense (DoD) Joint Operational Access Concept (JOAC) defines these terms: "Anti-access (A2) refers to those actions and capabilities, usually long-range, designed to prevent an opposing force from entering an operational area. Area denial (AD) refers to those actions and capabilities, usually of shorter range, designed not to keep an opposing force out, but to limit its freedom of action within the operational area." (Cuddington, 2015)

Figure 7-1 The Premise of Anti-Access / Area Denial


THE PREMISE OF ANTI-ACCESS/AREA DENIAL
Anti-access and area denial is a military strategy used to withhold an area from the enemy by using a minimum number of troops. The graphic below illustrates how this concept would be applied in one hypothetical scenario.
THE PROBLEM
An enemy army is coming to take an important city.
The army defending the city is smaller than that of the enemy
Even if the defending army can hold off the enemy, the enemy can take a nearby mountain. This will give them the strategic advantage they need to win.
enemy battalions
If the defending army were to to spread out across the entire entryway to defend the city and the mountain, it would be overwhelmed.
THE SOLUTION
By deploying technology such as rocket launchers and land mines, the defending army has less territory to protect.
land mines
Copyright Stratfor 2015 www.stratfor.com

Source: (Stratfor, 2019)

Some examples of existing and emerging A2AD capabilities:

- Multi-layered integrated air defense systems (IADS), consisting of modern fighter/attack aircraft, and fixed and mobile surface-to-air missiles, coastal defense systems,

- Cruise and ballistic missiles that can be launched from multiple air, naval, and land-based platforms against land-based and maritime targets,
- Long range artillery (LRA) and multi launch rocket systems (MLRS),
- Diesel and nuclear submarines armed with supersonic sea-skimming anti-ship cruise missiles and advanced torpedoes;
- Ballistic missile submarine (SSBN) force,
- Advanced sea mines
- Kinetic and non-kinetic anti-satellite weapons and supporting space launch and space surveillance infrastructure,
- Sophisticated cyber warfare capabilities,
- Electronic warfare capabilities,
- Various range ISR systems,
- Comprehensive reconnaissance-strike battle networks covering the air, surface and undersea domains; and
- Hardened and buried closed fiber-optic command and control (C2) networks tying together various systems of the battle network,
- Special Forces

(Erdogan, behorizon.com)

Recent Rise in A2-AD Ideologies and Challenges

As potential near peer adversaries to the US such as China, Russia, Iran and North Korea continue to gain technological ground and modernize multi layered defense networks, the US DoD and State Department have realized that control of the commons will soon be challenged and an increased understanding of A2-AD concepts is necessary in order to develop ways to mitigate, penetrate and exploit adversarial defense networks. The US's continued reliance on UAS as platforms to act as ISR and communications relays as well as deliver precision guided munitions has proven to be a more realistic way to counter the growing security threats posed by ever more robust adversarial A2-AD systems. Nathan Freier from the

Centers for Strategic and International Studies effectively codified through a series of question and answers why A2-AD concepts continue to remain a major theme at the forefront of military operational planning.

From the widest strategic perspective, U.S. access challenges manifest across traditional instruments of power. To the extent that these challenges adversely affect the security and prosperity of the United States and its allies, an open and stable international system, and/or freedom to transit the global commons, they will require coordinated U.S. government/allied responses to restore access. By definition, this will routinely involve military forces. (Freier, 2012)

This is not meant to suggest that all access challenges are military in origin and character. In the Asia-Pacific region, for example, China is as much or more an active political and economic challenger—seeking to raise myriad barriers to U.S. influence—as it is a military competitor. Likewise, in the Middle East, Iran has some dangerous military capabilities but successfully avoids direct military confrontation with the United States, advances its interests, and limits U.S. freedom of action most often through cost-imposing political subterfuge. What is certain, however, is that when adversaries effectively combine political, economic, and informational tools with important military capabilities, the access challenge becomes more acute and potent. (Freier, 2012)

U.S. military forces have a unique responsibility in helping secure access during times of peace, increased hostilities, and open conflict. The latter is the most demanding and, as of late, the subject of the greatest body of conceptual work. Under routine circumstances, maintenance of credible deterrent capabilities forward in key regions provides a stabilizing influence, actively underwrites the security of U.S./partner interests, and secures a concrete platform from which to expand presence and conduct operations in the event of heightened tensions or hostilities. (Freier, 2012)

In the event of war or major violent conflict, U.S. forces will face a variety of A2/AD challenges that will originate both from the hostile designs of thinking adversaries and from the "unstructured" lethality of contagious instability. In virtually every instance, forward-stationed U.S. forces will be insufficient to overcome lethal or fundamentally disruptive A2/AD challenges and effectively resolve the crisis by themselves. Therefore, future combat operations—whether coercive air and sea campaigns or more wide-ranging joint interventions—will require the United States and its partners to project substantial military capability over considerable strategic and operational distances. A2/AD challenges frustrate our ability to do so. (Freier, 2012)

Thus, at the "business end" of opposed operations, U.S. forces will increasingly compete with a diverse collection of adversaries for dominance across multiple domains—air, sea, land, space, and cyberspace. This will often occur without the benefit of extensive fixed U.S. regional basing and with "local" U.S. infrastructure under substantial pressure from hostile action. As a consequence, the character of specific lethal access challenges, their diversity, and their sophistication will differ significantly. In combination, the real constraints of finite military capability, the increasing lethality of virtually every conceivable contingency environment from peace operations to regional war, and lower U.S. risk tolerance make deep thought about lethal or fundamentally disruptive A2/AD challenges an urgent strategic priority. (Freier, 2012)

Anti-Access Challenges

To U.S. strategists, A2 challenges are intended to exclude our forces from a foreign theater or deny effective use and transit of the global commons. More broadly, A2 challenges might first involve political and economic exclusion, where competitor states actively attempt to deny the United States the broad political and economic influence it has long enjoyed. In military terms, this may translate into blanket denial of basing, staging, transit, or over-flight rights. (Freier, 2012)

Under more hostile circumstances, lethal A2 instruments include sophisticated longer-range adversary capabilities and methods like ballistic missiles, submarines, weapons of mass destruction, and offensive space and cyberspace assets. Equally dangerous but less technical A2 methods might include terrorism or proxy warfare employed by U.S. opponents to open alternative "fronts," distract attention, and impose excessive costs politically. (Freier, 2012)

Hostile A2 capabilities and methods are intended first to see U.S. risk calculations breach "high" or "unacceptable" levels during planning in order to prevent U.S. regional intervention altogether. But, in the event of active hostilities, adversaries would employ their lethal A2 assets from a distance to keep the United States at arm's length, perhaps deny introduction of U.S. forces and capabilities in substantial numbers, and barring either outcome, exact prohibitively high costs on the United States when and if U.S. forces attempt to breach an opponent's A2 defenses. Given China's increased assertiveness, current military capability, and raw potential, an acute, sophisticated, and comprehensive A2 challenge is emerging in Asia. There is clearly some grand strategic risk associated with excessively militarizing the nature of the competition between the United States and China, as the locus of real competition may lie substantially outside the reach of DoD and the military instrument. (Freier, 2012)

Area Denial Challenges

Over the near to mid-term, lethal area denial (AD) challenges present U.S. strategists with the most prolific barriers to effective theater entry and operation. Every conceivable contingency employment of air, sea, or ground forces will need to overcome significant AD obstacles. Lethal AD threats manifest at close range. Their effects begin accruing as U.S. forces enter a hostile or uncertain theater to conduct joint operations, and in the end, they complicate our attempts to establish an effective presence in, over, or in range of an adversary's territory or interests. Lethal or disruptive AD challenges are present and can attack U.S. vulnerabilities in all five key domains—air, sea, land, space, and cyberspace.

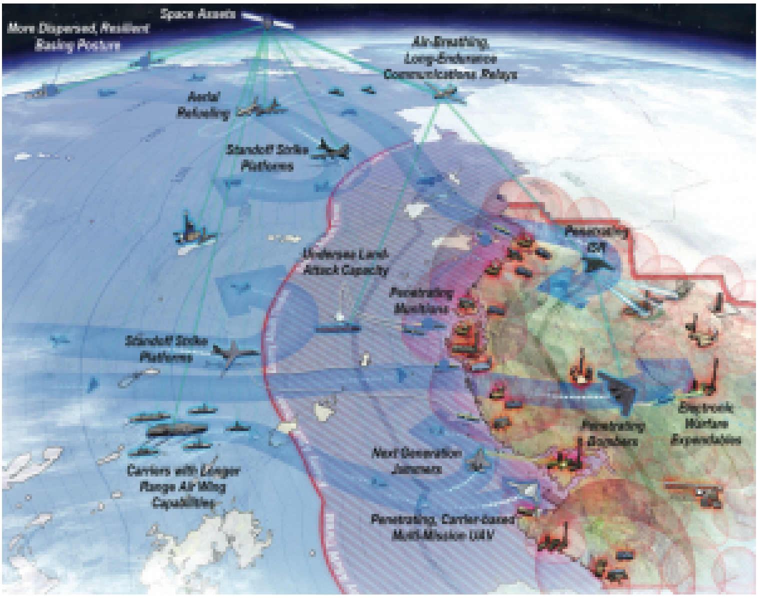
They do so first by providing the means to physically resist U.S. entry into theater. Subsequently, they limit freedom of action once U.S. forces have arrived. Then, they frustrate our efforts to rapidly achieve favorable strategic and operational outcomes. And, finally, they threaten to impose very high costs on U.S. forces should extended military operations become unavoidable. Like A2 challenges, AD threats can poison U.S. risk calculations well before the initiation of an operation by increasing the mission's perceived degree of difficulty. After entry, AD challenges force U.S. decisionmakers to persistently question the mounting costs associated with continued operations. (Freier, 2012)

Lethal AD capabilities range from the sophisticated to the crude but effective. They include cruise and ballistic missiles; weapons of mass destruction; mines; guided rockets, mortars, and artillery; electronic warfare; and short-range/man-portable air defense and anti-armor systems. Revolutions in information; personal computing, communications, and networking; and irregular and hybrid forms of warfare—combined with the proliferation of precision weapons and improvised battlefield lethality—substantially widen the universe of effective AD adversaries from individuals and loosely organized groups to sophisticated regional powers. Likewise, the networked mobilization of foreign popular, nonviolent resistance may also prove to be a significant challenge to freedom of action in the future as well. To the extent U.S. opponents can leverage all of these capabilities and methods both directly and through proxies, the more the AD challenge will expand geometrically. As noted above, an effective combination of political, economic, and informational methods with sophisticated lethal and/or disruptive AD capabilities will make any specific challenge more resilient and potent. (Freier, 2012)

Whereas lethal A2 challenges are virtually always the product of deliberate enemy design, AD challenges don't have to be. They can be "structured" or "unstructured." Iran's hybrid "mosaic defense," for example, is structured. Though highly unconventional, it is part of a coherent cost-imposing strategy. Its combination of ballistic and cruise missiles, unconventional naval forces, and hybrid ground defenses—matched with tight Persian Gulf geography, Iran's physical depth, and its deep ties to regional proxies—offer a complex structured AD challenge that strategic and operational planners would have to account for in the event of hostilities. (Freier, 2012)

U.S. forces are likely to face unstructured AD challenges in the course of interventions conducted under conditions of widespread disorder, where local authorities have little or no control over outcomes. Imagine military operations conducted in the same Iran described above; this time, however, after failure of the regime and in the midst of an ongoing civil war. U.S. forces might face multiple competing adversaries all boasting some relatively sophisticated, disruptive, and lethal AD capability but employing it all haphazardly under no discernible centralized command and control, making comprehensive defeat more problematic. (Freier, 2012)

Figure 7-2 Overcoming Adversarial Defenses


Space Assets
More Dispersed, Resilient Basing Posture
Air-Breathing, Long-Endurance Communications Relays
Aerial Refueling
Standoff Strike Platforms
Penetrating ISR
Undersea Land Attack Capacity
Penetrating Munitions
Standoff Strike Platforms
Electronic Warfare Expendables
Penetrating Bombers
Next Generation Jammers
Carriers with Longer Range Air Wing Capabilities
Penetrating, Carrier-based Multi-Mission UAV

Source: Image Attribute: Joint Operational Access Concept (JOAC) in an Anti-Access, Area Denial Theatre/ Source: McNeal & Associates (Associates, 2019)

According to the "Air-Sea Battle" concept, the general U.S. solution to the A2/AD issue is to develop a network of integrated forces capable of defeating the enemy across all modern war fighting domains: air, sea, land, space, and cyberspace. (US Department of Defense, 2013) This concept recognizes that adversary forces will likely attack without warning and forward friendly forces will be in the A2/AD environment from the outset of hostilities and must provide an immediate and effective response. (Cuddington, 2015)

Case Study: Countering Growing Chinese A2/AD in the Indo Pacific Region

The United States has long enjoyed "command of the commons": worldwide freedom of movement on and under the seas and in the air above 15,000 feet, with the ability to deny this same freedom to enemies. This command has contributed to a remarkable era of military primacy for U.S. arms against potential state rivals. (Cuddington, 2015)

Over the past few decades, state actors such as China have begun to establish themselves in the pacific region, challenging the US's ability to project power in the region. China is one of the most significant A2/AD threats at this time. China not only deters the United States from deploying into the Western Pacific, but also threatens to disrupt nearby operations such as around Taiwan or the South China Sea. (Cuddington, Jeff, 2016)

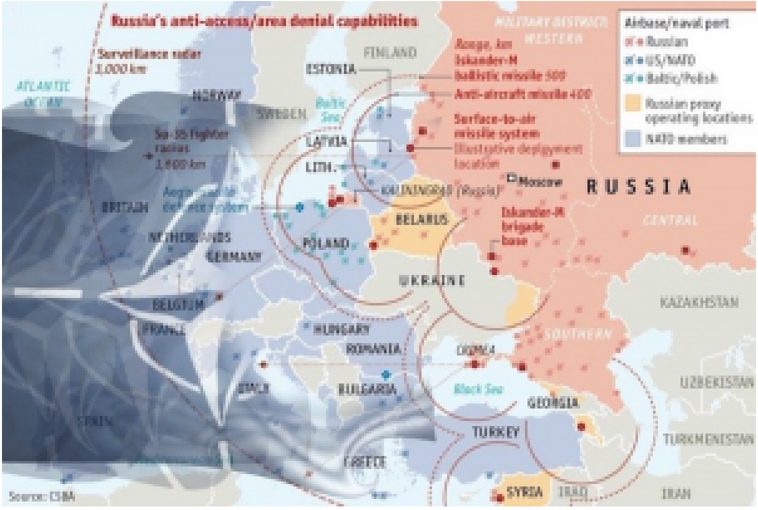
While U.S. advanced fighters and bombers have inherent advantages against China's defenses, these aircraft are not immune and are very limited in availability. A majority of American fighters, bombers, reconnaissance aircraft, and cruise missiles remain extremely vulnerable. China's integrated air defense system is virtually impossible to penetrate with current U.S. fourth-generation aircraft. (Posen, 2003)

Furthermore, China is expected to increase its threat range with the development of the S-400 (currently operational) missile system, extending their air defense coverage out to over 200 nautical miles. (Cuddington, Jeff, 2016)

Many observers now fear that this era may be coming to an end in the Western Pacific. For more than a generation, China has been deploying a series of interrelated missile, sensor, guidance, and other technologies designed to deny freedom of movement to hostile powers in the air and waters off its coast. As this program has matured, China's ability to restrict hostile access has improved, and its military reach has expanded. Many now believe that this "A2/AD" (anti-access, area denial) capability will eventually be highly effective in excluding the United States from parts of the Western Pacific that it has traditionally controlled. Some even fear that China will ultimately be able to extend a zone of exclusion out to, or beyond, what is often called the "Second Island Chain"—a line that connects Japan, Guam, and Papua-New Guinea at distances of up to 3,000 kilometers from China. A Chinese A2/AD capability reaching anywhere near this far would pose major challenges for US security policy. (Defense, 2006)

To avert this outcome, the United States has embarked on an approach often called AirSea Battle (ASB). Named to suggest the Cold War continental doctrine of "Air-Land Battle" (ALB), AirSea Battle is designed to preserve U.S. access to the Western Pacific by combining passive defenses against Chinese missile attack with an emphasis on offensive action to destroy or disable the forces that China would use to establish A2/AD. This offensive action would use "cross-domain synergy" among U.S. space, cyber, air, and maritime forces (hence the moniker "AirSea") to blind or suppress Chinese sensors. The heart of the concept, however, lies in physically destroying the Chinese weapons and infrastructure that underpin A2/AD. As Chinese programs mature, achieving this objective will require U.S. air strikes against potentially thou- sands of Chinese missile launchers, command posts, sensors, supply net- works, and communication systems deployed across the heart of mainland China—some as many as 2,000 kilometers inland. Accomplishing this mission will require a major improvement in the U.S. Air Force's and Navy's ability to and distant targets and penetrate heavily defended airspace from bases that are either hard enough or distant enough to survive Chinese attack, while hunting down mobile missile launchers and command posts spread over mil- lions of square kilometers of the Chinese interior. The requirements for this mission are typically assumed to include a major restructuring of the Air Force to de-emphasize short-range fighters such as the F-35 or F-22 in favor of longer-range strike bombers; development of a follow-on stealthy long-range bomber to replace the B-2, and its procurement in far greater numbers than its predecessor; the development of unmanned long-range carrier strike aircraft; and heavy investment in missile defenses and information infrastructure. The result would be an ambitious modernization agenda in service of an extremely demanding military campaign to batter down A2/AD by striking targets deep in mainland China, far afield from the maritime domains to which the United States seeks access. (US Department of Defense, 2013)

Figure 7-3 Air Space Denial: Russian A2AD Strategy and Its Implications for NATO



Source: (behorizon.org, russian-a2ad-strategy-and-its-implications-for-nato/ , 2019)

Integrated Air Defense System (IADS)

The integrated air defense system (IADS) threat today remains a formidable challenge to air operations in nearly any foreseeable major conflict. IADS modernization, coupled with significant advancements in multi- domain military operations (Cyber, Global C4ISR, Offensive Strike, Threats to Coalition Basing, etc.), poses a significant area denial threat to U.S. air dominance that was virtually guaranteed in past military operations. Fundamentally, the foundational pillars of the IADS kill chain have remained unchanged for decades; with mature processes and equipment widely fielded to perform indications and warning (I&W), find/fix, track, engage, and assessment functions. ((NASIC), 2019)

Battle Management Advancements: for the past 10+ years there has been significant advancement with adversary global C4ISR capabilities and their overall holistic approach to integrating disparate sources into a common, fused C4ISR infrastructure supporting IADS. While many advanced C4ISR concepts remain in their infancy, adversary current capabilities to process data globally in a timely, actionable manner poses a significant obstacle to U.S. global airpower and air operations. ((NASIC), 2019)

Weapons Control Advancements: since 2010, adversary IADS modernization has included deployment of long-range anti-access/ area denial (A2/AD) weaponry, supported by a vast deployment of layered tactical systems to augment long-range capabilities. These modern weapon systems threaten nearly every aspect of our counter-IADS / suppression of enemy air defense (SEAD) capabilities. Many of the emerging capabilities focus on the denial of airborne ISR and increasing the threat to 4th /5th Generation aircraft, cruise missiles, precision guided munitions, and UAVs. ((NASIC), 2019)

Understanding Emerging Vulnerable Gap

The potential exists for significant future developments to occur in the following technologies and concepts that are emerging but are not yet fully integrated and or operational:

- (U) Hypersonic defense
- (U) Cyber-enabled IADS
- Roll-out of modern directed energy weapons; combating airborne platforms at tactical ranges
- Full integration of "Big Data," artificial intelligence, and mature net centric IADS operations

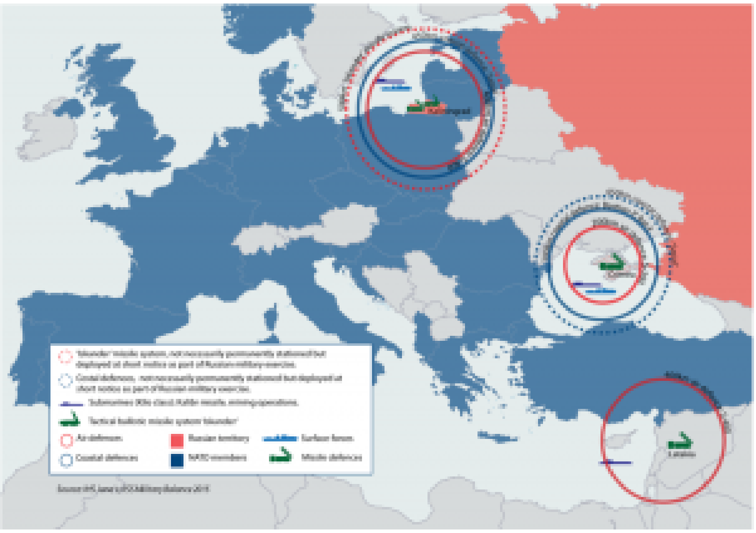
While adversary IADS capabilities continue to advance and pose a significant threat to U.S. air dominance, there are still critical vulnerabilities at nearly every echelon. C4I dependencies and centralized processes permeate these systems – and create opportunities for exploitation. ((NASIC), 2019)

Russian A2AD Case Study

Russia's recently deployed advanced A2AD capabilities such as; long range precision air defense systems, fighters and bombers, littoral anti-ship capabilities and ASW (Anti-Submarine Warfare), mid-range mobile missile systems, new classes of quieter submarines equipped with long range land attack missiles, counter-space, cyberspace, & EW weapons; and WMD assets in Kaliningrad in Black Sea and partly in Syria have changed the military environment. With additional deployments -thanks to modernization expected by 2020s- battlefield will be more complicated than ever. These A2AD capabilities allow Russia to have a new strategic buffer zone between NATO and Russia, but this time within Alliance` own territory. They provide the ability to target a large part of the Europe to influence, deter and deny NATO's potential operations in the High North, Baltic, Black Sea and East Mediterranean regions. (Busch, 2016)

The figure below depicts only a part of the Russian A2AD capabilities.

Figure 7-4 Russian A2AD Strategy Against NATO


Kaliningrad
'Iskander' missile system, not necessarily permanently stationed but deployed at short notice as part of Russian military exercise.
Coastal defences, not necessarily permanently stationed but deployed at short notice as part of Russian military exercise.
Submarines (Kilo class) Kalibr missile, mining operations.
Tactical ballistic missile system 'Iskander'
Air defences
Russian territory
Surface forces
Coastal defences
NATO members
Missile defences

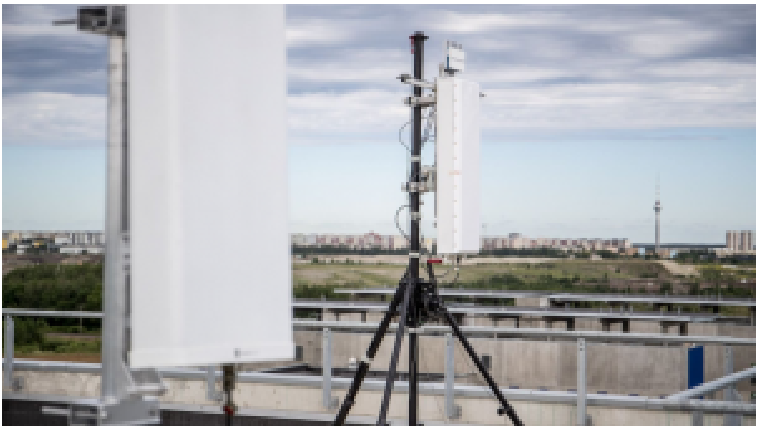
Source: IHS Jane's, IISS Military Balance 2016

Source: HIS Janes; IISS Military Balance 2015 & (behorizon.org, russian-a2ad-strategy-and-its-implications-for-nato/ , 2019)

Current C-UAS A2AD Civil Applications

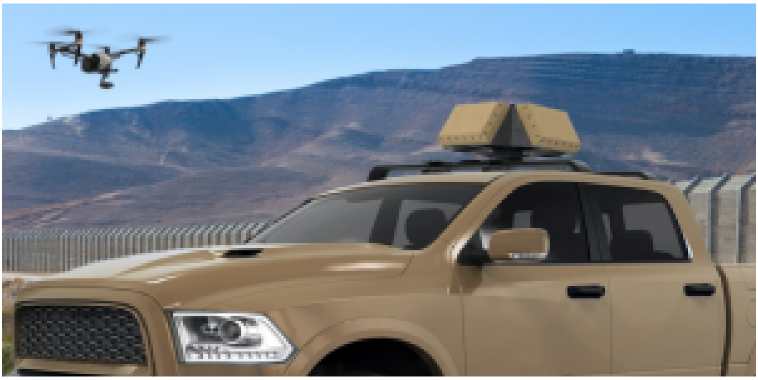
As the need for more complex area defense for countering illicit drone operations continues to grow, private industry has not forgotten the needs for companies and individual consumers to protect their personal and intellectual properties. Companies such as DeDrone and Drone Shield currently offer a range of integrable systems that are able to detect, track and deter commercial drones from entering private or localized airspace. The greatest risks to the public remain large open-air sporting venues / gatherings as well as domestic infrastructure / open to the air resources. The Department of Homeland Security (DHS) and US Customs and Border Protection will benefit greatly from using such technologies. Local integrated systems will be able to stop intruding drones from entering the US. These UAS have been reported carrying payloads containing contraband and narcotics. Drone Shield has developed Drone Sentry X that can intercept incurring drones. Federal prisons have also implemented similar systems from DeDrone in order to intercept and halt drone deliverables from entering a prison yard.

Figure 7-5 Drone Shield Drone Sentry



Source: (droneshield, droneshield.com/sentry, 2020)

Figure 7-6 Drone Sentry X



Source: (droneshield, dronesentry-x , 2020)

Conclusions

A2-AD and IADS are now center stage during all levels of operational planning conducted by the DoD. C-UAS considerations / technologies are the latest addition to planning and coordinating an effective area defense from aerial intrusions. While drones continue to operate in political grey areas focused on gaining access and intelligence, governments and military forces are continuing to seek non-kinetic technological means of tracking, denying and engaging these systems. Experts in C-UAS must be able to understand the unique challenges posed by fast moving systems with ever increasing standoff ranges. They must be able to recommend and employ systems that effectively counter these threats while at the same time adhere to international and domestic laws regarding vehicles in flight keeping the public safe from harm.

Innovative thinking at longer ranges will become more and more crucial. Advances in emerging technologies such as hypersonic vehicles that could potentially be delivered via UAS will continue to drive the need for a more dynamically integrated defense network(s). Decision processes will be forced to become that much faster in order to effectively defend against these new threats.

References

(NASIC), N. A. (2019, July 19). Emerging IADS Threats: Talking Points. *DoD Periodical.*

Associates, M. &. (2019, December). *OPINION-Need-of-the-Hour-A2AD.* Retrieved from www.indrastra.com: https://www.indrastra.com/2016/01/OPINION-Need-of-the-Hour-A2AD-002-01-2016-0084.html

behorizon.org. (2019, December). *russian-a2ad-strategy-and-its-implications-for-nato/* . Retrieved from www.behorizon.org: https://www.behorizon.org/russian-a2ad-strategy-and-its-implications-for-nato/

behorizon.org. (2019, December). *russian-a2ad-strategy-and-its-implications-for-nato/* . Retrieved from www.behorizon.org: https://www.behorizon.org/russian-a2ad-strategy-and-its-implications-for-nato/

Busch, K. a. (2016, February 09). No Denial: How NATO Can Deter Creeping Russian Threat. *www.cer.org.uk/insights* .

Cuddington, J. (2015). Intellignece Operations in Denied Area. *At Home and Abroad: Thinking Through Conflicts and Conundrums* .

Cuddington, Jeff. (2016, January). Opinion: Need of the Hour: New Intelligence .

Defense, O. o. (2006). Annual Report to Congress: Military Power of the Peoples Republic of China . *US DoD* , pp. 21, 25. .

droneshield. (2020, January). *dronesentry-x* . Retrieved from www.droneshield.com: https://www.droneshield.com/dronesentry-x

droneshield. (2020, January). *droneshield.com/sentry.* Retrieved from www.droneshield.com: https://www.droneshield.com/sentry

Freier, N. (2012). The Emerging Anti-Access/ Area Denial Challenge. *Center for Strategic and International Studies* .

Posen, B. (2003). Command of the Commons: The Military Foundation of US Hedgemony. *International Security*, Vol 28, No1. , pp. 5-46 .

Stratfor. (2019, December). *anti-access-area-denial-explained.* Retrieved from www.stratfor.com: https://www.stratfor.com/sites/default/files/styles/stratfor_large__s_/public/main/images/anti-access-area-denial-explainer%20(1).jpg?itok=mBf7FOAL

US Department of Defense. (2013, May). Air Sea Battle: Service Collaboration to Address Anti Access Area Denial Challenges. *DoD Periodical.*

Supplemental Readings

Cuddington, Jeff. (2015). "*Intelligence Operations in Denied Area*", VOL 2, NO 1, (2015): At Home And Abroad: Thinking Through Conflicts and Conundrums, licensed under a Creative Commons Attribution 3.0 License. ISSN: 2377-1852

Cuddington, Jeff. Jan 2016. *Opinion: Need of the hour: New*

Intelligence Priorities for Anti-Access, Area Denial. accessed Jan 2019 https://www.indrastra.com/2016/01/OPINION-Need-of-the-Hour-A2AD-002-01-2016-0084.html (Accessed Dec, 2019)

DeDrone: Drone Tracker 4.1 Integrated Counter Drone Systems
https://www.dedrone.com/blog/the-8-most-important-innovations-of-dronetracker-4-1
(Accessed Jan 2020)

Defense Matters, (2016) A2/AD Explained in Three Minutes
https://www.defencematters.org/news/a2-ad-explained-three-minutes-vid/1073/
(Accessed Dec 2019)

Erdogan, Aziz. (2018). Russian A2AD Strategy and Its Implications for NATO
https://www.behorizon.org/russian-a2ad-strategy-and-its-implications-for-nato/
(Accessed Dec 2019)

Freier, Nathan (2012) *The Emerging Anti-Access/ Area Denial Challenge.* Center for Strategic and International Studies. https://www.csis.org/analysis/emerging-anti-accessarea-denial-challenge (Accessed Dec, 2019).

Gholz, Eugene. (2019). *What is* A2AD *and Why Does it Matter to the United States?*
Charles Koch Institute.
https://www.charleskochinstitute.org/blog/what-is-a2ad-and-why-does-it-matter-to-the-united-states/ (Accessed Dec 2019)

Russia Missile Threat A2AD (Jan 2017)
https://missilethreat.csis.org/russia-nato-a2ad-environment/

Counter-Hypersonic (Dec 2019)

https://missilethreat.csis.org/mda-reveals-new-hypersonic-defense-program/

Hypersonic Countermeasures (Dec 2019)

https://aviationweek.com/defense/rfp-reveals-main-thrust-us-counter-hypersonic-plan

Barry R. Posen, “Command of the Commons: The Military Foundation of U.S. Hegemony,” *International Security*, Vol. 28, No. 1 (Summer 2003), pp. 5–46.

Office of the Secretary of Defense, *Annual Report to Congress: Military Power of the People's Republic of China* (Washington, D.C.: U.S. Department of Defense, 2006), pp. 21, 25;

Rem Korteweg and Sophia Besch, No denial: How NATO can deter a creeping Russian threat, 09 February 2016, http://www.cer.org.uk/insights/ (Accessed Dec, 2019)

Simon, Luia. (Jan 2017) Demystifying the A2/AD Buzz**https://warontherocks.com/2017/01/demystifying-the-a2ad-buzz/** (Accessed Dec, 2019)

U.S. Department of Defense, *Air Sea Battle: Service Collaboration to Address Anti-Access and Area Denial Challenges* (Washington, D.C.: U.S. Department of Defense, May 2013), http://www.defense .gov/pubs/ASB-ConceptImplementation-Summary-May-2013.pdf;

U.S. Department of Defense, *Joint Operational Access Concept* (Washington, D.C.: U.S. Department of Defense, January 17, 2012), http://www.defense.gov/pubs/pdfs/joac_jan%202012_signed.pdf.

Chapter 8: Emerging Interdiction Technologies

J.P. HOOD

Student Learning Objectives

The student will obtain an understanding of how the technologies affecting C-UAS trends are changing and advancing at a rapid pace. Everything from crude yet refined kinetic systems, hypersonic vehicle deliverables and cyber enhanced technologies are being developed to counter UAS incursion into protected air space. The student must be able to grasp new ideas, understand and maintain current doctrine and ideologies while thinking dynamically in order to remain relevant in the C-UAS realm.

Hypersonic Threats

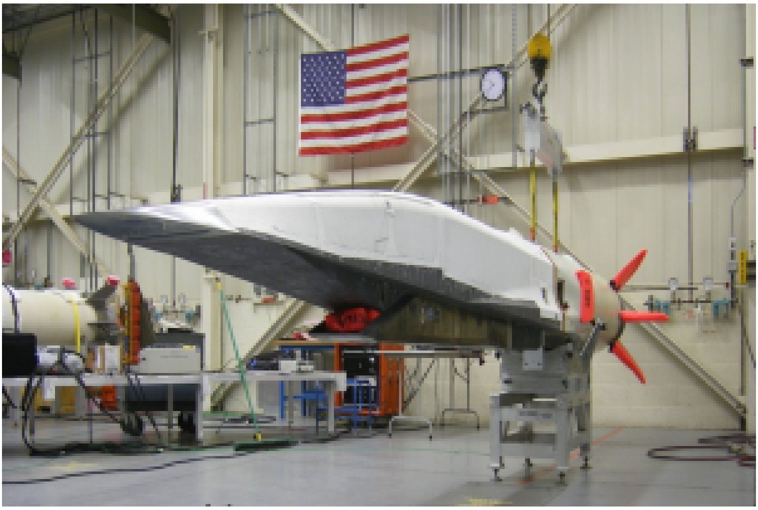
A hypersonic missile travels at speeds of Mach 5 and higher – five times faster than the speed of sound (3836 mph), which is around 1 mile per second. Some missiles, such as Russia's Kh-47M2 Kinzhal air-launched ballistic missile, are allegedly capable of reaching Mach 10 speeds (7672 mph) and distances up to 1200 miles. (Bosbotinis, 2018)

A Hypersonic Cruise missile is a type of missile that reaches its target with the help of a high-speed jet engine that allows it to travel at extreme speeds, in excess of Mach-5. It is non-ballistic – the opposite of traditional Intercontinental Ballistic Missiles (ICBM) which utilizes gravitational forces to reach its target. (Bosbotinis, 2018)

When hypersonic missiles become operational, the gap between missile defense systems and missile offence will be huge. Simply put, there is no single operational missile defense system that is capable of intercepting a hypersonic missile. Hypersonic missile research and development remains at the classified level, however in recent months many governments have announced successful tests and future projects. (Bosbotinis, 2018)

Hypersonic missiles offer a number of advantages over subsonic and supersonic weapons, particularly with regard to the prosecution of time-critical targets (for example, mobile ballistic missile launchers), where the additional speed of a hypersonic weapon is valuable. It can also overcome the defenses of heavily defended targets (such as an aircraft carrier). The development and deployment of hypersonic weapon systems will provide states with significantly enhanced strike capabilities and potentially, the means to coerce. This will be the case where a major regional power, such as Russia, may seek to coerce a neighbor, leveraging the threat of hypersonic strikes against critical targets. As such, the proliferation of hypersonic capabilities to regional states could also be destabilizing, upsetting local balances of power. However, it could also strengthen deterrence. (Bosbotinis, 2018)

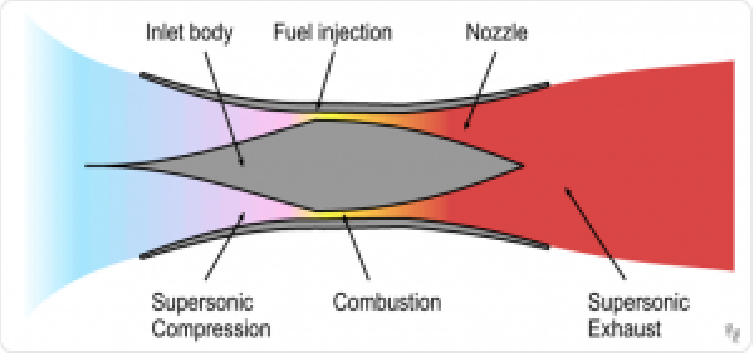
Figure 8-1: Boeing X-51 Hypersonic



Source: (Boyd, 2019)

Hypersonic technology comes from using a scramjet (**supersonic combustion ramjet**) which is a variant of a ramjet airbreathing jet engine in which combustion takes place in supersonic airflow. As in ramjets, a scramjet relies on high vehicle speed to compress the incoming air forcefully before combustion (hence *ram*jet), but whereas a ramjet decelerates the air to subsonic velocities before combustion, the airflow in a scramjet is supersonic throughout the entire engine. That allows the scramjet to operate efficiently at extremely high speeds. (Urzay, 2018)

Figure 8-2 Scramjet Engine Principles



Source: (Urzay, 2018)

Hypersonic Countermeasures

Although there are no current countermeasures in place, technologies such as directed energy weapons, particle beams and other non-kinetic weapons will be likely candidates for an effective defense against hypersonic missiles. “Hypersonic weapons reduce the time required to prosecute a target (especially compared to current subsonic cruise missiles), the warning time available to an adversary, and the time available for defensive systems to engage the incoming threat," says Bosbotinis. Although hypersonic threats would pose a significant challenge to current surface-to-air and air-to-air missile systems, such systems would, particularly in the conventional precision strike role, require a robust intelligence, surveillance, target acquisition and reconnaissance (ISTAR) network. (Bosbotinis, 2018)

Directed Energy Weapons

As UAS systems continue to advance in speed and maneuverability, enabling to remain outside of the engagement envelopes of traditional air defense systems, directed energy weapons have become the go to for low, slow and small UAS defense. These systems range in size from man portable equipment sets to permanent fixed sites. These systems typically offer a more cost effective and much safer way to deter, deny and destroy small tactical UAS with in a protected area of operations / facility.

In the fall of 2019, The US Air Force (USAF) has received the first anti-unmanned aerial system (UAS) laser weapon system from Raytheon to tackle the threat of enemy drones. The high-energy laser weapon system features an advanced variant of Raytheon's Multi-spectral Targeting System (MTS). It uses electro-optical / infrared sensors to detect and track enemy drones. Once the UAS is identified and targeted, the laser weapon system can engage the threat and neutralize it instantly. The technology involves a high-energy laser weapon system (HELWS) mounted on a small all-terrain vehicle. A single charge is enough for the HELWS to provide dozens of precise laser shots. Furthermore, the weapon system supports pairing with a generator on the field to provide a nearly infinite number of shots. (Media, 2019)

Figure 8-3: Raytheon Mobile High Energy Laser System

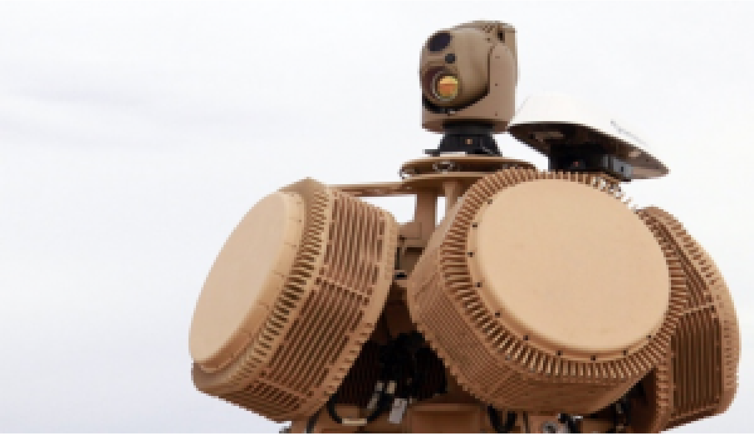
Source: (Raytheon, 2019)

The Raytheon company's advanced high-power microwave and high-energy laser defeated dozens of drone targets in a U.S. Air Force demonstration at the White Sands Missile Range in New Mexico in the Spring of 2019. Airmen took control of both the microwave and laser systems after just one day's training. They used an Xbox-style controller to direct the laser and a joystick to operate the high-power microwave in real-world scenarios at the U.S. Army White Sands Missile Range in New Mexico. The HEL system, paired with Raytheon's Multi-spectral Targeting System of sensors, uses invisible beams of light. Mounted on a small, all-terrain, militarized vehicle, the system detects, identifies, tracks and engages drones. Raytheon's HPM uses microwave energy to disrupt drone guidance systems. High-power microwave operators can focus the beam to bring down drone swarms. With a consistent power supply, an HPM system can provide virtually unlimited protection. (Raytheon, 2019)

On July 17th, 2019 a variant of the Marine Air Defense Integrated

System (MADIS) family of counter drone systems, the Light Marine Air Defense Integrated System (LMADIS), in use by the USMC, downed an Iranian drone in the Persian Gulf, which flew within 1,000 yards of a US Navy Vessel. The LMADIS is the product of a rapid development effort by Ascent Vision Technologies (AVT), the USMC Ground Based Air Defense team, and other partner suppliers. (BiancaV, 2019)

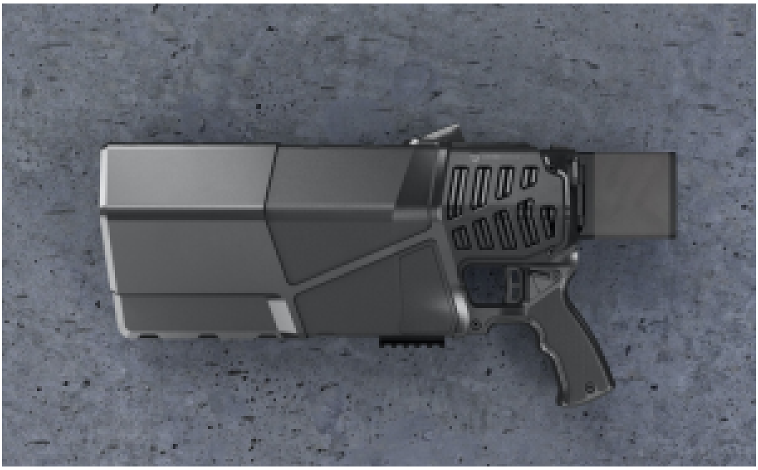
Figure 8-4: Ascent Vision Technologies Marine Air Defense Integrated System (MADIS)



Source: (BiancaV, 2019)

The Drone Gun MkIII is a compact, lightweight drone countermeasure designed for one hand operation. The product provides a safe countermeasure against a wide range of drone models. It allows for a controlled management of drone payload such as explosives, with no damage to common drones models or surrounding environment due to the drones generally responding via a vertical controlled landing on the spot, or returning back to the starting point (assisting to track the operator), with an immediate cease of video back to the drone pilot. RF disruption activation will also interfere with any live video streaming, first person view (FPV), back to the remote controller halting the collection of video footage and intelligence by the drone operator. (Shield, 2019)

Figure 8-5: Drone Gun MKIII



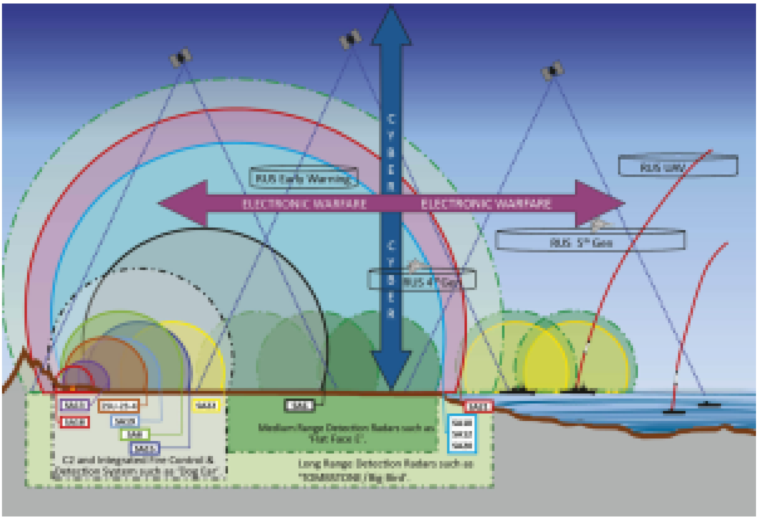
Source: (Shield, 2019)

Extreme Long-Range Cannon

In 2017, the US Army established a collection of cross-functional teams (CFTs) aimed at rapidly pushing forward key technologies to advance the services' next generation of capabilities. One of those teams was the Long-Range Precision Fires "pilot," an effort to develop the next generation of Army artillery—including "deep fires," an artillery capability that can strike at strategic targets well within an adversary's defenses. These systems seek to achieve a range of 1,000 nautical miles or more. There's strong incentive for the Army to succeed because an extreme-long-range gun could help deal with the difficulty posed by adversaries with advanced over-the-horizon radar, shore defenses, and air defense systems—such as the kind being put in place by China in the South China Sea. (Gallagher, 2019)

Cyber-Enabled IADS

Figure 8-6: Typical Layered Russian Air IADS


C
Y
B
E
R
RUS Early Warning
ELECTRONIC WARFARE
ELECTRONIC WARFARE
RUS UAV
RUS 5th Gen
C
Y
B
E
R
RUS 4th Gen
ZSU-23-4
Medium Range Detection Radars such as "Flat Face E".
C2 and Integrated Fire Control & Detection System such as "Dog Ear".
Long Range Detection Radars such as "TOMBSTONE / Big Bird".

Source: (Col Joseph Speed, 2019)

In order to allow friendly aircraft to conduct missions and support joint air power operations across the spectrum of warfare – from peacekeeping to high-intensity conflicts – NATO has nurtured developments in the Suppression of Enemy Air Defense (SEAD) mission. However, the newest generation of complex and capable enemy air defense assets threatens to overwhelm NATO's current SEAD abilities. (COL Speed USAF, 2018).

Over the last 20 years, potential adversaries of the Alliance have studied western military capabilities and have developed robust A2/AD capabilities in response. Examples are abundant and include threats such as the Russian SA-20 'Gargoyle' and SA-21 'Growler', the Chinese – built HQ-9, and the Dong-Feng 21. These capabilities are tailored to deny the 'western way of war' by precluding access to what is arguably the west's most potent influencer – air power. (COL Speed USAF, 2018)

Additionally, many state and non-state actors have been creatively employing military and commercial technologies to develop a range of capabilities for symmetric, asymmetric, and hybrid military activities, including AD. The technological trends include the following: anti-stealth technology, hypersonic weapons, cyber warfare, and access to and/or denial of space capabilities, to name a few. For example, Russian long-range surface to air systems now employ radar with anti-stealth technologies such as the 'NNIIRT 1L119 Nebo SVU/RLM-M Nebo M' mobile VHF active electronically scanned array (AESA) radar. In the realm of hypersonic, the Russians have an air-launched missile, the 'Dagger', which can reach and maintain Mach 10. In addition, China is developing anti-satellite capabilities such as the 'Dong Neng 2 & 3' exo-atmospheric vehicles. Primarily, these are direct-ascent missiles designed to ram and destroy satellites. (COL Speed USAF, 2018)

Advances in computing power and digital signal processing are allowing for more capable AD radars. These systems employ advanced techniques to improve acquisition range and target size detection and possess increased resistance to electronic attack or deception. In addition, new ideas in electromagnetic spectrum management are allowing radar technology to become more passive than active, which significantly complicates locating and targeting such sites. For instance, Russia is developing passive coherent radar designed for stealthy detection of moving aerial, ground and above-water targets in the protected area of important facilities. While passive radar systems are already being employed in both ground and air platforms, they are normally used to locate platforms vice engage them. That being said, passive radars will likely be able to target and guide weapons against air threats soon, significantly complicating the SEAD mission.

Adversaries' legacy systems of hierarchical data management and links are being replaced with multi-node, high-capacity, efficacy networks, contributing to highly resilient, redundant, and robust Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems. The resiliency of future C4ISR may be augmented by space-based technologies – such as micro-satellite constellations – making an Integrated Air Defense System (IADS) even more effective and agile. In addition, it is quite possible that a nodular system might enable air defense systems to continue to support operations through 'remote' operations, even if some parts of the IADS are damaged or destroyed. A current example of this is Russia's experimentation with multi-node quantum networks. In effect, suppressing or destroying local air defense assets, which are linked into a multi-node network, may not provide effective suppression of the enemy IADS. (COL Speed USAF, 2018)

The growing ability to operate systems remotely will not only increase range of detection but will also increase remote crew survivability. 'Remoting' operations and unmanned technologies may not only increase the survivability of an IADS, but they will likely extend its detection and targeting capabilities by hundreds of miles. For example, the advancements in space technology may extend the 'remoting' capabilities of an IADS to altitudes extending into space. The combination of the aforementioned activities may increase the passiveness of an IADS, deny its detection and targeting, and make it resilient to most SEAD activities. (COL Speed USAF, 2018)

Lastly, over the next twenty years very long-range surface-to-air weapons, with advanced seeker guidance, smart warheads, and new propulsion technologies, may be employed in enemy AD missions. In particular, Surface-to-Air Missile (SAM) engagement zones may be extended up to 500 km. One need look no further than the Russian

S-500 next-generation SAM system to see the lethality of future AD. Disturbingly, this particular missile system could enter service as early as 2020. These new long-range weapons' technologies may contribute to a highly mobile, flexible IADS when combined with increases in computing power and decreasing size of hardware and processors. (COL Speed USAF, 2018)

IADS of the future are becoming even more lethal, agile whole remaining difficult to detect on the battlefield. While the US will continue to remain the dominate force through the air and space, potential adversaries will most likely continue to heavily invest in ways to undermine advances in aerial capabilities. These AD systems have already become so advanced that the US military and other nations are re-looking long range kinetic means to counter them. Maintaining an adaptive and dynamic frame of mind will be crucial in identifying and ultimately defeating these emerging threats, ensuring continued success on the battlefields of the future.

Big Data and Artificial Intelligence Integration

Artificial Intelligence (AI) is the theory and development of computer systems able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages. Big data is the field that treats ways to analyze, systematically extract information from, or otherwise deal with data sets that are too large or complex to be dealt with by traditional data-processing applications.

The incorporation of Artificial Intelligence into defense strategies has already begun to transform NATO's ISR and defense capabilities in regard to the assimilation and processing of data in order to effectively identify targets. Science and technology advancements are helping to shape both the requirements and solutions for new approaches in order to meet NATO capability needs.

These capabilities will ultimately enhance military decision-making and accelerate the acquisition of actionable intelligence. The focus was on the impact on the OODA (observe, orient, decide, act) loop. We can see major impacts from AI, machine learning and big data in the observe function in terms of being able collect and assimilate large amounts of data and then process that efficiently and effectively to identify potential targets. This then helps orient towards specific areas of interest or targets of interest that you are looking for through your ISR capabilities. (Bayley, 2018)

These techniques can also be used in a defensive manner as well. Enhanced systems can potentially be used to detect, track and decide whether or not to engage a threat based on stored data sets and pre-determined patterns. This could potentially remove humans from the decision-making process but at the same time could reduce the time required to engage faster moving, more technologically advanced threats.

Conclusions

C-UAS technologies are changing and advancing. Hypersonic missiles, Directed Energy weapons (also covered in Chapter 10), long- range cannons, mobile drone guns and Cyber -enabled IADS represent steps in the future of Counter-UAS countermeasures. Much of the research work on these fine weapons is classified, necessitating only a brief open source treatment by the authors about this subject.

References

Bayley, J. (2018). *Transforming ISR Capabilities through AI, Machine Learning and Big Data: Insights from Dr. Thomas Killion, Chief Scientist,* NATO. Retrieved from DefenceIQ.com: https://www.defenceiq.com/defence-technology/news/transforming-isr-capabilities-through-ai-machine-learning-and-big-data

BiancaV. (2019, July 22). *ascentvision.com*. Retrieved from AVT

Products Down Iranian Drone: https://ascentvision.com/avt-products-down-iranian-drone/

Bosbotinis, J. (2018, August 28). *Hypersonic Missiles: What Are They And Can They be Stopped*. Retrieved from defenceiq.com: https://www.defenceiq.com/defence-technology/case-studies/hypersonic-missiles-what-are-they-and-can-they-be-stopped

Boyd, I. (2019, May 1). *us-russia-china-race-to-develop-hypersonic-weapons*. Retrieved from theconversation.com: https://theconversation.com/us-russia-china-race-to-develop-hypersonic-weapons-114694

Col Joseph Speed, &. L. (2019, japcc- journal 27). *challenges-of-future-sead-operations*. Retrieved from www.japcc.org: https://www.japcc.org/challenges-of-future-sead-operations/

COL Speed USAF, L. S. (2018). *Joint Air Power Competence Centre*. Retrieved from japcc.org: https://www.japcc.org/challenges-of-future-sead-operations/

Gallagher, S. (2019, October 15). *Bringing in the big gun: Army paves way for strategic cannon*. Retrieved from arstechnica.com: https://arstechnica.com/tech-policy/2019/10/army-aims-to-test-extreme-long-range-strategic-cannon/

Media, V. (2019, October 23). *airforce-technology.com* . Retrieved from Air Force Technology: https://www.airforce-technology.com/news/usaf-raytheon-counter-uas-laser-weapon-system/

Raytheon. (2019, September 25). *raytheon.com*. Retrieved from Defense at the Speed of Light: Directed Energy Systems Down Drones in USAF Demonstration: https://www.raytheon.com/news/feature/defense-speed-light

Shield, D. (2019). *DroneShield.com*. Retrieved from DroneGun MKIII: https://www.droneshield.com/dronegun-mkiii

Urzay, J. (2018). Supersonic Combustion in Air-Breathing Propulsions Systems for Hypersonic Flight. *Annual Review of Fluid Mechanics* , 50: 593-627.

Supplemental Readings

Russia Missile Threat A2AD (Jan 2017)

https://missilethreat.csis.org/russia-nato-a2ad-environment/

Counter-Hypersonic (Dec 2019)

https://missilethreat.csis.org/mda-reveals-new-hypersonic-defense-program/

Hypersonic Countermeasures (Dec 2019)

https://aviationweek.com/defense/rfp-reveals-main-thrust-us-counter-hypersonic-plan

USAF Man-portable service rifle jamming module (Area Denial)

https://invisidiction.com/invisible-interdiction-awarded-air-force-contract-for-rail-mounted-uas-denial-system/

Chapter 9: Non- Kinetic: Military Avionics, EW,CW,DE,SCADA Defenses

R. K. NICHOLS

Student Objectives

Chapter 9 is a potpourri of non-kinetic technologies for C-UAS. The student will be introduced to military avionics systems and the roles they play in the defense matrix. Avionics are the primary target of C-UAS efforts. A side-theme throughout this chapter is that most military manned aviation roles can be filled with the less costly unmanned option at reduced human liability. One of the most interesting roles is the maritime patrol aviation (MPA) and is singled out for coverage. Four areas will be explored in more detail: electronic warfare (EW), cyber warfare (CW), directed energy (DE) weapons and acoustic defenses. SWARMs continue to be a concern and are addressed. (Osborn, 2019)

What Is the Counter -UAS Problem?

The risk of successful terrorist attacks on USA Air Defense Systems (ADS) via sUAS/UASs is greater because of improving commercial capabilities and accessibility. Advanced small drones, capable of carrying sophisticated imaging equipment and significant payloads, are readily available to the public. A range of terrorist, insurgent, criminal, corporate, and activist threat groups have demonstrated their ability to use civilian drones and gather intelligence. How does the country defend against a growing UAS threat? This is also known as the counter – UAS Problem. General James D Mattis, SECDEF summed up the Problem succinctly: (Nichols, et al., 2019)

"Unmanned Aircraft are being developed with more technologically systems and capabilities. They can duplicate some of the capabilities of manned aircraft for both surveillance/ reconnaissance and attack missions. They can be small enough and / or slow enough to elude detection by standard early warning sensor systems and could pose a formidable threat to friendly forces." (Chairman, 2012)

Operational Protection from Hostile UAS Attacks – A Helicopter View

"According to LCDR Boutros of the Navy War College, developing technologies do not paint a pleasant picture of counter – UAS problem (Boutros, Operational Protection 2015). UAS has seen a widespread proliferation among both state and non-state actors. This is a cause for concern to US Operational Commanders." (Boutros, 2015) General James D Mattis, SECDEF concluded:

"The proliferation of low cost, tactical unmanned aerial systems demand we think about this potential threat now… we must understand the threat these systems present to our joint force and develop the tactics, techniques and procedures to counter the problem." (Chairman, 2012) (Myer, 2013)

Joint Publication (JP) 3-01 identifies friendly assets that an adversary may attack during a campaign using UAS. A Theater Commander must plan for counter – UAS actions against air defense sites, logistics centers, and national critical infrastructure. (Boutros, 2015) "Due to their small size and unique flying signatures, many UAS are difficult to detect, identify, track, and engage with current joint air defense systems. The increasing proliferation of global UAS has exposed a critical vulnerability in the protection function of operational commanders, requiring joint efforts to include intelligence, Electronic Warfare (EW), cyber warfare, (CW) and FIRES." (Boutros, 2015)

But UAS are not invincible. Neutralizing threats or mitigating risk includes active and passive defense methods with kinetic and non-kinetic FIRES.[1] (US DoD – JP 3-0, 2012)

Countering UAS Air Threats

Advanced UAS can carry large payloads great distances. US Predator and Global Hawk UAS, [See Figure 9-1] "Chinese Pterodactyl [See Figure 9-2] and Soring Dragon counterparts, and Iranian Ababil can carry at least 500 Kg payloads greater than 300 km." (Boutros, 2015) "They can be armed or unarmed, with ISR payloads, communications relays, Over-The-Horizon (OTH) target acquisition, and precision strike capabilities." (Boutros, 2015)

"Shorter range, tactical, small/micro UAS may not have the distance or payload capacity of more advanced systems, but they can impact a campaign (or US Homeland Defense) in equally serious ways. Because of their size, their heat signatures are almost nonexistent. They easily evade detection. They offer more freedom of action. They can be launched from within US air defense zones and fly to their targets in less time than it takes for a coordinated response." (Boutros, 2015) [Nightmare alert: Imagine a SWARM of UAS carrying small potent binary bomb payloads attacking a US Carrier at port less than one mile away from the UAS launch point.] The enemy can effectively balance space, time, and force (arguably frequency too). (Beaudoin, 2011) "Small UAS (sUAS) can perform short-range ISR, be outfitted with explosive charges or chemical and biological agents for aerial dispersion, or simply fly over troops or civilians to demoralize." (Boutros, 2015) [Nightmare alert: Given the effectiveness of enemy use of IEDs in Iraq and Afghanistan, a mobile, airborne version would take the Problem to an entirely new level!] (Nichols R.-0. , 2016)

Vulnerabilities Perspective

"sUAS are vulnerable to kinetic and non-kinetic outside influence in six different areas; their link to a ground station, the ground station itself, the aircrafts various sensors, avionics, cyber weapons, directed energy weapons (DE) and acoustical weapons (AW)." The military recognizes the first three factors, the authors concentrate on the latter group.

"In 2009 Iraqi insurgents successfully hacked into US Reaper drones, crashing them." (Boutros, 2015) (Horowitz, 2014). "In September of 2011, ground control stations at Creech AFB were infected by a virus, temporarily grounding the entire UAS fleet." (Boutros, 2015) (Hartman, 2013) UAS onboard sensors can be manipulated in many ways. "High intensity light directed at an optical sensor can blind it. GPS receivers can be cyber-spoofed, which consists of transmitting a stronger, but false, GPS signal to a receiver, resulting in inaccurate navigation. Influencing the local magnetic field can have adverse effects on both onboard hard drives and sensors that require magnetic orientation to operate correctly." (Boutros, 2015) (Hartman, 2013) The object is to better understand UAS subsystems, to facilitate exploiting their weaknesses.

Figure 9-1 Global Hawk

Source: (Rogoway, 2018)

Figure 9-2 Chinese Pterodactyl

Source: (Defence, 2014)

The author's research suggests that: The hostile technology of remote-controlled warfare is difficult to control or abort; the best defense (counter – UAS) is to address the root drivers of these threats. The threat-roots are SAA, SCADA and avionics. SAA and SCADA are vulnerable to both cyber and EW weapons. An EMS subset of special interest are acoustical countermeasures as research has confirmed their effectiveness against SWARMS. (Nichols, et al., 2019)

Conventional Vulnerabilities of Air Defense Systems (ADS), Attacks By sUAS and Countermeasures

A simplified, non-classified view of the US Air Defense System (ADS) against a hostile UAS attack occurs in two stages:

1. Early Detection and Identification of "Danger Close" (Myer, 2013) [2]

2. Applied appropriate countermeasures with secondary goal of restricted collateral damage.

The traditional ADS family of tools for Detection include:

1. Active Radar Surveillance – generate waves, use rebound echoes on UAS to locate, estimate distance, approach speed, size, penetration vector and short-term trajectory, and
2. Passive Monitoring – covers electromagnetic spectrum via visible, thermal infrared, radio waves on common communications channels.

When considering hostile UAS defense planners need to consider several issues. The US ADS is optimized for missiles and aircraft deployed at high altitude and speeds. ADS data fusion (detection, identification, weapon lock-on, execute countermeasures) works better with larger targets, not very small ones like UAS / sUAS. US ADS is effectively reactive for longer ranges. Close reactive engagements are sub-optimal. US ADS are not optimal for sUAS /UAS. (Nichols R.-0. , 2016) Neither were Saudi Arabian ADS against the Iranian attack on oilfields. (Gallagher, 2019)

"There are clear vulnerabilities of the US ADS to UAS:

- sUAS can be launched into action close to target(s), less than 1 mile.
- sUAS exhibit a small Radar signature. The detection phase is hindered.
- Reactive dictates quick response near target. This is not always possible.
- sUAS / UAS are designed for slow, low flight. Low flying sUAS avoids Radar identification.
- sUAS / UAS electric motors are both quiet and have limited thermal signature. This makes for difficult detection for noise.
- sUAS /UAS operate in urban areas. Urban sphere presents additional problems and potential collateral damage." (Nichols

R.-0. , 2016)

Conventional Countermeasures Against sUAS /UAS

There are two families of conventional countermeasures used to disrupt /destroy hostile UAS/sUAS systems (Regulatory ~ locked in firmware GPS No-Fly Zones, Registration, FAA rules excluded).

Active Measures – Designed to incapacitate, destroy the sUAS/ UAS threat in a direct way (Ground-to- Air Defense (GTA), missiles or, acoustical gun, or simple cyber rifle or DE weapon)

However, there are some defensive issues to be considered:

- GTA efficiency against sUAS, reactive targets are reduced, even less efficient in urban zones where public at risk.
- Simultaneous attacks on multiple fronts very difficult to apply and defense measures are mitigated. [3]

UAS countermeasures research is improving. The goal is to increase ability of GTA to react and improve capabilities to a defined to a saturation limit. Team formation allows decoys and shields. SWARM formation is easier to detect. Arrival of a cloud of robot drones is hard to mask, but tough to neutralize. Commercial company Liteye has developed an Anti-UAV Defense System (AUDS) which are able to detect, track, and disrupt sUAS operation by pulsed, brief focused broadcast of direction frequency jamming. Liteye has also developed a mobile version call M-AUDS. (Liteye, 2018) China has developed a "5-sec" laser weapon to shoot down sUAS at low altitude (500 m) with a 10KW high energy laser beam. Its range is 1.2 mi and handles sUAS speeds up to 112 mph. (Nichols R.-0. , 2016)

Passive – Designed to protect indirectly; physical protections around target, decoys, shields, organized roadblocks, nets, jamming of sensors of the aggressor, GPS total or partial cyber-Spoof of signals. Passive countermeasures have some positive outcomes. Decoys can be effective if the ADS know what the sensors employed for sUAS Kamikaze attack and how they are used in the SAA subsystem. Communication jamming is effective against level 1 & 2 drones which require pilot interaction. It can disrupt inter–drone communications required for either team or SWARM formations. Sensor Jamming – especially GPS signals – giving false GPS information, camera/gimbal dislocation, and heading sensor demagnetization is effective regardless of automation.

The 2011 Iranian incident taught US ADS planner's lessons about passive spoofing waypoints and Loss of Signal (LOS) via GPS. LOS is an emergency condition. sUAS/UAS have programmed responses. One of those responses may be," return to waypoint". Two types of spoofs were executed. A complete spoof uses the friendly SAA to estimate course, groundspeed, time to target to force a LOS and final waypoint change. A partial spoof reports false positions, during LOS and changes waypoints for perceived emergency conditions. Both spoofs are difficult to detect & effective (Editor, 2012)

Aggressor Counter-Countermeasures Specific to UAS Deployment – SWARM

The authors contend that a UAS SWARM attack is practically unstoppable unless the defender (US ADS) exhibits strong collaboration and ability to match/identify the SWARM locations in a timely matter. This requires combined active and passive measures. This portends the ADS computer networks must process, detect, identify, and target information (and make critical decisions) significantly faster and more effectively than their enemies. Cost is an additional vulnerability factor. SWARMS can be assembled, delivered, and targeted in a relatively inexpensive weapons package. A SWARM can use local counter jamming on target nets. (Nichols R.-0. , 2016)

Implications from Attack by Iran on Saudi Arabian Oil Fields

On 14 September 2019, Houthi rebels in Yemen claimed their attack on the Abqaiq and Khurais oilfields in Saudi Arabia. (Gallagher, 2019) The effect was to temporarily take out 5% of the global oil production capacity. (Gallagher, 2019) Houthi rebels claimed responsibility for the attack, saying that 10 drones (mixed origins) and 17 missiles were deployed. (Lister, 2019) See Figure 9-3. Ballistic missile attacks by the Houthis have been previously deployed using old Soviet and Iranian "Scud" SRBMs. No prior attack, since the Yemen conflict began four years ago, has interrupted oil supplies.

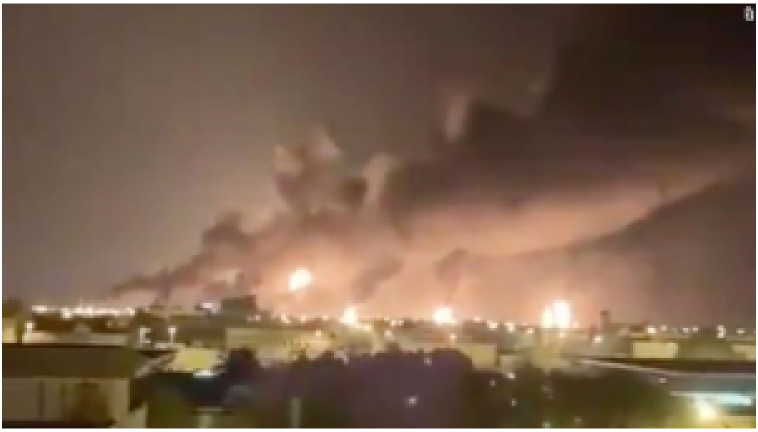
The Houthis have sent dozens of drones and short-range ballistic missiles against Saudi Arabia in the past two years. Many have been intercepted by Saudi Air Defenses; others have fallen harmlessly. Very few have caused limited damage and casualties. (Lister, 2019) The Abqaiq oilfield is 800 miles from Houthi-held parts of Yemen. The drones used were from North Korean Iranian and Chinese origins. (Lister, 2019) The Iranian drones were dubbed the UAV-X and have a range of 740 – 930 miles. This is a step up from the SRBMs that were based on North Korean technology with a maximum range of 186 miles. (Lister, 2019) The Chinese drones have several names: "Qaseth-1" ("Striker-1"), a rebrand of the Iranian Ababil-2 UAV and the "Mirsad-1" used by Hezbollah until 2018. (Gallagher, 2019) *The step-up in the conflict game is the Iranian clone, KH-55 with a range of 1,550 miles*. These were *reportedly* used in the Saudi Arabian oil field attacks. (Gallagher, 2019)

The take-away from this attack is not just the loss of global oil processing capacity but the vulnerability and exposure of the Saudi Arabian Advanced Air defenses. Most of the Saudi Arabian ADS are designed to defend against traditional threats and are ill-equipped to tackle the asymmetrical aerial threats such as drones. The vulnerability is enhanced when so many essential oil-related infrastructure parts are concentrated in a small area: storage, processing, compressor trains and distribution. (Lister, 2019)

Think of this problem more globally. China, North Korea and Iran [refer to as CNKI cooperation] are aggressively cooperating on drone technologies for use against a major oil production region.

The technology is cost-effective as well as human capital efficient. Drones substituting for manned aircraft.

Figure 9-3 shows A haze of smoke is seen from the attacked oil plant in Saudi Arabia



Source: (Sheena McKenzie, 2019) https://www.cnn.com/middleeast/live-news/saudi-oil-attack-dle-intl/h_1ab7e8469e98525f887c3a4e588dde8a

Let's expand the threat. Refer to Figure 9-4. Note that the Strait of Hormuz lies between Iran and Saudi Arabia, with Bahrain, Qatar, UAE and Oman in the sandwich. Between the Gulf of Oran and the Persian Gulf, about 20% of the global oil movement / supply travels through the Strait of Hormuz. (EIA, 2019) The US 5th Fleet currently protects this oil flow. There have been several *clashes* between Iranian vessels and US Vessels. Drones cross over the US Fleet every day and test its patience.

The key theme for this chapter is non – kinetic C-UAS technologies. Remember, payloads can be anything: CBRN deployment devices, drugs, surveillance packages, shaped charges, lasers, super resolution cameras, weather instruments, GPS/GNSS cyber weapons, missiles, etc.

The problem is twofold: what is the risk assessment for CNKI drone technologies cooperation acted on either target (US 5th Fleet or Saudi Oil Fields -both in range of KH-55's) and what countermeasure technologies are available to counter the threats presented and to mitigate those risks and system vulnerabilities?

Military Avionics

Avionics is a generic name for a diverse set of functions being provided by AVIation electrONICS. Moir and Seabridge provide a fair history of the Avionics since the word was coined in 1930s. (Moir I. &., 2006) As avionics systems have evolved, the level of functional integration has increased dramatically. Technology has actually blurred functional boundaries. The outcome of this evolution has been to increase performance; sensor types; functionality; *cost*; integration; complexity; supportability and reuse; software / executable programs; memory; throughput; reliability; data handling; data links; and obsolescence. (Moir I. &., 2006)

The result has been to decrease size; weight; power consumption; and technology windows. (Moir I. &., 2006) The basic military avionics system according to the DoD standards is shown in Figure 9-5.

Military Aviation Roles

The authors contend with all due respect to USAF, USN, USMC, USA that most *manned* (piloted) military aircraft roles can be replaced by *unmanned* aircraft systems. The military was quick to understand the opportunities offered to them by the ability to leave the ground and gain the advantage of height in the battlefield. Military aircraft perform a variety of aviation roles using fixed-wing and rotary-wing aircraft. The roles define the type of aircraft because of the specialist nature of the tasks. Several aircraft types are designed for multi-roles or to change roles during the mission (aka swing-roles). Military aviation roles are driven by advances in the technology of sensors and avionics not by pilot abilities. (Moir I. &., 2006) More sensitive and effective sensor systems are capable of detecting targets, the use of stealth techniques increases the effectiveness of delivery platforms and increased capability of on-board computing systems.

Drones compact these sensor technologies. They eliminate wasted space. They can process on-board data close to their manned counterparts. Clearly cheaper to produce, they are expendable in battle.

In a military defense environment, a variety of military avionics systems exist[4]:

1) Air Superiority – Deny the enemy the airspace over the battlefield, thus allowing ground forces to rein freely in destroying ground targets.

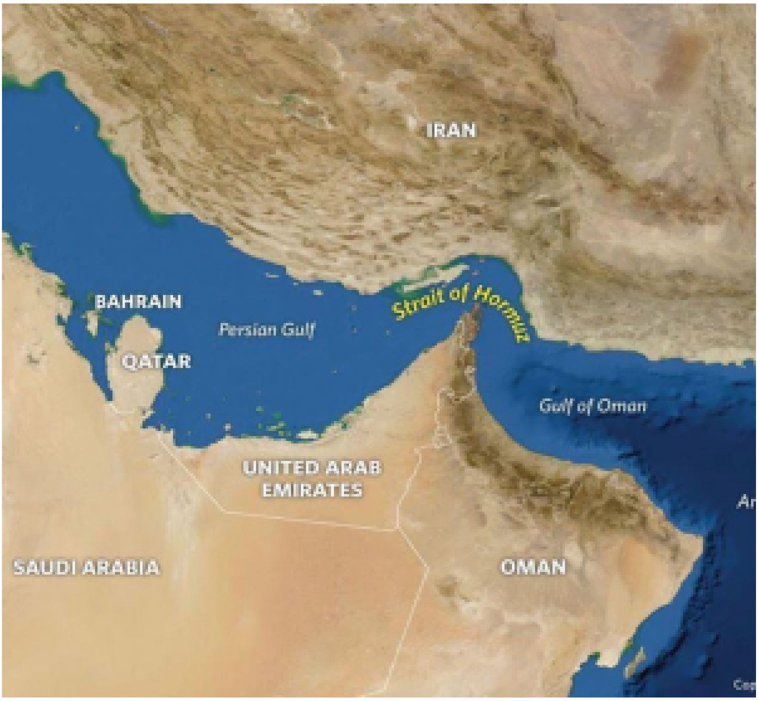
2) Ground Attack – Assist tactical situation on the battlefield [close air support (CAS)]. This role includes the ability of designating targets by laser and precision bombing.

3) Strategic Bomber -The mission is to penetrate deep into enemy territory and to carry out strikes to weaken defenses.

4) Maritime Patrol Aircraft (MPA) – The mission is huge, to cover 60% of the earth's surface (water). The MPA is the most complex of systems aircraft with the demanding role embracing a broad spectrum of tactical and strategic tasks / tools, as well as, support for civilian and humanitarian activities. (Moir I. &., 2006) It includes sub-roles of Anti-surface unit warfare (ASuW); and Anti-submarine Warfare (ASW); Search and Rescue (SAR); Exclusive Economic Zone Protection (EEZP); and Customs and Excise Cooperation (C&EC). Each of these are broken down further into associated tasks / architectures as shown in Table 9-1 & 9-2. Figures 9-6 & 9-7 show two examples (P-3 Orion and Saab Swordfish) MPAs.

MPA interests the author because of his work on UAVs and intelligence gathering by Chinese in the Spratly Islands and his research into acoustic defenses / countermeasures against hostile SWARMS. Even with all of its complexity a good portion of MPA missions can be accomplished by unmanned aircraft systems.[5] Table 9-2 shows typical MPA platform architecture. Figure 9-8 shows the MQ-4C Triton BAMS MPA (unmanned). Note how powerful the UAS is and how well it meets the requirements of the MPA role.

Figure 9-4 Strait of Hormuz



Source: (Stratfor, 2019)

5) Battlefield Surveillance -The mission is providing detailed

knowledge if the tactical scenario on the battlefield with real-time intelligence of enemy and friendly forces.

6) Airborne Early Warning – Early detection and warning of airborne attack is critical to give air superiority and defensive forces sufficient time to prepare a sound defense. (Moir I. &., 2006)

7) Electronic Warfare (EW) – The role is composed of four subgroups: Electronic countermeasures (ECM) or jamming are common forms of EW used to disrupt communications or enemy radars. Electronic support measures (ESM) – actions taken to intercept, locate, record and analyze radiated electromagnetic energy for the purpose of gaining tactical advantage. Signals Intelligence (SIGINT) consists of Communications Intelligence (COMINT), Radar Intelligence (RADINT), Electronic Intelligence (ELINT) and Measurement and Signal Intelligence (MASINT).[6]

8) Photographic Reconnaissance – This role includes photographic imagery (IMINT) used to confirm SIGINT intelligence.

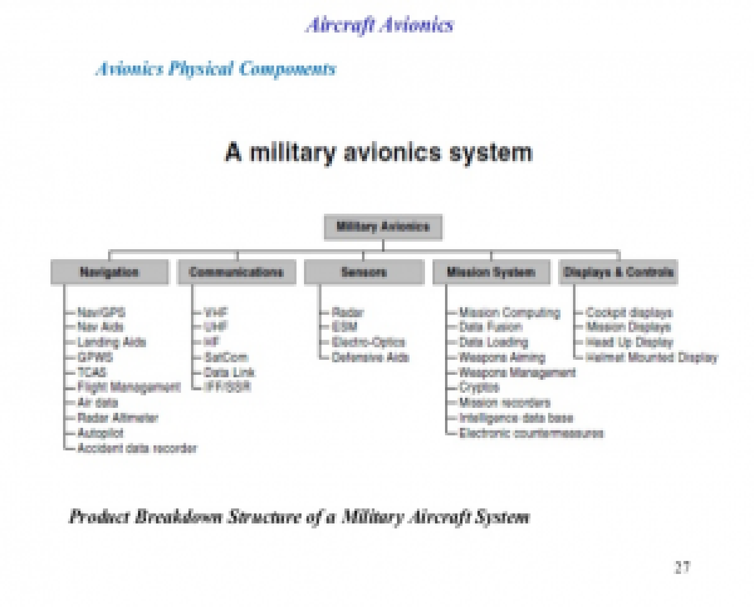
9) Air-to-air refueling – This role is required to extend range or endurance. This role is not easily replaced by UAS -to- UAS refueling. In 2018, Dr Saeed Kahn, Kansas State University, developed a method of drone-to-drone transfer of energy to replenish a UAV battery in flight.

10) Troop / material Transport – Logistics is the primary goal for this role . There is significant initial work on UAMs but as of this writing, this role is not replaceable (safely) by unmanned A/C.

11) Unmanned Aircraft Systems (UAS) – Many UAS have evolved to perform roles described in the previous list with ever-increasing performance and intelligence. (Nichols, et al., 2019)

The basic avionics system has the following major systems: Navigation, Communications, Sensors, Mission System and Displays and Control. Each major has several subsystems, for example, Sensors include Radar, ESM, Electro-Optical, Defensive Aids, and the author adds Acoustical. (Moir I. &., 2006)

Figure 9-5 A Military Avionics System



Aircraft Avionics

Avionics Physical Components

A military avionics system

Military Avionics

- Navigation
  - Nav/GPS
  - Nav Aids
  - Landing Aids
  - GPWS
  - TCAS
  - Flight Management
  - Air data
  - Radar Altimeter
  - Autopilot
  - Accident data recorder
- Communications
  - VHF
  - UHF
  - HF
  - SatCom
  - Data Link
  - IFF/SSR
- Sensors
  - Radar
  - ESM
  - Electro-Optics
  - Defensive Aids
- Mission System
  - Mission Computing
  - Data Fusion
  - Data Loading
  - Weapons Aiming
  - Weapons Management
  - Cryptos
  - Mission recorders
  - Intelligence data base
  - Electronic countermeasures
- Displays & Controls
  - Cockpit displays
  - Mission Displays
  - Head Up Display
  - Helmet Mounted Display

Product Breakdown Structure of a Military Aircraft System

27

Source: p27, https://www.slideshare.net/solohermelin/8-fighter-aircraft-avionicspart-i

Table 9-1 MPA Roles and Tasks

ASuW	ASW	SAR	EEZP	C&EC
Reconnaissance	CAS to task forces & convoys	Location of survivors	Oil rig surveillance	Anti-illegal immigration
Shadowing	Open ocean search	Dropping of survival equipment	Fishery protection	Anti-gun running
Strike against surface vessels	Extended tracking of submerged targets	Scene-of-action commander for rescue operations	Pollution detection & dispersal	Anti-terrorist operations
Tactical support of maritime strike aircraft	Deterrence of hostile submarines	Escort to rescue helicopters		Anti-drug smuggling
Over-the-horizon targeting for friendly vessels	Cooperation with friendly submarines	Cooperation with rescue services		
Intelligence collection	Intelligence collection	Escort of aircraft in difficulties		
Communications relay				
Limited airborne early warning capability				

Source: (Moir I. &., 2006), pp.16-17

Table 9-2 Typical Maritime Patrol Aircraft Platform Architecture[7]

Source: (Moir I. &., 2006), p23

Avionics	Communications	Mission System
Navigation GPS /GNSS	VHF	Maritime Radar
FMS	UHF	Electro-optics turret
Autopilot	HF	ESM
ADF	SHF SatCom	DASS
DME	Link 16-	MAD
TACAN	Link 11	*Acoustic Systems*
TCAS	Marine Band	Mission Recording
Landing Aids	Shortwave	Data loader
GPWS		Cameras
LPI RadAlt		Oceanographic database
Air data		Mission computing
Digital Map		Mission crew workstations
Homing		Intelligence databases
Direction Finding (DF)		
MDP		
Displays & Controls		
IFF /SSR		
Avionics data bus		

Figure 9-6 P-3 Orion MPA

Source: https://www.naval-technology.com/features/feature-the-top-10-maritime-patrol-aircraft/

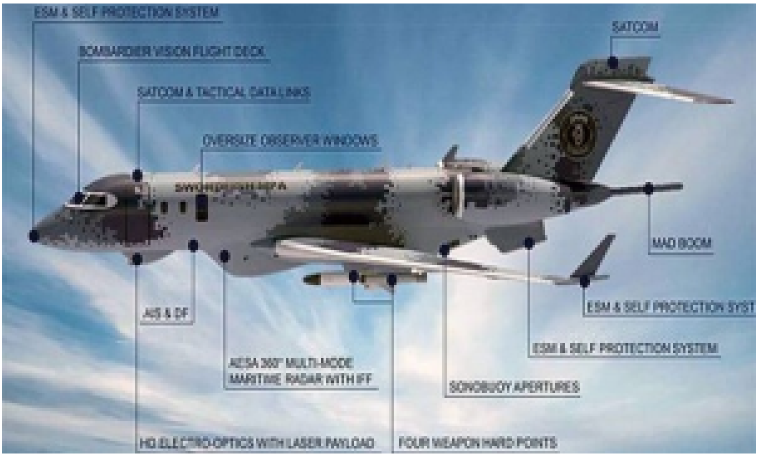
P-3 Orion MPA Example

The P-3 Orion is a long-range maritime patrol aircraft (MPA) with multi-mission capabilities. Its 16-hour fly-time and high ferry range of 8,944 km make it the top MPA in the world. The aircraft was developed by Lockheed Martin principally for the US Navy. The aircraft entered service in 1962 and is currently in service with 21 operators in 17 countries worldwide.

The aircraft can conduct a variety of missions such as maritime / over-land patrol, anti-submarine warfare, anti-piracy, anti-terrorism, drug interdiction and the prevention of illegal immigration. Lockheed Martin offers a P-3 Mid-Life Upgrade (MLU) program to extend the aircraft's service life by 20 to 25 years.

The aircraft can be equipped with infrared and electro-optical (EO) sensors, as well as special imaging radar to detect objects at long ranges. Its large internal weapons bay and ten external hardpoints can house a range of weapons. Four Allison T56-A-14 engines provide the P-3 Orion with a long-range cruise speed of 350k at 25,000ft. (Naval Technology Team, 2019)

Figure 9-7 MPA Example – Swordfish


ESM & SELF PROTECTION SYSTEM
BOMBARDIER VISION FLIGHT DECK
SATCOM & TACTICAL DATA LINKS
OVERSIZE OBSERVER WINDOWS
SWORDFISH MPA
SATCOM
MAD BOOM
ESM & SELF PROTECTION SYST
ESM & SELF PROTECTION SYSTEM
AIS & DF
AESA 360° MULTI-MODE
MARITIME RADAR WITH IFF
SONOBUOY APERTURES
HD ELECTRO-OPTICS WITH LASER PAYLOAD
FOUR WEAPON HARD POINTS

Source: https://defence.pk/pdf/threads/boeing-saab-in-race-for-s-koreas-maritime-patrol-aircraft-order.524698/

Saab Swordfish MPA

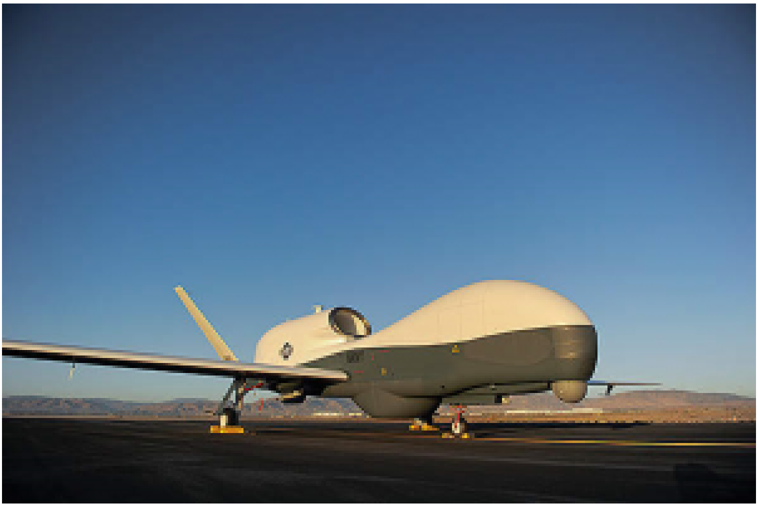
The Saab Swordfish MPA is a multi-mission maritime patrol aircraft that is capable of conducting maritime ISR, maritime counterterrorism, anti-piracy, anti-submarine warfare (ASW) and anti-surface warfare (ASuW) missions. High dash speed and long endurance make the Saab Swordfish MPA an ideal maritime patrol aircraft.

The Saab Swordfish MPA comes with an advanced sensor and C4I package comprising 360° rotating multi-mode maritime surveillance radar, electro-optical sensors with laser payload, automatic identification system (AIS), identification friend or foe

(IFF), electronic warfare and self-protection system, SATCOM, and tactical data links. It also features four weapon hardpoints to carry weaponry load.

Based on the Global 6000 business jet, the Swordfish MPA has a maximum cruise speed of 450k and a long-range cruise speed of 360k. It can remain airborne for 11.5 hours and conduct patrols. (Naval Technology Team, 2019)

Figure 9-8 MQ-4C Triton BAMS MPA (unmanned)



Source: (Naval Technology Team, 2019)

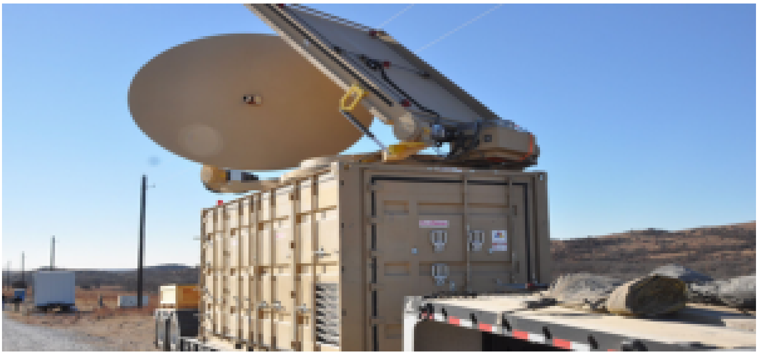
MQ-4C Triton BAMS MPA UAS

MQ-4C Triton is a new broad area maritime surveillance (BAMS) unmanned aircraft system (UAS) unveiled by Northrop Grumman for the US Navy. The UAS will complement the navy's Maritime Patrol and Reconnaissance Force family of systems, delivering SIGNIT (signals intelligence), C4ISR and maritime strike capabilities. The US Navy intends to procure 68 MQ-4C Triton UAS to carry out surveillance missions, along with the manned P-8 Poseidon maritime patrol aircraft. Appendix 9-2 details the MQ-4C design features.

C-UAS Premise [8]

Let's restate the major premise that almost all manned and unmanned systems used in military aviation are vulnerable to attack. (DTRA, 2019) **Hostile actions are both kinetic and *non-kinetic* against the avionics systems. The following sections are concerned with the latter sphere which includes *directed energy* (DE), *cyber warfare*, (CW), *electronic warfare*, (EW), *and a specialized* EMS *subset acoustical countermeasure* (AC)s. [9] All these may defensively apply to hostile unmanned aircraft systems.[10]**

Figure 9-9 High-Power Microwave Weapon to Destroy or Disable Swarms of Unmanned Aircraft



Source: (Military & Aerospace Electronics, 2019)

Effects of Directed Energy (DE) Weapons (EDEW)

Directed energy weapons make up diverse types of weapons such as lasers, particle beams, microwaves and even bullets. All DE weapons are just devices that deposit energy in targets, and that energy which must be deposited to achieve a given level of damage is relatively insensitive to the type of weapon employed. (Nielsen, 2012)[11] American DE weapons may, in fact, change the way future wars will be fought. (Beason, 2005)

Energy cannot be deposited in a target unless it is first delivered to the target. This is called *propagation* of energy. This subject was covered in: (Adamy D. , 2001), (Adamy D. , 2009), and (Nichols, et al., 2019) There is always some loss of energy during propagation. The DE must deliver more energy than needed to damage the target, to compensate for the loss along the way. DE weapon design depends on two factors: First, the anticipated target, which determines the energy required for damage. Second, the anticipated scenario (range, environment, time, etc. See Table 9-3) which determines how much energy must be produced to ensure that an adequate amount energy is delivered in the time available. (Nielsen, 2012)

Table 9-3 Battlespace Dimensions

Dimension	Function	Action
Latitude	Friendly Force Location	Direction of Weapons
Longitude	Enemy Force Location	Maneuver of Forces
Elevation		
Time	Speed of Maneuver	Timeliness of Attack
	Timing of Weapon Release	Enemy Vulnerability
Frequency	Bandwidth Required	Rate of Information Flow
	Bandwidth Available	Interference
	Frequency of Transmissions	Vulnerability to Jamming
		Vulnerability to Intercept

Source: (Adamy D. -0., 2015)

Energy required for damage

Damage may be defined as *Soft* damage which is an upset to the UAS computers to *hard* damage meaning the complete vaporization of the UAS in the air. The former is sensitive to the details of the attack, the hardness of chips, the computer(s) details, communications, circuits and sub circuits. Vaporization produces immediate feedback as to target status – catastrophic. Determining how much energy a weapon must produce to damage a target, two things must be known: how much energy it takes to damage the target, and what fraction of the energy generated will be lost in propagating to it. (Nielsen, 2012)

Ice Cube

Consider the energy required (damage level) to vaporize an ice cube. [12] Pull an ice cube from the refrigerator. Its temperature is below the temperature it will melt. First, we must raise the temperature to melting temperature. The energy required is proportional to both the necessary ΔT rise and the amount of ice in the cube. From thermodynamics, the expression covering this is:

E = mC (Tm-Ti), where E is energy required in Joules, m = mass of ice cube in grams, Ti = the initial temperature in Celsius, Tm= melting temperature, C is the heat capacity constant of proportionality (J/gm x o C).[13] So, E = 2100 Joules of energy required to raise it to the melting point. This is not enough. We must melt the ice cube. Heat of fusion (Lm) is the amount of energy required to convert 1 gm of solid to 1 gm of liquid. With an additional 16,700 Joules, we now have a small water puddle. But our object is to vaporize the ice cube – hard damage. Using the specific heat equation again, E = mC (Tv-Tm), we require an additional 21,000 Joules to raise the ice cube as molten water to vapor at the same temperature by supplying the heat of vaporization, Lv = 2,440 Joules per gm of water. This means an additional 122,000 Joules of energy are required. The total amount of energy needed to vaporize an ice cube of 50 gm is 161,000 Joules. Lv accounts for about 75% of the required energy.

10,000 Joules

(Nielsen, 2012) gives a table of thermal properties of Aluminum, Copper, Magnesium, Iron and Titanium. It shows that most solid materials (See Table 9-4) have density on the order of 1 – 10 gm /cubic centimeter and that 10,000 Joules is sufficient energy to vaporize about one cubic centimeter of anything! 10,000 Joules is a magic number because it is close to the energy delivered by a wide range of DEs. (Nielsen, 2012) A typical rifle round has about 10 gm and is fired at a muzzle velocity of 1000 m/s. (Halsam, 1982) This corresponds to a kinetic energy (KE) of (mv 2 /2) of 5,000 Joules. A roman Catapult could throw a 20 Kg stone over 200 meters. The KE required for this use is about 40,000 Joules. (Foley, March, 1979) A medieval crossbow could launch an 85-gm bolt over 275 meters. This required 13,000 Joules. (Vernard Foley, January, 1985)

Table 9-4 Thermal Properties of Common Materials

Material	Density Gm/ cm3	Melting Point, Tm 0C	Vaporization Point, Tv 0C	Heat Capacity (J/ gm0C)	Heat of Fusion (J/gm)	Heat of Vaporization (J/gm)
Aluminum	2.7	660	2500	0.9	400	1100
Copper	8.96	1100	2600	0.38	210	4700
Magnesium	1.74	650	1100	1.0	370	5300
Iron	7.9	1500	3000	0.46	250	6300
Titanium	4.5	1700	3700	0.52	320	8800

Source: Table 1-1 (Nielsen, 2012)

Energy Alone Sufficient for Hard Damage?

In a nutshell, no. A nuclear bomb releases a lot of energy. One Kiloton yields 4,000,000,000,000 Joules. Well above the 10,000 Joule criterion, but at a distance of less than a mile from detonation, a concrete structure is undamaged. Over the same range an artillery shell with only 10,000 Joules of energy could easily destroy such a structure. Consider also the sun. It delivers about 5,000 Joules of energy over every square centimeter of the earth's surface, yet we see no cars melting or people fried. *Clearly, the energy must be delivered over a small region and in a short time to the target. Energy is not the silver bullet for damage.* We must consider also density of energy on the target (Joules per square centimeter),[14] the rate of energy delivery, or power (Joules/ sec or Watts). The nuclear bomb is not a DE weapon like the artillery shell. Much of the energy released does not intersect with the concrete structure and is "wasted". The artillery shell is a DE and concentrates all of its energy right to the target in question. If we spread the energy of the bomb over a surface of a sphere at a range of one mile, the energy density is only 13 Joules per square centimeter, far less that the DE artillery shell density of 10,000 Joules per square centimeter. With the spreading of blast energy accounted for, the nuclear bomb is consistent with other weapon types. (Nielsen, 2012)[15]

Energy Delivery Rate

If energy is delivered over too long a period, it is not effective in damaging the target UAS. The target can shed energy as rapidly as it is deposited. Cars in a parking lot, (unfortunately fatal to youngsters or animals left in the car) until they become so hot that they radiate energy away as rapidly as its deposited, so they don't heat up to a point of sustained damage. After that they heat up to a constant temperature. Only if energy is delivered more rapidly than the target can handle it will damage ensue. (Nielsen, 2012)

From thermodynamics, we know that energy can be transferred away (lost in propagation) from a target by conduction, convection and radiation.

Thermal conduction losses (energy flow or "downhill" temperature gradient (slope of curve of temperature v distance) from hot regions to cold regions moving the temperature to equilibrium in the system). The equation for thermal conduction is

$U = -k(dT / dx)$ Equation 9-1

Where U = rate of flow of energy across a surface, J/cm2 sec

dT /dx = the slope of the temperature curve, degrees / cm

k = constant of proportionality called thermal conductivity[16] in J/ sec cm deg

Energy flows until the temperature is the same everywhere in the system.

Convection (heat loss by macroscopic motion of molecules). Think of an attic fan moving hot air out of the attic, where motion is induced by the fan blades. The expression for wind induced convection for temperature v distance:

$dT /dt = - V dT/ dx$ Equation 9-2

Where V = wind velocity

T = temperature in time at point x

dT /dx is the rate of change of Temperature in time at point x

For a target to lose energy by conduction or convection, it must be immersed in the atmosphere, water or some fluid medium to supply the necessary molecules to carry the energy away.

Black Body[17] radiation can occur in space or in a vacuum. Molecule movement is not just random, they vibrate, rotate and incorporate energy in their internal structure.

The total intensity of radiation emerging from the surface of a Black Body, S (Watts/cm2) is:

$S = \sigma T4$ Equation 9-3

Where σ = Stefan-Boltzmann constant = 5.67 x 10-12 (Watts/cm2 K4), K= Kelvin temperature.

Implications

Damaging targets depends not only on delivering energy, but also concentrating the energy in both space and time. In space we deliver about 10,000 Joules per cm2 of target surface, either at a single point, (bullet) or over the whole surface, as in a nuclear weapon. In time, energy must be delivered more rapidly than the target can shed energy through conduction, convection and radiation loss mechanisms. The fluence (Joules / cm2) or Intensity (Watts /cm2) necessary to damage a target will vary with time or pulse width that the weapon engages the target.[18]

Energy Losses in Propagation

There are two types of energy losses in propagation: the spreading of energy such that it does not interact with the target, and the wasting of energy in interactions with a physical medium, such as the atmosphere, through which it passes to destroy the target. Type one occurs whether the weapon or target is located on earth or in the vacuum of space. Type two occurs primarily when weapon or target lies within the atmosphere. Table 9-5 shows the Energy losses in propagation as a function of weapon type and loss mechanisms.

Table 9-5 Energy losses in Propagation

Weapon Type	Energy Loss Mechanism
Kinetic Energy (bullets, rockets)	Atmospheric Drag
Lasers	Absorption by molecules Scattering by molecules Absorption by aerosols (small particles) Scattering by aerosols
Microwaves	Absorption by molecules Scattering by molecules Absorption by water droplets Scattering by water droplets
Particle Beams	Energy losses to electrons Scattering from nuclei Scattering from electrons Radiation

Source: (Nielsen, 2012)

Advanced DE research is both fascinating and mostly classified. Below are examples of military systems that may be used for C-UAS defenses.

Directed Energy (DE) Counter Weapons, High-Powered Microwave (HPM) Defenses, High-Power Lasers (HPL)

The US Air Force Research Laboratory is investing US$16 million in further field assessment of Raytheon's Phaser High Power Microwave System outside the continental U.S. [See Figure 9-9] The testing phase will span over 12 months in which the Phaser will engage simulated and real unmanned aerial systems threats. The evaluation will explore the effectiveness of Phaser's counter-drone engagement without disrupting the necessary installation operations.

The effectiveness of Phaser against drones has already been demonstrated at the Army MFIX exercise in 2018, when the system eliminated 33 drones, 2-3 at a time. Currently mounted on a shipping container-like box, Raytheon plans to significantly reduce the size in future versions.

AFRL already evaluates two other HPM systems – the Tactical High-Power Operational Responder (THOR), [See Figure 9-10] that deploys as a means to provide base defense against drones, and 'Counter-Electronic High-Power Microwave Extended-Range Air Base Air Defense' system, or CHIMERA, designed to engage multiple targets over a larger area.

The HPM contract follows a separate Air Force contract in which Raytheon will build two prototype high-energy laser systems, also to be deployed overseas. The HPM and HEL systems can be used independently or together to counter-unmanned aerial system threats. "There's more than one way to defeat a drone," said Dr. Thomas Bussing, Raytheon Advanced Missile Systems vice president. "We are delivering the world's first defensive directed energy systems that can be used alone or in tandem to defeat enemy drones at the speed of light." (Eshel, 2019)

Figure 9-10 THOR

Source: (Eshel, 2019)

Raytheon announces delivery of first laser counter-UAS system to U.S. Air Force

U.S. defense contractor Raytheon Co announced that it successfully delivered the first high-energy laser counter-unmanned aerial system to the U.S. Air Force earlier this month.

In recent years, the Defense Department has assessed directed energy weapons—more commonly known as “lasers”—as an affordable alternative to traditional firepower to keep enemy drones from tracking and targeting troops on the ground. The system will be deployed overseas as part of a year-long Air Force experiment to train operators and test the system’s effectiveness in real-world conditions. See Figure 9-11.

Raytheon’s high-energy laser weapon system uses an advanced variant of the company’s Multi-spectral Targeting System, an electro-optical/infrared sensor, to detect, identify and track rogue drones. Once targeted, the system engages the threat, neutralizing the UAS in a matter of seconds.

"Five years ago, few people worried about the drone threat," said Roy Azevedo, president of Raytheon Space and Airborne Systems. "Now, we hear about attacks or incursions all the time. Our customers saw this coming and asked us to develop a ready-now counter-UAS capability. We did just that by going from the drawing board to delivery in less than 24 months."

Raytheon installed its high-energy laser weapon system on a small all-terrain vehicle. On a single charge from a standard 220-volt outlet, the HELWS can deliver intelligence, surveillance and reconnaissance capability and dozens of precise laser shots. It can also be paired with a generator to provide a nearly infinite number of shots.

Raytheon Company is integrating multiple proven technologies to counter the unmanned aerial system threat across a wide range of scenarios – from commercial airports to forward operating bases to crowded stadiums. Raytheon's portfolio of sensors, command and control systems, and kinetic and non-kinetic effectors covers all aspects of the UAS threat. (Raytheon, 2019)

Figure 9-11 Raytheon announces delivery of first laser counter-UAS system to U.S. Air Force

Source: (Raytheon, 2019)

Modern Communication Threats to UAS

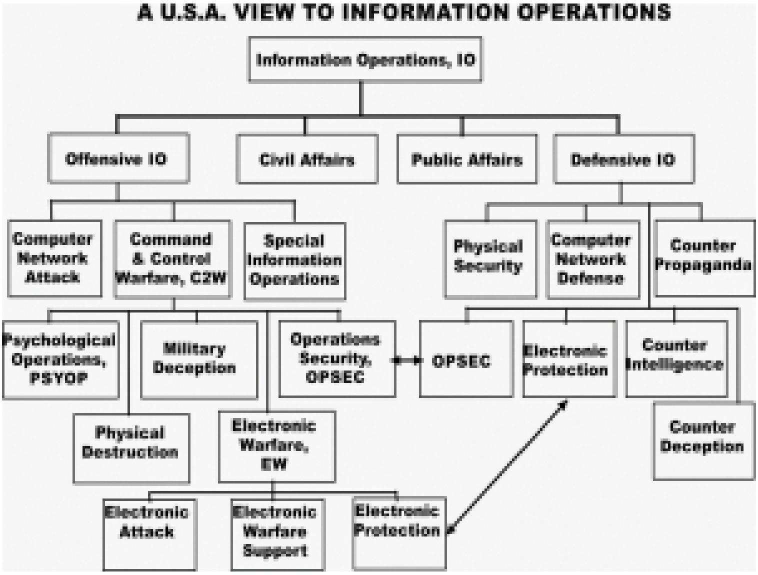
Unmanned Aerial Systems (UAS) are in widespread use for reconnaissance, EW, and weapons delivery. They are extremely dependent on interconnection with ground stations by command and data links. (Adamy D. , 2001) The increased use of Low Probability Intercept (LPI) has become a significant challenge to electronic warfare (EW) communication links. (Adamy D. , 2001) This chapter explores LPI and Jamming. The student should then have enough background to understand the criticality of LPI and Jamming of UAS communication links. Air defense missiles and associated radars make significant use of interconnecting links. (Adamy D. , 2001) SUAS sometimes use cellphones to command and control the UAVs. Cell phones are widely used for command and control function in nonsymmetrical warfare situations. (Adamy D. , 2001) ISIS and other terrorist groups use cell phones to trigger improvised explosive devices.

Cybersecurity attacks on data communications links are highly classified. Similarly, modern radar threats to hostile installations are also generally classified. Before examining LPI and communications signals/link- jamming, we first review the EW environment specific to UAS. Time for a few definitions of terms.[19]

Information Operations (IO) and the part EW plays

Figure 9-12 shows the global view of Information operations. Note how nicely all the prior definitions fit into the puzzle? Note that EW is a key component of IO, but not the singular dominant puzzle piece. [20]

Figure 9-12 Information Operations



Source: *http://c4isys.blogspot.com/2013/11/basics-of-information-operations-24.html* *also Source:* JP 3-13 (Joint Publication) and pertains to Information Operations (IO) in the United States. http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf

Autonomy vs. Automation

Table 9-6 shows the normal five levels of automation that characterize UAS systems with examples of commercial vehicles. NASA presents a more detailed level of automation breakdown based on the OODA (Observe, Orient, Decide and Act) decision loops. (Barnhart, 2012) However, Table 9-6 should suffice to understand the cyber-purview. Level 1 slave and Level 2 Automated (minimal) are commonly found on UAS sold at Amazon, Walmart, and similar outlets. The pilot makes all the decisions and has complete control of flying orders. Level 3 steps up the navigation capabilities using an a priori mission plan.

Levels 4 and 5 add higher-level decision-making capabilities; collision avoidance without human intervention, complex mission planning in all weather conditions, expert systems intelligence without human intervention i.e. Artificial Intelligence (AI) and advanced Sense and Avoid systems (SAA). Level 5 is not commercially available; many designers are well on their way to a fully operational Level 5 UAS.

Table 9-6 UAS Automation Scale

Level 1: Slave – assisting piloting, reaction to disturbance

Level 2: Automated – maintains its flying orders and receives higher level orders

For Levels 1 and 2 are common, require pilot intervention and continuous communication link;

reasonable prices < $1500 US, small, weight < 10lbs: Drone Parrot, Quad Flyer GAUI

Level 3: **Automated Navigation** (a priori mission plan)

For Level 3 micro-UAS premium (< $20,000 US): Dragonfly, Microdrone Gmbh,

Fly-n-Sense, Mikrokopter

Level 4: Response from contextual data *Collision Avoidance* (CA) (w/o human intervention)

For Level 4 minimum knowledge of surrounding environment, reacts to events, perform CA,

uses active SAA, requires mission plan

Level 5: Decision-Maker (expert system) from contextual data: navigation in unknown environment,

complex missions, coordination and collaboration of signals

For Level 5 AI, decision making with heavy networked computer support, perceptive sensors

for space and time, complex mission in unknown environments, capable of intelligent adjustments

including mission rescheduling, keyword- adaptive control Levels 4 and 5 are confined

to laboratories. (Nichols R.-0. , 2016)

Table 9-7 UAS Collaboration shows four types of possible UAS collaboration. At the lower end of a threat scale is the isolated UAS or a small group of UAS. The advantages lie in a specific mission, which may be piloted or autonomous. They carry light payloads and are affordable. They are easy to assemble in the field. An example is the Raven used by US Special Forces. The disadvantage (countermeasure applied) is to identify the pilot or leader vehicle and destroy/disable it. A UAS attack team is particularly effective against divided attack targets, Level 3 allows automatic navigation, synchronized actions, and limited updated mission information. With increased team members, synchronization is not guaranteed. Disabling part of the UAS Team does not guarantee that mission failure. The real vulnerability of the UAS team is the Chief. All synchronization and updates go through the Chief. Disable/destroy the Chief and the Team is rendered useless. Determining who the Chief is critical.

Far more dangerous is the Swarm configuration especially in the higher levels of autonomous engagement. Swarms have several advantages. They are efficient based on numbers; they demonstrate emergent large group behaviors and reactions. Even not controllable or automated, they show a decentralized intelligence – think shoal of fish with evolving local rules. UAS Swarms are a highly resistant form, not changing based on survivability of members. There is no hierarchy like a team. Destroy part of the swarm and the rest will continue their mission without abatement.

The two known countermeasures are: 1) **Disrupt / Change the Strategic Global View of Swarm (its only real vulnerability) and 2) Force defender collaboration. (Nichols R.-0. , 2016)** China appears to be the leader in innovative UAS swarm intelligence, through the efforts of the Chinese Electronics Technology Group Corporation (CETC). (Kania, 2017) This is not a threat to be underestimated.

Table 9-7 UAS Collaboration

Type 1: Isolated Individual UAS

Advantages: piloted or autonomous w/ specific mission to perform. Small, easy to assemble, affordable, light payloads.

Countermeasures: Stop, Disable or Destroy Pilot, Threat removed.

Type 2: Group of Individual UASs (Isolated with own mission but not coordinated)

Advantages: sphere of action may be different for each mission, increased numbers, and increases success of attacks by defenses saturation

Countermeasures: Stop, Disable, Discover and Deter or Destroy Pilot(s), Threat(s) may be removed.

Type 3: Team of UASs (All members assigned specialized tasks and coordinated by Chief)

Advantages: Particularly effective against divided attack targets, Level 3 allows automatic navigation, synchronized actions, but no update to mission plans based on field activities.

Disadvantages: Level 4 (w/o humans) yields surrounding reactions but may lose synchronization between team members.

Level 5 permits continuous updates, communications, commando style.

Countermeasures: Stop, Disable or Destroy Team members. Determine behavior logic and intervene. Survival of team members is critical to defense actions. Threat mitigated.

Type 4: UAS Swarm (Uniform mass of undifferentiated individual's w/o Chief at level 4 or 5)

Advantages: Efficient based on numbers, emergent large group behaviors and reactions, not controllable or automated, decentralized intelligence – think shoal of fish w/ evolving local rules; highly resistant form, not changing based on survivability of members, no hierarchy

Countermeasures: Disrupt / **Change the Strategic Global View of Swarm (its only real vulnerability). Defender collaboration. (Kania, 2017)**

Commercial Small Unmanned Aircraft Systems (sUAS) Overview

There is a natural tendency to think that small unmanned aircraft systems present no threat, especially to US defenses. They are simply recreational or commercial toys. But they present a threat to National Airspace (NAS) – especially near airports. Figure 9-13 shows the results of a sUAS crashing into a jetliner in 2016.

Figure 9-13 Drone Crash into 737-700 passenger jet while landing at Mozambique

Source: UK Express, http://www.express.co.uk/travel/articles/751165/drone-boeing-737-plane-crash-mozambique. Also See: https://youtu.be/2jzx8BpDuHE

USA FAA Part 107 special rule forbids use of sUAS within a five-mile radius of an airport. (FAA, 2018)

Table 9-8 shows some of the available options and each year more capabilities are being added. Imaging, camera capabilities, weatherproofing, and payloads all can be used to gather intelligence, provide reconnaissance or deliver a lethal payload. They are radar resistant and deploy with a very small heat signature, so they can be in close target quickly, before defenders can activate countermeasures.

Table 9-8 Commercial sUAS Parameters

- “**Flying Characteristics** Available as **RTF** (off-the-shelf Ready to Fly); **BNF** (Bind and Fly –with custom transmitter); **PNF** (Plug and Fly with custom transmitter, receiver, battery, and charger). RTF and BNF – no prior flight experience required.

- **Models** most rotary multicopter – quad (4), hexa (6) octo (8) variants. Fixed wing used for deployments in agriculture, public safety, emergency response and ISR (Intelligence, Surveillance, and Reconnaissance) many fully customizable to achieve specific capabilities, flight time, payload capacity, programmable flight, maximum speed and weather hardening.
- **Average SUAS flight time** 18 minutes, average range approximately one mile, cost $600 US, dry conditions" (Angelov, 2012)

Specifications affecting hostile UAS operations

- **Payload capacity** function (weight and size more than gimbal, camera, battery) LIDAR or infrared or experimental sensors require larger capacity and subject to easier detection.
- **Range** function (signal transmission, LOS, image relay distance, battery and power constraints).
- **Weather Proofing** function (limited operating conditions, mostly dry. Upgradable to near military grade to operate in extreme conditions) Retrofit to harden for weather is a trade-off for weight, cost, flight time and payload capacity unless no of rotors increases.
- **Imaging** function (available medium –high resolution cameras of > 12 megapixels, with still and video) Infrared and LIDAR installable.
- **Automated and Programmable Pilot / Follow Me** settings function (predetermined flight mission path based on GPS coordinates (Fly-by-wire). Some with Follow Me autopilot settings enable the SUAS to automatically follow the operator. (Angelov, 2012)

Airborne Sensing Systems

There are two technologies available for airborne sensing of other aircraft; cooperative and non-cooperative. Cooperative technologies receive radio signals from other aircraft's onboard equipment. Two requirements for cooperative behavior. First ATC Transponder, which responds to ground-based secondary radar interrogations for air traffic control (ATC) usage. Traffic Alert Collision Avoidance System (TCAS) uses the same technology in FAA classes of airspace. Second is the Automatic Dependent Surveillance – Broadcast systems (ADS-B). ADS-B technology uses the Global Positioning System (GPS) or alternative navigational source to make broadcasts of its own aircraft position, velocity, and data required to avoid collisions. (Angelov, 2012) Table 9-9 shows typical sensor coordinate systems. The first three cooperate with each other, the latter five are non-cooperative technologies. (Angelov, 2012)

Table 9-9 Typical Sensor Coordinate Systems

Sensor Technology	**Coordinate System**
Active interrogation of Mode A/C transponder	Relative range, altitude
TCAS	Relative range, altitude
ADS-B	Latitude, longitude, altitude, velocity
Electro-Optical	Bearing (azimuth and elevation)
Laser /LIDAR	Relative range
Onboard radar	Relative range, Bearing (azimuth & and elevation)
Ground-based radar	Range and bearing from ground-reference
Acoustic	Bearing

Sensor Parameters

Sensor technologies use standard parameters to provide a basis for comparison and ISR performance. Table 9-10 Standard Sensor Parameters shows the base set:

Table 9-10 Standard Sensor Parameters

Sensor	**Function**
“Field of View	Describes angular sector within sensor making measurements. Outside this field of view, sensor is blind.
Range	Distance measured by sensor, within which some good probability of detection of targets
Update Rate	Interval at which sensor provides measurements
Accuracy	Uncertainty of position measurement – usually single dimension
Integrity	Probability that measurement falls beyond some normal operation limit
Data Elements	Cooperative sensors – specific data to enhance ISR platform, ex: trajectory, identity, intent” (Angelov, 2012)

SAA Critical Control Systems include circuitry to affect UAS movement, landing, control of direction, detection, and correction of the aircraft. Many of these functions are incorporated into a UAS Autopilot, if capable.

Autopilot

Table 9-11 shows the common components found in UAS autopilots. These provide the means for UAS to affect movement, control, communications, detection, emergency operations, battery, waypoint delivery, and payloads.

Table 9-11 Common components found in UAS autopilots

- “Main Program/Processor: processing sensor data & implementation of control of UAV

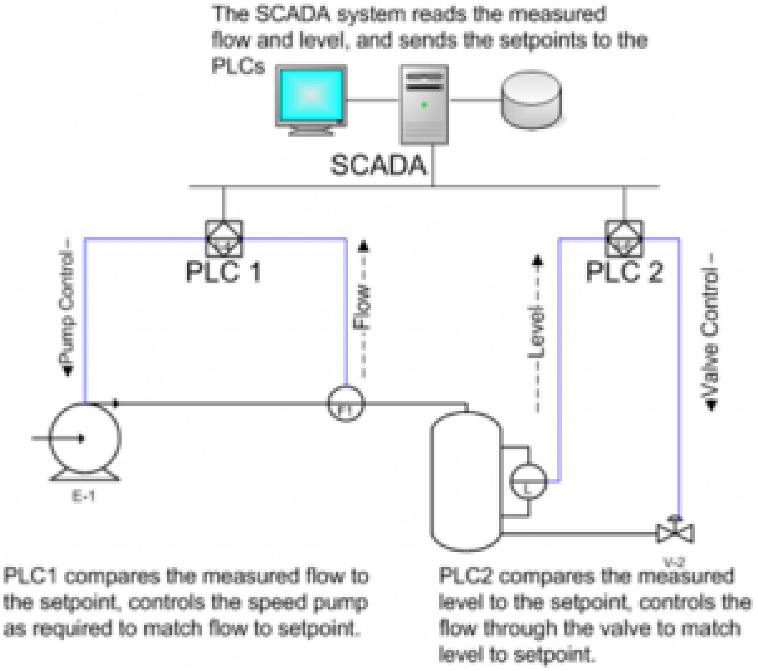
- Magnetometer: measuring direction
- GPS: determine global position
- Airspeed/Altimeter: measure air speed & altitude
- UAV Wireless Communication: communicating with ground station
- Power System: provides power to UAV
- Inertial Measurement Unit: measures movement of UAV
- Boot Loader Reset Switch loads programs into main program board
- Actuators: receives commands from main processing board & moves control surfaces
- Manual Flight Control: overrides autopilot & gives control of UAV control surfaces to ground station" (Clothier R. R., 2011) (Boutros, 2015)

SCADA

The security fault "low hanging fruit" in UAS systems is SCADA. There are hundreds of millions of SCADA systems. They are used to control every practical machine you can imagine. SCADA stands for **Supervisory Control and Data Acquisition.** SCADA started in the 1940's to control manufacturing processes such as flow rates, temperatures, valves, pressure, density, chemical, mechanical processes of all kinds. See Figure 9-14 for Legacy SCADA system for Chemical Plant. (Nichols R., Nov 28-30, 2006)

SCADA systems have improved significantly over the decades in all areas except one – **SECURITY**. SCADA systems are a security sieve. Figures 9-15 & 9-16 show examples of SCADA Architectures. (Nichols R., Nov 28-30, 2006) An interesting example are the automated/computerized systems in modern cars.

Figure 9-14 for Legacy SCADA system for Chemical Plant.


The SCADA system reads the measured flow and level, and sends the setpoints to the PLCs
SCADA
PLC 1
PLC 2
Pump Control
Flow
Level
Valve Control
FT
LT
E-1
V-2
PLC1 compares the measured flow to the setpoint, controls the speed pump as required to match flow to setpoint.
PLC2 compares the measured level to the setpoint, controls the flow through the valve to match level to setpoint.

Source: (Nichols R. , Nov 28-30, 2006)

Everything is controlled by SCADA; tires, engine, seat belts, safety bags, oil pressure, even door locks. However, cyber hackers can exploit SCADA to disable a car remotely, with the driver still in it! Greenburg, Wired (2015). Hackers Remotely Kill a Jeep on the Highway—With Me in It. (Greenburg, 2015)

"**UAS ARE JUST FLYING SCADA MACHINES!**" (Nichols R.-0. , 2016) Table 9-12 SCADA shows the principle functions that apply to all SCADA systems, especially UAS.

Table 9-12 SCADA Functions

- Supervisory Control and Data Acquisition (SCADA) systems facilitate management with remote access to real-time data

- Channel to issue automated or operator-driven supervisory commands to remote station control devices
- A human–machine interface (HMI) is responsible for data presentation to human operator

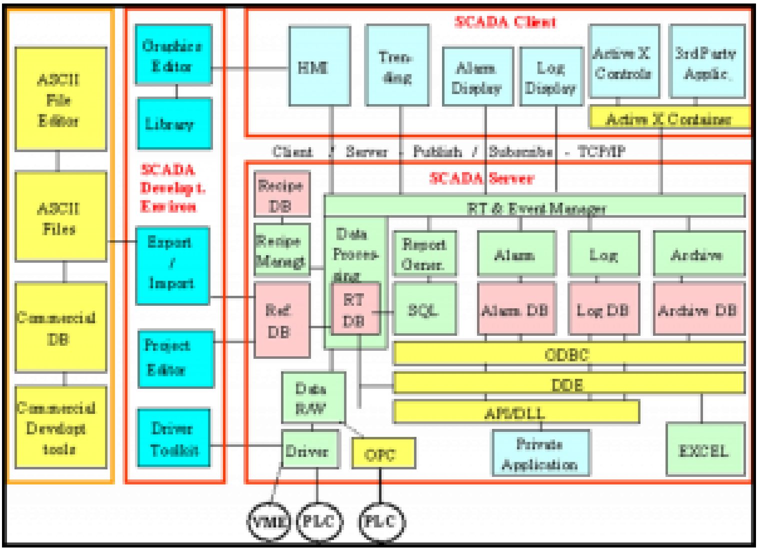
- Composed by a console that makes it possible to monitor & control process

- Remote terminal units (RTUs) are microprocessor-controlled electronic devices that interface sensors to SCADA by transmitting telemetry data

- Is a process control system for computerized real-time monitoring and control
- Typically consists of:
  - Master Control Unit (MCU)
  - Remote Terminal Unit (s) (RTU)
  - Communication Links
- Supervisory system is responsible for:
  - Data acquisition
  - *Control activities on process*
- Programmable logic controllers (PLCs) are final actuators used as field devices
- Communication infrastructure connecting supervisory system to RTUs
- Various process & analytical instrumentation
- RTU's Alarm Systems
  - Doors
  - Battery Backup
  - Low Power/Loss of Power Alarm
  - Power Protection
  - Passwords for Keypads, PC ports

- Log Alarm (or Event) When Local User Plugs PC in or Signs On
- Log Event when Local User Changes Values

Figure 9-15 UAS SCADA System Internals



Source: (Nichols R. K., Hardening US Unmanned Systems Against Enemy Counter Measures, 2019)

SCADA systems have plenty of cyber related vulnerabilities. Most are connected to computers. Those vulnerabilities multiply when connected to the Internet. SCADA systems differ from the IT structures. (Shapiro, 2006) Table 9-13 Sample SCADA Design Vulnerabilities apply to all systems including UAS. (Nichols R. , Nov 28-30, 2006)There are so many design flaws and vulnerabilities in SCADA systems that the US government has a special SCADA testing lab in Utah and has published copious recommendations to improve security. (NTSB, 2009)

Table 9-13 Examples of SCADA Design Vulnerabilities

- Ease of operation outweighs security
- Commonly set up on operating systems with known vulnerabilities
- Poor authentication systems in place
- Remote access allowed for maintenance &/or IT support
- Interconnectivity to vulnerable corporate networks
- Weak access control lists on firewalls
- Proper Network Access Control (NAC) is most crucial to prevent unauthorized connection within network

- First target of compromise for an attacker
- No use of standard IT defense software
- Wireless technology common
- System connect to unsecured remote processors
- SCADA software not designed with robust security features
- Public information often available on specific systems
- Poor physical security on remote access points
- No use of standard IT defense software
- Wireless technology common
- System connect to unsecured remote processors
- SCADA software not designed with robust security features
- Public information often available on specific systems
- Poor physical security on remote access points. (Kilman, 2003)

Attack Vectors

A brief overview of UAS Attack Vectors (by no means the exhaustive list) is demonstrated in Table 9-14. (Nichols R.-0. , 2016)

Table 9-14 Common Attack Vectors

“Common Vectors

- Backdoors & holes in network perimeter
- Protocol vulnerabilities
- Attacks on field devices through cyber means Database attacks
- Communications hijacking & Man-in-the-middle attacks
- Cinderella attack on time provision & synchronization
- Bogus input data to controller introduced by compromised sensors &/or exploited network link between controller & sensors
- Manipulated & misleading output data to actuators/reactors from controller due to tempered actors/reactors or compromised network link between controller & actuators

- Controller historian changes – feed forward control
- Distributed Denial of Service – missing deadlines of needed task actions
- Backdoors and holes in network perimeter
- Vulnerabilities in common protocols
- Attacks on field devices through cyber means
- Database attacks
- Communications hijacking and Man-in-the-middle attacks
- Cinderella attack on time provision and synchronization
- To a control engineer, possible attacks can be grouped into following categories:
- Bogus input data to controller introduced by compromised sensors and/or exploited network link between controller and sensors

- Manipulated and misleading output data to actuators/reactors from controller due to tempered actors/reactors or compromised network link between controller and actuators

- Controller historian

- Denial of Service – missing deadlines of needed task actions

Attacks on Software:

- No Privilege Separation in Embedded Operating System
- Buffer Overflow
- Structured Query Language Injection

Possible UAS Attack Hardware / Software

- SkyJack© [21]
- Aircrack-ng© [22]
- Node-ar-drone©
- Raspberry Pi©
- Parrot AR. Drone -2©
- Alfa© AWUS036H wireless adapter
- Edimax© EW-7811Un wireless adapter
- Snoopy© [23]

Attacks on Communication Stack

- Network Layer
- Transport Layer
- Application Layer

Auxiliary tools:

- Password Theft
- Wireshark
- Man-In-the-Middle Attacks
- Trojan Horse Virus
- Distributed Denial of Service Attacks" (Nichols R.-0. , 2016)

Cyber – Attack Taxonomy

UAS SCADA systems susceptible to a broad range of cyber and network specific attacks on the SAA modules in the aircraft and communication structures from the ground or satellite links. These represent system threats and vulnerabilities of the UAS structure, increasing the risk of hostile use or takeover. (Nichols R. , Nov 28-30, 2006)A UAS Cyber Attack Taxonomy is an organized view of potential cyber threats to UAS assets. *The Taxonomy is a list of agents that increase risk of a successful attack on* US UAS ADS *assets.* The risk of success of terrorist attacks on USA Air Defense Systems (ADS) via UASs is higher because of improving commercial capabilities and accessibility.

A qualitative view of information risk (*also a measure of cyber-attack lethality*) in a system such as SAA or computer network is expressed as:

Risk = (Threats x Vulnerabilities x Impact / Countermeasures) Equation 9-4

And at time state 0, this equation can be reduced to

Risk ~ function (Threats / Countermeasures) Equation 9-5

(Nichols R.-0. , 2016)[24]

At time state =0, where Vulnerabilities & Impact are constants and drop out of the equation.

Threats are real, and if applied in the absence of appropriate countermeasures, will increase the likelihood of a successful cyber-attack. Vulnerabilities are weaknesses in the system that a threat may or may not exploit. Vulnerabilities essentially in the system, ab initio. Threats can be mitigated or improved based on the attack circumstances. Impact is an after-the-fact accounting of the cyber-attack. No matter what the magnitude, it is a constant. Countermeasures are a host of technologies that can be applied to mitigate threats and reduce Risk. Increased Threats means increased Risk. Increased Countermeasures means decreased Risk. In practice, these equations require a qualitative legend to make comparable cases. Conversely, decreased threats means decreased Risk and decreased countermeasures means increased Risk. (Nichols R.-0. , 2016)Some authors use Vulnerabilities to assess Risk. (Garcia, 2006) Therefor our cyber-attack taxonomy must work for either Risk approach. There are many approaches to evaluating Risk. The authors choose the simplest approach to understand the attack vectors.

Software – Based Vulnerabilities

"Military UAS defense systems deploy widely used software in their network devices: Operating systems, open source software, routers, radio frequency devices, Internet Connection Sharing (ICS) and SAA SCADA." (Sood A.K. & Enbody, 2014) UAS ground system network software may have the standard vulnerabilities; "hardcoded passwords, backdoors in firmware, insecure protocols, Remote Command Execution (RCE), default passwords for Human-Machine Interfaces (HMIs), Insecure authentication and authorization, malicious hardware, critical infrastructure systems have hardcoded passwords embedded in firmware which may allow attackers to gain complete access to system." (Sood A.K. & Enbody, 2014) It doesn't end there.

Other software-based vulnerabilities: "Backdoors exist for support or remote access purposes, Hardcoded passwords easily obtained by: Reverse engineering firmware, analyzing functional components," (Sood A.K. & Enbody, 2014) Remote Code Execution (RCE) which is an attacker's ability to execute attacker's commands on target machine or target process remotely. Another RCE vulnerability is a software bug that gives attacker way to execute arbitrary code or ability to trigger arbitrary code execution from one machine on another. (Nichols R.-0. , 2016)

Unfortunately," Remote Code Execution (RCE) can be triggered by exploiting security flaws in: Operating system components, browsers," ICS, SCADA, routers, Microsoft Office, Adobe Reader, and

Java. Remote Code Execution (RCE) is a powerful threat to UAS and supporting computer systems. "Attackers exploit security issues; buffer overflows (stack, heap, integer), use-after free errors, race conditions, memory corruption, privilege escalations and dangling pointers."

Remote Code Execution (RCE) vulnerabilities keeps growing and RCE vulnerabilities allow "attackers to execute arbitrary code on compromised systems, drive-by downloads, spear phishing attacks." (Sood A.K. & Enbody, 2014)

ICS/SCADA is particularly vulnerable to remote code execution vulnerabilities. Another form is SQL injections, "which exploits weaknesses in web applications to allow attackers' queries to be executed directly in backend database" and allow attackers to extract sensitive information such as credentials, emails, critical documents, intelligence. "Data stolen using SQL injection can provide critical information for advanced UAS targeted attacks." (Sood A.K. & Enbody, 2014)

The final group in the software- based vulnerabilities set is "insecure authentication and file uploading flaws. These allow remote attackers to access critical systems by exploiting weak authentication design and uploading malicious code or firmware. This security issue persists due to inability of systems to implement granular control through proper authentication and authorization checks. File uploading attacks exploit a system's inability to determine type of files being uploaded on server." (Sood A.K. & Enbody, 2014)

Hardware-based Vulnerabilities

The US sometimes picks the wrong vendors to supply its UAS critical hardware. Hardware imported from China includes backdoor access to hardware after deployment. "Exported Chinese manufacturing units compromised military-grade FPGA computer chips, circuits, and counterfeit devices, such as scanners." "Zombie Zero malware has been implanted in software of scanner hardware manufactured in China as part of attack targeting shipping and logistics industries, especially printers. When scanners are connected to networks, they provide platforms for compromising networks. Counterfeit devices and circuits developed in China for U.S. military and defense contractors to be used in warships, missiles, airplanes and UAS." (Sood A.K. & Enbody, 2014) (Threat to all nations that receive hardware pre-installed with malware.) (Nichols R.-0. , 2016)

"Hardware based vulnerabilities observed in actual attacks on military defense systems (Army) and applications include the following; backdoors and hardcoded passwords, compromised

GPS Satellite Communication (SATCOM) systems," SCADA systems vulnerable to buffer overflows, and compromised GPS SATCOM systems. The Navy had its share of hardware-based threats; Remote Code Execution – "XMLDOM Zero-day vulnerability was exploited to attack U.S. Veterans of Foreign Wars' website, SQL injections, Royal Navy website hacked, U.S. Army website hacked, insecure protocols, spoofing and hijacking and attacks to spoof GPS communication to control U.S. drones." (Sood A.K. & Enbody, 2014)

Wireless attacks are the most generic form of hacking. "Strategies to compromise a system's ability to be controlled by rightful owner include:

- Password Theft
- Wireshark
- Man-In-the-Middle Attacks
- Trojan Horse Virus
- Gain Scheduling Fuzzing,
- Digital Update Rate,
- Distributed Denial of Service,
- Buffer Overflow."(Rani, 2015)

Forms of MIM attacks are:

- URL manipulation
- Rogue Domain Name Server
- Address Resolution Protocol poisoning
- Duplication of Media Access Control
- False Emails" (Rani, 2015)

Gain Scheduling attack methods Sensor spoofing to cause mode confusion,

- Overriding gains through hacking,
- Infinite switching between gains, will cause loss of control,
- Causing Denial of Service (DOS) between controller gain block, and UAS controller block by overloading the on-board processor." (Kim, 2012)

Other possible Attacks on UAS Systems

- Autopilot Hardware Attack. (Kim, 2012)
- Wireless Attack. (Nichols R.-0., 2016)
- Control System Security. (Kim, 2012)
- Application Logic Security. (Nichols R.-0. , 20

Electronic Warfare (EW) – UAS Purview[25]

Warfare is conducted by adversaries who go to great pains to understand their enemy's intentions, strengths, weaknesses, and to minimize the threats to their own forces and territory.

The detection and interception of messages/data, combined with ground observations, provide an ability to observe troop movements and facilitate counteractions by opposing forces. UAS plays a significant role in these missions.

Communication Links for UAS are critical and must be secured

Modern warfare is conducted in a rich electromagnetic environment with radio communications and radar signals from many sources. ***Unmanned aircraft systems (UAS) / UAV / UUV / Drones are an integral part of modern warfare. UAS communications networks and links to ground stations are critical to the successful military use of UAS.*** Securing UAS links from EW attacks is a fundamental concern to military planners and civilian authorities. UAS BLOS communications require stable communications. Disrupting these communications links is a goal of hostile forces.

The key role of EW is to search these radio-frequency bands to cull information that can be used for intelligence analysis or by front-line operators. The information gathered may affect a tactical advantage on the battlefield, or in any stage before or after. (Moir I. a., 2006)

Adamy (2001) is correct when he suggests that the, "*key to understanding* EW *principles (particularly the* RF*) part is to understand radio propagation theory. Understanding propagation leads logically to understanding how they are intercepted, jammed or protected*." [26]

Main Contention

***It is the author's contention that UAS communication links are vulnerable and must be evaluated to protect US Unmanned Aircraft in the cyber or electronic domain. Further, those links may be electronically jammed, cyber-spoofed (especially navigational), or made ineffective with electronic or cyber or directed energy or acoustic interference.*[27]**

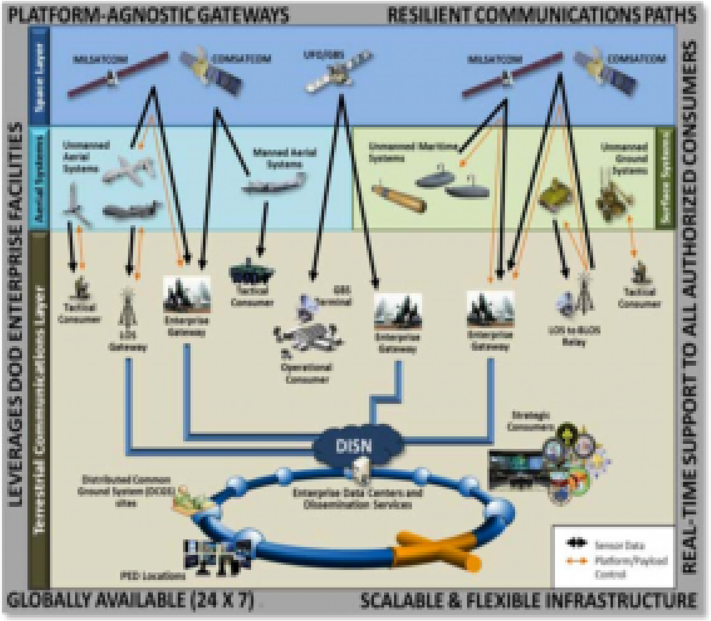
Communications Jamming -UAS

The purpose of communication is to move information from one location to another. All the following types of transmitted signals are communications:

- "Voice or non-voice communications (video or digital format)";

- “Command signals to control remotely located assets;”
- “Data returned from remotely located equipment”;
- “Location and motion of friendly or enemy assets (land, sea, or air);”
- UAS communications links from it ground station for control of the aircraft;
- UAS communications links from another aircraft or satellite affecting its flying characteristics;
- UAS communication signals (from any source) that affect the SAA / navigation / payload / waypoints;
- Computer-to-computer communications;
- Data links;
- Weapon-firing links;
- ISR data links;
- Cell phones.

Figure 9-16 High -Level C4 Operational Concept Incorporating UAS



High-Level C4 Infrastructure Operational Concept Graphic (OV-1)

Source: (DoD-03, 2015)

"The purpose of communications jamming is to prevent the transfer of information. Communications jamming requirements depend on the signal modulation (strength), the geometry of the link, and the transmitted power." (Adamy D. , 2009) *Another way to think of jamming is a method to "interfere with the enemy's use of the electromagnetic spectrum. Use of EMS involves the transmission of information from one point to another*". (Adamy D. , 2009)

"The basic technique of jamming is to add an interfering signal," along with the desired signal, into an enemy's receiver. "Jamming becomes effective when the interfering signal is strong enough to overwhelm the desired signal." This prevents the enemy from recovering the information from the desired signal. (Adamy D. , 2009) There are two possible methods for a successful jam: either the jamming signal is stronger than the desired "signal or the combined signals received have characteristics that prevented the processor from properly extracting the desired information." (Adamy D. , 2009) A simple case of jamming unintentionally is when your AM news station (listening in the car) becomes overwhelmed by junk music. You can hear the beginning of the interference as noise, then the junk signal is strong, then as the car moves out of the area, the AM news station regains its status. (Adamy D. , 2009)

The cardinal rule of jamming is that you jam the receiver, NOT the transmitter. (Adamy D. , 2001)

"The primary difference between radar and communication jamming is in the geometry. Whereas a typical radar has both the transmitter and the associated receiver at the same location, a communication link, because its job is to take information from one location to another, always has its receiver in a different location from that of the transmitter." (Adamy D. L., 2004)

Communication is often done using transceivers (each including both transmitter and receiver), but only the receiver at location B in the figure is jammed. If transceivers are in use and one desires to jam the link in the other direction, the jamming signal must reach location A." (Adamy D. L., 2004)

Another difference of radar jamming is that the radar signal makes a round trip to the target, so the received signal power is below the transmitted power by the fourth power of the distance (often stated as 40 log range). Since the jammer power is transmitted one way, it is only reduced by the square of distance." (Adamy D. L., 2004) Table 9-15 shows the Types of Jamming. (Adamy D. , 2001)

To be effective, the jammer must get its signal into the enemy's receiver – through the associated antenna, input filters, and processing gates. This depends on the signal strength the jammer transmits in the direction of the receiver and the distance and propagation conditions between the jammer and the receiver. (Adamy D. , 2009)

Table 9-15 Types of Jamming

Type of Jamming	Purpose
Communications jamming	Interferes with enemy ability to pass information over a communication link
Radar jamming	Causes radar to fail to acquire its target, to stop tracking target, or to output false information
Cover jamming	Reduces the quality of the desired signal so that it cannot be properly processed, or the info is lost / unrecoverable
Deceptive jamming	Causes radar to improperly process its return signal to indicate the correct range or angle to target
Decoy	Looks like the target more than the actual target; causes a guided weapon to attack the decoy rather than intended target

Source: (Adamy D. , 2001)

Jammer-to-Signal Ratio

The real test of jammer effectiveness is the effectiveness with which information flow is stopped. “A jammer interferes with communication by injecting an undesired signal into the target, receiver along with any desired signals that are being received.” (Adamy D. , 2009) “The obstructing signal must be strong enough that the receiver cannot recover the required information from the desired signals." The ratio of the jamming signal to the desired signal is known as the jamming–to-signal ratio **(J/S),** stated in dB.[28] Effective J/S depends on the transmitted modulation, but the Adamy formula works in general. (Adamy D. , 2001)

The formula for communication J/S is:

$$\mathbf{J / S = ERPJ - ERPS - LJ + LS + G\ RJ - G\ R \qquad Equation\ 9\text{-}6}$$

Where: **J/S** = the ratio of the jammer power to the desired signal power at the input to the receiver being jammed in dB

ERPJ the effective radiated power of the jammer in dBm

ERPS the effective radiated power of the desired signal transmitter, in dBm

LJ the propagation loss from jammer to receiver, in dBi[29]

LS The propagation loss from the desired signal transmitter, in dBm

GRJ the receiving antenna gain in the direction of the jammer, in dBi

GR The receiving antenna gain in the direction of the desired signal transmitter, in dBi." (Adamy D. , 2001)

Many UAS (especially UAV or sUAS) have a target receiving antenna with a 360-degree azimuth coverage. They use whips or monopoles. They are inexpensive. With a 360-degree antenna, the communications J/S equation simplifies to:

$$\mathbf{J / S = ERPJ - ERPS - LJ + LS \qquad Equation\ 9\text{-}7}$$

The receiving antenna has the same gain toward the jammer and the desired signal transmitter. The two gain terms cancel out. (Adamy D. , 2009)

A J /S calculation would indicate a successful jam when the desired signal fully compromised. (Adamy D. , 2001) The terminology is slightly different for the power terms (removing the “effective radiated” and using “power total” instead). The principle is still the same. (Adamy D. , 2009) See Appendix 9-3 for example J/S calculation.

US Army Field Manual FM 34-40-7 (23 Nov 1992) *Communications Jamming Handbook*, presents three alternative methods for calculating the jamming power required and distance to target. For the designer of an anti-UAS Drone gun, (Figure 9-17) which transmits a jammer signal to a UAS to overwhelm the desired ground station command signals, one needs the know the power and height of the drone. Since the drone is moving the jammer signal must radiate in such a manner that it covers a volume of space until target “UAS lock.”

Drone gun – Chinese alternative

A Chinese firm makes an anti-drone gun that costs about $35,000 USD and operates on 5.8 GHz and 2.4 GHz.[30] 80% of consumer drones operate on these frequencies. “The gun tricks the drone into thinking it has lost connection with its controller.” “RC signal lost” is flashed on drone screen – aircraft returning to home point.” The drone can be recovered intact. This gun has an operational limit of about 700 meters (0.43496 miles).

Figure 9-17 Drone Jammer Model KWT-FZQ.

Source: Tri-band Anti Drone Rifle KWT-FZQ/DG10-A

Manufacturer: Globaldroneuav.com https://globaldroneuav.com/Product/Police-drone-jammer-effective-drone-controller.html Appendix 9-1 details this anti-drone gun.[31]

Calculating the minimum of "amount of jammer power output required in watts" for this easy drone capture would be of interest. (Army, 1992) Appendix 9-4 of FM 34-70 (Army, 1992)gives a slightly different version of the Adamy equation 9-5:

$$P_j = P_t \text{ x } K \text{ x } (H_t / H_j)2 \text{ x } (D_j / D_t)N$$

Equation 9-8

Where:

P j **=** Minimum amount of jammer power output required , in watts

P t = Power output of the enemy drone, in watts

H j = Elevation of the jammer location above sea level, feet

H t = Elevation of enemy transmitter location above sea level, in feet

D j = Jammer location – to-target receiver location distance, in km

D t = Enemy transmitter location -to- target receiver location, in km

K = 2 for jamming frequency modulated receivers (jamming tuner accuracy)

N = Terrain and ground conductivity factors

5 = very rough terrain with poor ground conductivity

4 = Moderately rough terrain with fair to good ground conductivity

3 = Farmland terrain with good ground conductivity

2 = Level terrain with good ground conductivity

F = Frequency in MHz (Army, 1992)

"Note: The elevation of the jammer location and the enemy transmitter location does not include the height or length of the antenna above the ground. (Army, 1992) It is the location deviation above sea level.

Given the following parameters:

P j **=** Minimum amount of jammer power output required , in watts = (SOLVE)

P t = Power output of the enemy transmitter -to drone, in watts = 5 watts

H j = Elevation of the jammer location above sea level, feet, use 385m =.385 km

H t = Elevation of enemy transmitter location above sea level, in feet use 386m =.386 km

D j = Jammer location – to-target receiver location distance, in km = 700 m = 0.700 km

D t = Enemy transmitter location -to- target receiver location, in km = 372m = 0.372 km

K = 2 for jamming frequency modulated receivers (jamming tuner accuracy) = 2

N = Terrain and ground conductivity factor = Use 4 for moderate terrain with fair to good ground conductivity (Army, 1992)

F = Frequency in MHz, use 37.5 MHz in the band

Parameters were chosen so that the height ratio would drop-out and the distance would induce some ground conductivity effects consistent with the FM 34-40-7 examples.

Plugging the numbers and solving for P:

P j = 5 x 2 x (1)2 x **(0.7 / 0.372)4 = 10 x (1.88) 4 = 10 x 12.46 = 125 watts**

So, under these hypothetical conditions the jammer gun requires 125 watts (2 60-watt light bulbs) to take down the drone. Theoretically, if the jammer was using a log periodic array (LPA) the power could be cut in half to 62.5 watts (1 bulb). Now if this calculation is reasonable, the buyer is spending $35,000 USD to take down a small irritating drone (invasion of privacy) using a 60-watt bulb. A double-aught shotgun shell with a 12-gauge Remington and yellow shooter sunglasses will have the same effect (might even be more satisfying) for 1/100 the cost. The medium size drones present a more interesting case. More power is needed to lock on to the higher altitude UAS. The term of interest in the jamming equation from FM 34-40 -7 is the ratio of the distances to the fourth power (or second power for perfect terrain). That can have a major impact on jammer output power. (Army, 1992)

Radar Range Equation

Equation 9-9 is not the only place we see a term taken to the 4th power. The famous “Radar Range Equation *is dominated by the R4 factor in the denominator*. There is no corresponding function in the numerator of equation 9-9, with an exponent greater than unity. (Toomay, 1982) There is no magic bullet to achieve a high-performance system. If low cross section targets are to be engaged, a combination of high-power, high gain, large aperture, and low noise needs to be dictated." (Toomay, 1982)

The standard Radar Range Equation (RRE) is:

$$\mathbf{S / N = (P\ GTAr\sigma\ ) / [(4\pi)2\ R4\ KTS\ LS\ ]} \qquad \textbf{Equation 9-9}$$

Where:

S / N = is one pulse received signal to noise ratio, dB

P = Isotropic source of an electromagnetic pulse of peak power, Mw

GT = Gain of the transmit antenna, dB

Ar = Receive antenna effective area, m2

σ = Radar Cross Sectional Area, m2

R4 = *Energy density received at detected target range*, R, *nm*

K = Boltzmann's constant (Noise component)

TS = Measured noise temperature, Kelvin units above absolute zero

LS = Losses existing in the system (lumped together), dB

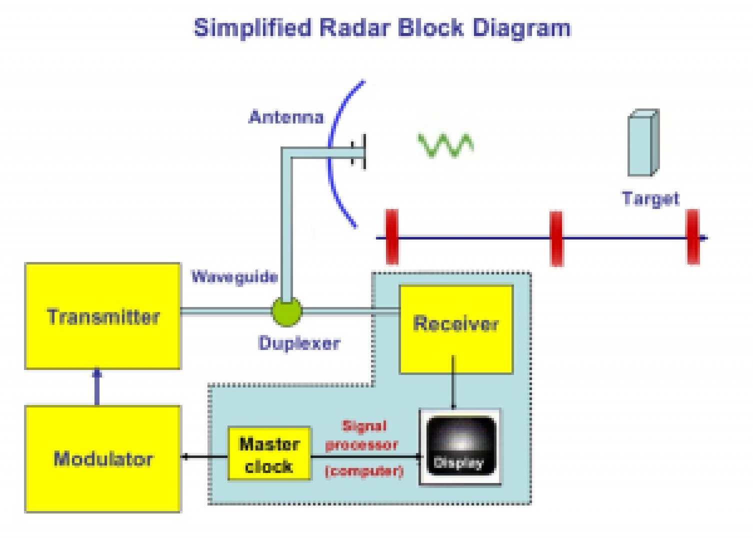
Inherent in equation 9-9, is the fact that the range of the radar to a "detected object can be calculated by: R = ct / 2, where c is the speed of light (3 x 108 m/s) x time , in sec. also, λ = c / f, where λ is the wavelength in Hz, and frequency, f is the cycles/second for the sinusoidal oscillator." (Toomay, 1982)

The point of this diversion into Radar history was that the performance of both the jamming equation and the radar range equation are affected by a power of 4th exponent. This affects equipment design, cost, effectiveness of detection or capture.

"The principles of a primitive radar are formed. Figure 9-18 diagrams its functions. A burst of electromagnetic energy, oscillating at a predetermined frequency is generated and radiates into free space from an antenna. A clock is started. The electromagnetic energy propagates outward at the speed of light, reradiating (scattering) from objects it encounters along its path. Part of the scattered energy returns to the radar (is received) and can be detected there because it imitates the frequency and duration of the transmitted pulse." (Toomay, 1982)

Figure 9-19 shows a simple surveillance RADAR. Compare this to 2019 version in Figure 9-20 which requires computer simulations to sort out the parameters.

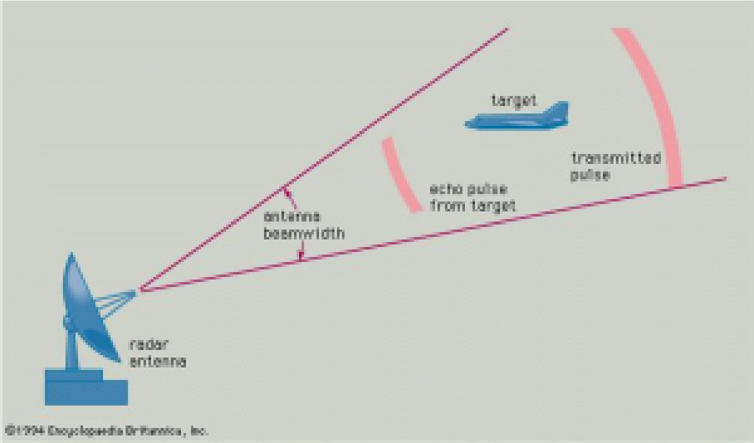
Figure 9-18 Simple Radar Block Diagram



Source: Simple Radar PPTX by Linkedin SlideShare (2018) https://www.slideshare.net/remotesensor1/radar-transmitter-4-1

A full derivation of all the terms, the radar spherical geometry and derivations of subset equations are in all legacy and modern radar texts and papers.

Figure 9-19 Simple Surveillance Radar



Source: Encyclopedia Britannica, (1994)

Complex RADAR / RES Simulations

Figure 9-20 shows that RADARS can be quite complex. They lend themselves to computer simulation to determine optimum parameters for a variety of systems.

Advancement of computer technologies and computer networks opens the possibilities of effective modeling of progressively sophisticated electronics. Nowadays, the time spent on the procedures of modeling complex *radio electronic systems* (RES) has been tangibly shortened. The shortened time spent on computation and steadily promoted adequacy of computer models to real systems and waveforms make it possible to transform the process of designing sophisticated systems (radars, air defense missile systems, their components and subsystems) based on modeling. Information circulates about real facts of full-scale designing of large-size aerial vehicles using adequate computer models.

Objects of modeling:

- RES with easily changeable structure and parameters;
- various signals circulating in radio electronic systems and in air;
- objects controlling such systems, for example, missiles in the process of guidance;
- influence of physical factors on quality and parameters of the processes described (ambient temperature, humidity, pressure, influence of the atmosphere on propagation of radio waves, etc.).

Computer modeling radically simplifies and saves time expenditure on developing complex RES, considerably alleviates the designer's qualification requirements, minimizes physical modeling and financial costs.

They are used for:

- optimization of the structure and parameters of newly developed radars, ADMS, EW assets;
- analysis of effectiveness of operation of Radars (ADMS), EW assets in complex jamming environments, facing the use of intensive maneuvers by the targets, etc.;
- researching the principal operational and technical characteristics of radars, ADMS, EW assets (detection envelope, kill envelope, tracking accuracy, etc.)

ADMS computer modeling systems are designed for:

- analysis of the processes of target detection and tracking in surveillance radars
- analysis of the processes of detection, reception of targeting, detection and acquisition of targets (lock-on) by tracking radars;
- analysis of the process of target lock-on and tracking by an air

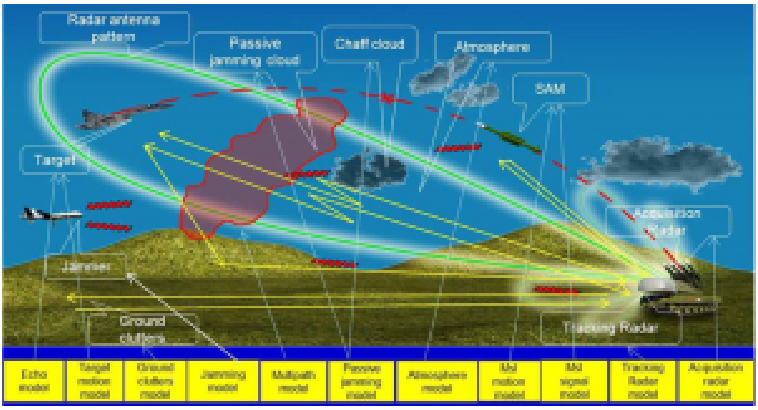
defense missile (SAM);

- analysis of the process of missile flight, collision with target, warhead detonation and effectiveness of the kill;
- selection and substantiation of the ADMS structure and parameters.

The modeling system comprises:

- models of the detection radar;
- models of the tracking radar;
- models of the missile motion;
- models of the missile signal;
- models of influence of the atmosphere on propagation of radio waves;
- models of motion of the target(s);
- models of target echoes;
- models of clutters induces by volume- and surface-distributed reflectors;
- models of jamming;
- models of multipath caused by influence of the Earth;
- models of the atmosphere.

Figure 9-20 Computer modeling of sophisticated radio electronic systems



Source: (radiotechnika – Republic of Belarus, 2019)

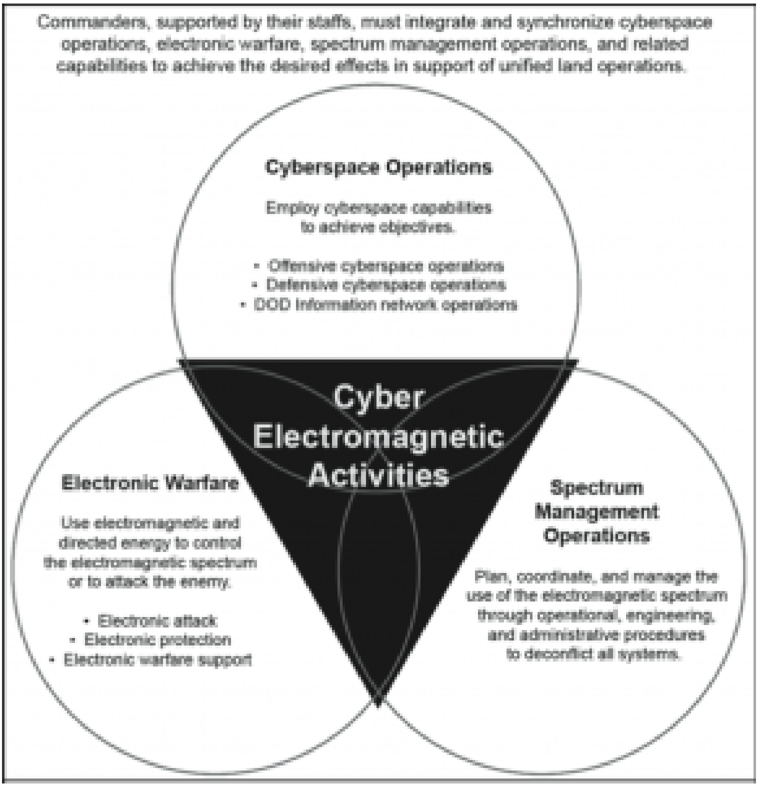
Conclusions

UAS are vulnerable to a variety of non-kinetic defenses, to wit: IO, cyber, EW, and as we shall see next chapter, acoustic. UAS are also vulnerable to DE weapons[32] UAS avionics is a prime target for both cyber and EW C-UAS defenses. SAA and SCADA systems are most susceptible to cyber-attacks.

Discussion Question

- There is a closely related science that intersects with EW and that is Cyber. There are distinct parallels and intersections between Cyber and EW. For instance, the sister of signal spreading techniques is encryption. See Figure 9-21 showing the intersection of Cyber, EW, and Spectrum Warfare designated as Cyber Electromagnetic Activities (CEA)[33] [34] [35] [36] The reader will research all major C-UAS intersections viewed in Figure 9-21 and provide examples.

Figure 9-21 Cyber Electromagnetic Activities



Commanders, supported by their staffs, must integrate and synchronize cyberspace operations, electronic warfare, spectrum management operations, and related capabilities to achieve the desired effects in support of unified land operations.

Employ cyberspace capabilities to achieve objectives.

- Offensive cyberspace operations
- Defensive cyberspace operations
- DOD Information network operations

Use electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy.

- Electronic attack
- Electronic protection
- Electronic warfare support

Plan, coordinate, and manage the use of the electromagnetic spectrum through operational, engineering, and administrative procedures to deconflict all systems.

Source: FM 3- 38 (2014)

References

Adamy, D. -0. (2015). *EW 104 EW against a New Generation of Threats*. Boston: Artech House.

Adamy, D. (2001). *EW 101 A First Course in Electronic Warfare*. Boston, MA: Artech House.

Adamy, D. (2009). *EW 103 Tactical Battlefield Communications Electronic Warfare.* Boston, MA: Artech House.

Adamy, D. L. (2004). *EW 102 A Second Course in Electronic Warfare.* Boston: Artech House.

Adamy, D.-9. (1998, Jan). Lesson 4: the basic link for all EW functions. (electronic warfare)(EW Reference & Source Guide). *Journal of Electronic Defense, Jan 1998 Issue.*

Administrator. (2015, June 15). *Standing Wave and Fundamental Frequency.* Retrieved from Electronics Hub: https://www.electronicshub.org/?s=fundamental+frequency

Alford, L. (2000). Cyber Warfare: Protecting Military Systems. *Acquisition Review Quarterly.*

Angelov, P. (2012). *Sense and avoid in UAS research and applications.* Hoboken: NJ.

Army, U. (1992, November 23). US Army Field Manual FM 34-40-7. *Communications Jamming Handbook.*

Austin, R. (2010). "*Design for Stealth*", *Unmanned Aircraft Systems* UAVS *Design Development and Deployment.* New York: John Wiley and Sons.

Barker, W. (2003, August). *SP 800-59 Guidelines for Identifying an Information System as a National Security System.* Retrieved from NIST: https://csrc.nist.gov/publications/detail/sp/800-59/final

Barnhart, R. K. (2012). *Introduction to Unmanned Aircraft Systems.* New York: CRC Press.

Beason, D. (2005). *The E-Bomb: How America's new directed energy weapons will change the way future wars will be fought.* Cambridge, MA: Da Capo Press.

Beaudoin, L. e. (2011). Potential Threats of UAS Swarms and the Countermeasures Need. ECIW.

Boutros, D. (2015, May 15). *US Navy War College.* Retrieved from Operational Protection from Unmanned Aerial Systems: http://www.dtic.mil/dtic/tr/fulltext/u2/a621067.pdf

Brenner, J. (2011). *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare.* New York: Pilgrim Press.

Burch, D. (2015). *RADAR for Mariners*. New York: McGraw-Hill.

C4ISystems. (2013). *basics-of-information-operations*. Retrieved from Blogspot: http://c4isys.blogspot.com/2013/11/basics-of-information-operations-24.html

Carter, A. (2012, May 24). *EEWeb*. Retrieved from The Sound Intensity: https://www.eeweb.com/profile/andrew-carter/articles/the-sound-intensity

Chairman, U. (2012, March 23). Countering Air and Missile Threats, final coordination, JP 3-01. CJCS.

Clothier, R. (2017, April 02). *The Smart Skies Project: Enabling Technologies for UAS Operations in Non-segregated Airspace*. Retrieved from QUT ePrints: http://eprints.qut.edu.au/40465/3/40465.pdf

Clothier, R. F. (2010). *The Smart Skies Project: Enabling technologies for future airspace.* . Clothier, R.A., Frousheger, D., Wilson, M., (2010). The Smart Skies Project: Enabling technologies for future airspace. Australian Research Center for Aerospace Automation, Commonwealth Scientific and Industrial Research Organization, Boeing Research an. Australian Research Center for Aerospace Automation, Commonwealth Scientific and Industrial Research Organization.

Clothier, R. R. (2011). The Smart Skies project. *IEEE Aerospace and Electronic Systems Magazine*.

DAU. (2018, July 2). *Cyber Tabletop Guidebook*. Retrieved from DOD / DAU: https://www.dau.mil/cop/test/_layouts/15/WopiFrame.aspx?sourcedoc=/cop/test/DAU%20Sponsored%20Documents/The%20DoD%20Cyber%20Table%20Top%20Guidebook%20v1.pdf&action=default&DefaultItemOpen=1

Defence, P. (2014, May 7). *China's Pterodactyl drone*. Retrieved from defence.pk: https://defence.pk/pdf/threads/saudi-arabia-signs-deal-for-chinas-pterodactyl-drone.312761/

DoD. (2018). *Dictionary of Military Terms*. Retrieved from JCS.Mil: http://www.jcs.mil/doctrine/dod_dictionary/

DoD-01. (2018). *JP 1-02*. Retrieved from Department of Defense

Dictionary of Military and Associated Terms: www.dtic.mil/ doctrine/new_pubs/jp1_02.pdf

DoD-02. (2018). *Information Operations (IO) in the United States*. Retrieved from JP 3-13 : http://www.dtic.mil/doctrine/new_pubs/ jp3_13.pdf

DoD-03. (2015). *Unmanned Systems Roadmap 2013 to 2038*. Retrieved from DTIC: http://www.dtic.mil/dtic/tr/fulltext/u2/ a592015.pdf

Drones, Q. S. (2017, July 11). *quadcopters-have-hit-the-sound-barrier/*. Retrieved from quadstardrones.com: https://quadstardrones.com/2017/07/11/quadcopters-have-hit-the-sound-barrier/

DTRA. (2019, October 18). Private Communication re Aviation Vulnerabilities. (Nichols, Interviewer) Retrieved from https://www.dtra.mil/

Editor. (2012, April 22). *RT Question More*. Retrieved from Iran starts cloning of American spy drone: https://www.rt.com/news/ iran-spy-drone-copy-667/

EIA. (2019, June 20). *The Strait of Hormuz is the world's most important oil transit chokepoint*. Retrieved from EIA – US Energy Information Administration: https://www.eia.gov/todayinenergy/ detail.php?id=39932

Entokey, a. G. (2019, May 16). *entokey.com/acoustics-and-sound-measurement/*. Retrieved from entokey.com/acoustics-and-sound-measurement/: https://entokey.com/ acoustics-and-sound-measurement/

Eshel, T. (2019, September 14). *AFRL to Test a Drone-Swarm Killer HPM*. Retrieved from Defense Update: https://defense-update.com/20190923_hpm.html

FAA. (2018, February 1). *Part 107 Rule for sUAS*. Retrieved from Fly under the Special Rule for Model Aircraft: https://www.faa.gov/ uas/getting_started/model_aircraft/

Filbert, F. &. (2014, (July – August). *Joint Counter Low, Slow, Small Unmanned Aircraft Systems Test. Fires PB644-14, no* 4. Washington: DoD.

Fitts, R. (1980). *The Strategy of Electromagnetic Conflict*. Los Altos, CA: Peninsula Publishing.

Foley, W. S. (March, 1979). Ancient Catapults. *Scientific American*, 240, 150.

Gallagher, S. (2019, September 16). *Missiles and drones that hit Saudi oil fields: Made in Iran, but fired by whom?* Retrieved from Arstechnica.com: https://arstechnica.com/tech-policy/2019/09/missiles-and-drones-that-hit-saudi-oil-fields-made-in-iran-but-fired-by-whom/

Garcia, M. (2006). *Vulnerability Assessment of Physical Protection Systems*. Albuquerque: Sandia National Laboratories,BH.

Gelfand. (2004). *"Physical Concepts", Hearing an Introduction to Psychological and Physiological Acoustics, 4th ed.* New York City.

Gelfand, S. A. (2009). *Essentials of Audiology, 3rd Edition*. Stuttgart, DE: Thieme.

Glasstone, S. &. (1977). The Effects of Nuclear Weapons, 3rd Edition. In S. &. Glasstone, *Chapter V, Figures* 5.20, 5.22 *&* 5.23. Washington, DC : UGPO.

Greenburg, H. (2015). *Hackers Remotely Kill a Jeep on the Highway—With Me in It*. Retrieved from Wired : https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Halsam, C. M.-S. (1982). *Small Arms and Cannons*. Oxford: Brassey's Publishers.

Hartman, K. a. (2013). The Vulnerability of UAVs to Cyber Attacks – An Approach to the Risk Assessment. *2013 5th International Conference on Cyber Conflict* . Tallin: NATO CCD COE Publications.

Horowitz, M. C. (2014). *Droning On: Explaining the Proliferation of Unmanned Aerial Vehicles*. University of Pennsylvania and Texas A&M Universities. University of Pennsylvania and Texas A&M Universities.

Howard, C. (2019, June 21). *What is the Strait of Hormuz, where Iran shot down US Navy drone?* Retrieved from Fox News: https://www.foxnews.com/world/whats-the-strait-of-hormuz-iran-shot-us-navy-drone

Hubbard, R. K. (1998). *Boater's Bowditch.* Camden, MA: International Marine.

Kania, E. (2017, July 6). Swarms at War: Chinese Advances in Swarm Intelligence. China Brief Volume: 17 Issue 9. *China Brief Volume*: 17 *Issue* 9.

Kaye, T. a. (2001, September 30). ACHIEVING INFORMATION DOMINANCE:. Retrieved from DODCCRP-Space and Naval Warfare Systems Center San Diego: http://www.dodccrp.org/events/2002_CCRTS/Tracks/pdf/026.PDF

Kilman, D. &. (2003). *Framework for SCADA Security Policy.* Albuquerque, NM: Sandia National Laboratories. Retrieved from Energy.gov: https://www.energy.gov/sites/prod/files/Framework%20for%20SCADA%20Security%20Policy.pdf

Kim, A. G. (2012, June). *Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles.* Retrieved from Infotech@Aerospace.com: https://www.researchgate.net/publication/268571174_Cyber_Attack_Vulnerabilities_Analysis_for_Unmanned_Aerial_Vehicles

Kirk, J. (2015, August 5). *sounds-can-knock-drones-sky.* Retrieved from www.computerworld.com.au/article/581231: https://www.computerworld.com.au/article/581231/sounds-can-knock-drones-sky/

Lister, T. (2019, September 16). *Attack is a game-changer in Gulf confrontation.* Retrieved from CNN: https://www.cnn.com/middleeast/live-news/saudi-oil-attack-dle-intl/h_3e647100fa720927c962d7643472b12d

Liteye. (2018, August 25). *AUDS.* Retrieved from Liteye Corporation: http://liteye.com/products/counter-uas/auds/

LRAD. (2019, May 189). *LRAD 450XL Datasheet.* Retrieved from LRADX: http://www.lradx.com/wp-context/uploads/2015/05/LRAD_datasheet_450XL.pdf

LRAD Corporation. (2019, October 18). *Product sheet LRADS 1000x.* Retrieved from LRAD Corporation : https://lradx.com/lrad_products/lrad-1000xi/

Marshall, D. M. (2016). *Introduction to Unmanned Aircraft Systems, 2nd Edition.* New York: CRC Press.

Merriam-Webster. (2019, May 17). Merriam-Webster Online Dictionary.

Merrick, K. (2016). Future Internet. 10.3390/*fi*8030034 *Review*, 8(3), p. 34.

Military & Aerospace Electronics. (2019, October 14). *Air Force researchers to test high-power microwave weapon to destroy or disable swarms of unmanned aircraft.* Retrieved from Military & Aerospace Electronics: https://www.militaryaerospace.com/unmanned/article/14068535/high-power-microwave-unmanned-aerial-vehicle-uav-swarms

Moir, I. &. (2006). *Military Avionics Systems.* New York City, NY: Wiley.

Moir, I. a. (2006). *Military Avionics Systems.* New York: Wiley Aerospace Series.

Monahan, K. (2004). *The Radar Book: Effective Navigation and Collision Avoidance.* Anacortes, WA: Fineedge Publications.

MORS. (2018). *Military Operations Research Society* . Retrieved from http://www.mors.org/meetings/oa_definition.htm

Myer, G. (2013, May-June). *Danger Close Definition.* Retrieved from US Army Magazine: www.benning.army.mil/infantry/magazine/issues/2013/May-June/Myer.html

NASA. (2018). *Unmanned Aircraft Systems* (UAS) *Integration in the National Airspace System* (NAS) *Project.* Retrieved from NASA: https://www.nasa.gov/feature/autonomous-systems

Naval Technology Team. (2019, June 11). *feature-the-top-10-maritime-patrol-aircraft/.* Retrieved from https://www.naval-technology.com: https://www.naval-technology.com/features/feature-the-top-10-maritime-patrol-aircraft/

Naval Technology Team. (2019, October 18). *MQ-4C Triton Broad Area Maritime Surveillance* (BAMS) UAS. Retrieved from Naval Technology: https://www.naval-technology.com/projects/mq-4c-triton-bams-uas-us/

Nichols, R. K. (1996). *Classical Cryptography Course, Volume I.* Laguna Hills, CA: Aegean Park Press.

Nichols, R. K. (2008, September 05). Counterintelligence & Sensitive Compartmented Information Facility . (SCIF) *Needs – Talking Points.*

Nichols, R. K. (2019, March 14). Hardening US Unmanned Systems Against Enemy Counter Measures. *7th Annual Unmanned Systems Summit*. Alexandria, VA, USA: PPTX presentation , self.

Nichols, R. K., Mumm, H. C., Lonstein, W. D., Ryan, J. J., Carter, C., & and Hood, J.-P. (2019). *Unmanned Aircraft Systems in the Cyber Domain, 2nd Edition.* Manhattan, KS: NPP eBooks. 27. Retrieved from www.newprairiepress.org/ebooks/27

Nichols, R. (Nov 28-30, 2006). Cyber Terrorism, Critical Infrastructure, & SCADA Presentation. In R. Nichols (Ed.), *Defense Threat Reduction Agency Conference.* Shirlington VA: Utica College, Utica NY.

Nichols, R.-0. (2016, March 29). NCIE UAS SAA Final Rev 4. *2016 INFOWARCON conference presentation April* 4-7, Nichols, R.K. et. al. (3-29-2016) Presentation to INFOWARCON April 4-7 on NCIE UAS SAA Final Rev 4, presented to 2016 INFOWARCON conference, Memphis TN. Available as PPTx presentation download from author or in CANVAS. Memphis, TN, USA: INFOWARCON16.

Nielsen, P. E. (2012). *Effects of Directed Energy Weapons.* Middletown, DE: CreateSpace Independent Publishing Platform.

NTSB. (2009, September 16). *National SCADA testbed Documents and Media.* Retrieved from National SCADA Testbed Fact Sheet: https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/NSTB_Fact_Sheet_FINAL_09-16-09.pdf

Osborn, K. (2019, October 15). *Swarm Hell: Can the U.S. Army Stop Hundreds of Drones Armed with Explosives?* Retrieved from National Interest: https://nationalinterest.org/blog/buzz/swarm-hell-can-us-army-stop-hundreds-drones-armed-explosives-88206

Pettit, R. (1982). *ECM and ECCM Techniques for Digital Communication Systems.* Belmont, CA: Lifetime Learning Publications .

Pierson. (2019, May 16). *tuning-fork-waves-sound.* Retrieved from airfreshener.club – Pierson Education: https://airfreshener.club/quotes/tuning-fork-waves-sound.html

radiotechnika – Republic of Belarus. (2019, October 20). *Computer modeling of sophisticated radio electronic systems.* Retrieved from http://radiotechnika.by/: http://radiotechnika.by/en/products/radar/computer_model_difficult_systems/

Randall K. Nichols, D. J. (2000). *Defending Your Digital Assets against Hackers, Crackers, Spies and Thieves.* New York: RSA Press.

Rani, C. M. (2015). Security of unmanned aerial vehicle systems against cyber-physical attacks. *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology.*

Raytheon. (2019, October 23). *Raytheon announces delivery of first laser counter-UAS system to U.S. Air Force.* Retrieved from Defense Blog: https://defence-blog.com/news/raytheon-announces-delivery-of-first-laser-counter-uas-system-to-u-s-air-force.html

Rogoway, T. (2018, September 5). *Global Hawk.* Retrieved from www.thedrive.com: https://www.thedrive.com/the-war-zone/23383/exclusive-u-s-air-force-rq-4-global-hawk-drone-crashed-off-spain-last-june

Said Emre Alper, Y. T. (December 2008). A Compact Angular Rate Sensor System Using a Fully Decoupled Silicon-on-Glass MEMS Gyroscope. JOURNAL OF MICROELECTROMECHANICAL SYSTEMS, VOL. 17, NO. 6.

Shapiro, J. (2006, February 14). *Slideplayer.com.* Retrieved from Cybersecurity: http://slideplayer.com/slide/4545982/

Sheena McKenzie, M. W. (2019, September 17). *Saudi attacks send oil prices soaring.* Retrieved from CNN: https://www.cnn.com/middleeast/live-news/saudi-oil-attack-dle-intl/h_1ab7e8469e98525f887c3a4e588dde8a

Singer, P. W. (2010, February 25). Will Foreign Drones One Day attack the US? . *Newsweek.*

Sood A.K. & Enbody, R. (2014, December 19). *https://www.georgetownjournalofinternau-s-military-defense-systems-the-anatomy-of-cyber-espionage-by-chinese-hackers.*

Retrieved from georgetownjournalofinternationalaffairs.org/online-edition: https://www.georgetownjournalofinternationalaffairs.org/online-edition/u-s-military-defense-systems-the-anatomy-of-cyber-espionage-by-chinese-hackers

Stratfor. (2019, October 20). *strait-of-hormuz-chokepoints.* Retrieved from https://www.stratfor.com: https://www.stratfor.com/sites/default/files/styles/wv_small/public/strait-of-hormuz-chokepoints.jpg?itok=xSgx6Hhi

Studios, D. D. (2017). Boaters Ref. USA.

Toomay, J. (1982). *RADAR for the Non – Specialist. London; Lifetime Learning Publications.* London: Lifetime Learning Publications.

TRS, S. (2018, July 10). *Tontechnic-Rechner-Sengpielaudio.* Retrieved from Tontechnic-Rechner-Sengpielaudio Calculator: www.sengspielaudio.com/calculator-wavelength.htm

Uni-wuppertal. (2019, May 15). *Inverse Square Law, General.* Retrieved from hydrogen.physik.uni-wuppertal.de/hyperphysics/: http://hydrogen.physik.uni-wuppertal.de/hyperphysics/hyperphysics/hbase/forces/isq.html

Usenix.org. (2019, 6 9). *MEMS, Drones, & Sound Sourcing.* Retrieved from Usenix.org: www.usenix.org

Vernard Foley, G. P. (January, 1985). The Crossbow. *Scientific American*, 252, 104.

Weise, E. (2017, August 23). *could-hackers-behind-u-s-navy-collisions.* Retrieved from USATODAY: https://www.ruidosonews.com/story/tech/news/2017/08/23/could-hackers-behind-u-s-navy-collisions/594107001/

Wikipedia. (2018, August 26). *Human Hearing Range.* Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Hearing_range

Wiley, R. G. (1993). *Electronic Intelligence: The Analysis of Radar Signals, 2nd ed.* Norwood, MA: Artech House.

Wilson, M. (2012). The Use of Low-Cost Mobile Radar Systems for Small UAS Sense and Avoid. *Sense and Avoid in UAS Research and Applications.*

Yan. (2017, December 23). *China's commercial drone market to* *top 9 bln USD by 2020.* Retrieved from Xinhuanet: http://www.xinhuanet.com/english/2017-12/23/c_136847826.htm

Yu, X. &. (2015). Sense and avoid technologies with applications to unmanned aircraft systems: Review and prospects. *Progress in Aerospace Sciences*, 74, 152-166.

Yunmonk Son, H. S. (2015, August 12-14). Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors. *Proc. 24th Usenix Security Symposium.* Washington, DC: USENIX. Retrieved from https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/son

Zaharia, M. D. (2012). *Discretized Streams: An Efficient and Fault-Tolerant Model for.* Retrieved from UNIX Org: https://www.usenix.org/system/files/conference/hotcloud12/hotcloud12-final28.pdf

Zwijnwenburg, W. (2014, October 8). *ZwijnwenbDrone-tocracy? Mapping the Proliferation of Unmanned Systems.* Retrieved from Sustainable Security.org.

Appendix 9-1 Tri-band Anti Drone Rifle KWT-FZQ/DG10-A[37]

Source: (LRAD Corporation, 2019)

Manufacturer: Globaldroneuav.com https://globaldroneuav.com/Product/Police-drone-jammer-effective-drone-controller.html

Functions and features

1. Full range cover within three frequency section and high-power transmission helps to achieve the ideal effects.
2. Fast trigger, easy use and daughter switch design make control more ease and comfort.
3. Dual lithium batteries for power supply last work time longer.

4. The strong internal line connector and external fuses port make the whole vehicle and component parts fastened securely.
5. All aluminum alloy case body design and glass fiber material for antenna cover make its appearance lighter and faster.

ce dimension ：（mm）L×W×H；1323mm×403mm×341 mm

Weight（Kg）:4.7kg±0.2kg（mainframe + battery）

0.6kg±0.1kg（sighting telescope）

Source: Tri-band Anti Drone Rifle KWT-FZQ/DG10-A

Manufacturer: Globaldroneuav.com https://globaldroneuav.com/Product/Police-drone-jammer-effective-drone-controller.html

Appearance dimension ：（mm）L×W×H；1323mm×403mm×341 mm

Weight（Kg）:4.7kg±0.2kg（mainframe + battery）

0.6kg±0.1kg（sighting telescope）

Source: Tri-band Anti Drone Rifle KWT-FZQ/DG10-A

Manufacturer: Globaldroneuav.com https://globaldroneuav.com/Product/Police-drone-jammer-effective-drone-controller.html

Technical parameters

SN	Parameter name：	Parameter index record：
1	Power supply-	Work voltage V
2	Work current A	≤9A@DC14.8V
3	Work time	≥1.5h
4	Radio Frequency	**Work frequency range MHz**
5	Output power dBm	40dBm@1550～1620MHz（±1dB）
6	37dBm@2400～2483MHz（±1dB）	
7	37dBm@5725～5852MHz（±1dB）	
8	Out of band rejection	＜-36dBm@30～1000MHz ＜-30dBm@≥1GHz
9	Specification &environment	Weight
10	Dimension	1323mm×403mm×341 mm, with battery ar
11	Work environment humidity	≥95%
12	Work temperature	-25℃～55℃
13	Storage temperature	-40℃～70℃

Appearance dimension：（mm）L×W×H；1323mm×403mm×341 mm

Weight（Kg）:4.7kg±0.2kg（mainframe + battery）

0.6kg±0.1kg（sighting telescope）

Source: Tri-band Anti Drone Rifle KWT-FZQ/DG10-A

Manufacturer: Globaldroneuav.com https://globaldroneuav.com/Product/Police-drone-jammer-effective-drone-controller.html

Appendix 9-2 MQ-4C Triton design features

The MQ-4C Triton is based on the RQ-4N, a maritime variant of the RQ-4B Global Hawk. The main aluminum fuselage is of semi-monocoque construction, while the V-tail, engine nacelle and aft fuselage are made of composite materials. The forward fuselage is strengthened for housing sensors and the radomes are provided with lightning protection, and hail and bird-strike resistance.

The UAS has a length of 14.5m, height of 4.7m and a wingspan of 39.9m. It can hold a maximum internal payload of 1,452kg and external payload of 1,089kg.

Mission capabilities of MQ-4C Triton BAMS UAS

The MQ-4C is a high-altitude, long-endurance UAS, suitable for conducting continuous sustained operations over an area of interest at long ranges. It relays maritime intelligence, surveillance and reconnaissance (ISR) information directly to the maritime commander.

The UAS can be deployed in a range of missions such as maritime surveillance, battle damage assessment, port surveillance and communication relay. It will also support other units of naval aviation to conduct maritime interdiction, anti-surface warfare (ASuW), battle-space management and targeting missions.

The MQ-4C is capable of providing persistent maritime surveillance and reconnaissance coverage of wide oceanographic and littoral zones at a mission radius of 2,000 nautical miles. The UAS can fly 24 hours a day, seven days a week with 80% effective time on station (ETOS).

Payloads of Northrop's unmanned system

The payload is composed 360° field of regard (FOR) sensors including multifunction active sensor (MFAS) electronically steered array radar, electro-optical / infrared (EO/IR) sensor, automatic identification system (AIS) receiver and electronic support measures (ESM). The payload also includes communications relay equipment and Link-16.

The MTS-B multispectral targeting system performs auto-target tracking and produces high-resolution imagery at multiple field-of-views and full motion video. The AN/ZLQ-1 ESM uses specific emitter identification (SEI) to track and detect emitters of interest.

Engine and performance of the US's UAS.

MQ-4C Triton is powered by a Rolls-Royce AE3007H turbofan engine. It is an advance variant of the AE3007 engine in service with the Citation X and the Embraer Regional Jet. The engine generates a thrust of 8,500lb.

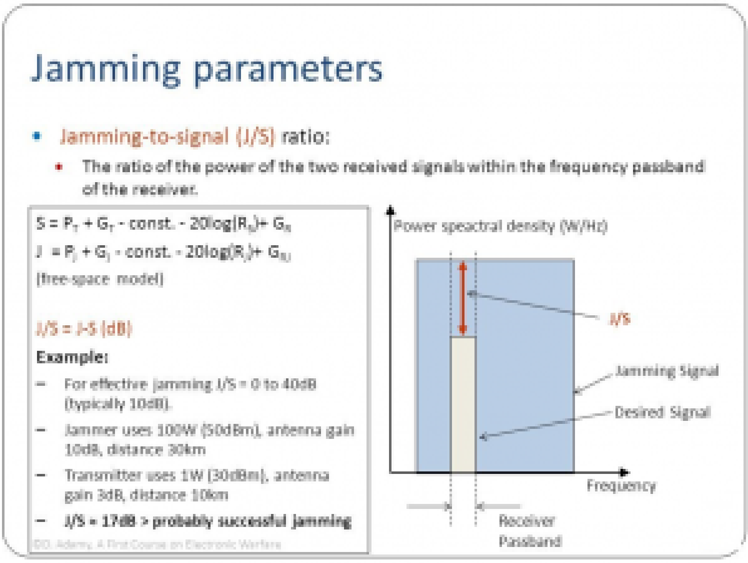
The UAS can fly at a maximum altitude of 60,000ft. It has a gross take-off weight of 14,628kg. Its maximum unrefueled range is 9,950 nautical miles and endurance is 30 hours. The maximum speed is 357mph.

Ground control station

The UAS is operated from ground stations manned by a four-man crew, including an air vehicle operator, a mission commander and two sensor operators. The UAS can fly 24 hours a day, seven days a week with 80% effective time on station (ETOS).

The ground station includes launch and recovery element (LRE) and a mission control element (MCE). The MCE performs mission planning, launch and recovery, image processing and communications monitoring. The LRE controls related ground support equipment as well as landing and take-off operations. (Naval Technology Team, 2019)

Appendix 9-3: J/S Calculation Example



Jamming parameters

- Jamming-to-signal (J/S) ratio:
  - The ratio of the power of the two received signals within the frequency passband of the receiver.

$S = P_T + G_T$ - const. - $20\log(R_S) + G_R$

$J = P_J + G_J$ - const. - $20\log(R_J) + G_{RJ}$

(free-space model)

J/S = J-S (dB)

Example:

- For effective jamming J/S = 0 to 40dB (typically 10dB).
- Jammer uses 100W (50dBm), antenna gain 10dB, distance 30km
- Transmitter uses 1W (30dBm), antenna gain 3dB, distance 10km
- **J/S = 17dB > probably successful jamming**

DD. Adamy, A First Course on Electronic Warfare

Source: Cagalj, M. (2014) & Adamy, D, (2001) EW 101

Quote from manufacturer Globaldroneuav.com: (Adamy D. , 2009)

Endnotes

[1] **FIRES** definition (US DoD – JP 3-0) the use of weapon systems to create a specific lethal or nonlethal effect on a target.

[2] **Danger Close** Definition www.benning.army.mil/infantry/magazine/issues/2013/May-June/Myer.html Nov 14, 2013 – 1) danger close is included in the “method-of-engagement” line of a call-for-fire request to indicate that friendly forces are close to the target. ... Danger close is a term that is exclusive from risk estimate distance (RED) although the RED for 0.1 percent PI is used to define danger close for aircraft delivery. *Pi* = Probability of incapacitation. 2) Definition of “danger close” (US DoD) In close air support, artillery, mortar, and naval gunfire support fires, it is the

term included in the method of engagement segment of a call for fire which indicates that friendly forces are within close proximity of the target.

[3] See Team or SWARM formats, Tables 3-1 and 3-2 in (Nichols, et al., 2019)

[4] (Moir I. &., 2006) provides data on all the listed military avionics systems, including role description, key performance characteristics, profile, crew component, systems architecture, major components (avionics, communications, mission systems and weapons), and pictures of aircraft types in the role. The purpose of this section is to detail one role, the Military Maritime Role (MPA) to show that UASs can perform the role in support of the author's opening contention that manned (piloted) aircraft systems can be replaced by unmanned (no crew) aircraft systems for a variety of the key performance characteristics for less investment and reduced liability to US forces. Every role listed reasonable fits within the author's contention, again presented without any intended disrespect to our US military forces.

[5] Authors conclusions.

[6] These are legacy definitions from (Moir I. &., 2006) and are included for functional purposes. Chapter 14 of (Nichols, et al., 2019) update these definitions to USA and NATO categories. ES = Electronic Warfare support (old ESM); EA = Electronic attack – which is the old ECM but also includes ASW and Directed Energy (DE) weapons; and EP = Electronic Protection is the old ECCM.

[7] Again, the chosen material for Table 9-2 has legacy implications by design. Many of the included systems have been significantly upgraded and, in some cases, classified as to performance. All the system names are found in the Abbreviations List. MPA represents a huge category in tasks and is a primary user of acoustic data.

[8] The EW, CW and Acoustic Countermeasures discussions are

updated from Chapter 3: *Understanding Hostile Use and Cyber-Vulnerabilities of* UAS: *Components, Autonomy v Automation, Sensors*, SAA, SCADA *and Cyber Attack Taxonomy*;” Chapter 8:” *Designing* UAS *Systems for Stealth*;” Chapter 14: *Exposing* UAS *Vulnerabilities via* EW *and Countering with* LPI *Signals*;” and Chapter 19: *Audiology, Acoustic Countermeasures against* SWARMS *and Building* IFF *Libraries*.” (Nichols, et al., 2019)

[9] The EW, CW and Acoustical sections are updated / illustrated from our previous textbook (Nichols, et al., 2019)

[10] In (Nichols, et al., 2019), we studied the EMS, datalinks and cyber-vulnerabilities of UAS. Here we consider electronic warfare as a method of overwhelming, destroying, or controlling the information, transmitted by communication datalinks, to alter the mission of the UAS deployment. Chapter 14: *Exposing* UAS *Vulnerabilities via* EW *and Countering with* LPI *Signals*;” in (Nichols, et al., 2019) and (Moir I. &., 2006) in their Chapter 6 *Electronic Warfare* give reasonable discussions of the fundamentals, technologies, missions and key players for EW. They by no means cover the field however, they serve as a starting point on the long road of EW discoveries.

[11] Nuclear weapons may be characterized in terms of megatons, bullets in terms of muzzle velocity, and particle beams in terms of amperes of current. The commonality is amount of energy absorbed by the target which leads to similar levels of damage achieved at similar levels of energy deposited. (Nielsen, 2012)

[12] Joules is the preferred unit for DE. A joule is approximately the energy required to lift a gallon of milk a distance of three feet or 1/50,000 of the energy needed to brew a cup of 6 oz coffee. For us old-time engineers for reference points: 1 BTU = 1055 J; 1 Calorie = 4.19 J; 1kw hr = 3.6 x 106 J; 1eV = 1.6 x 10-19 J and 1 erg = 10-7 J.

[13] For this example, C= 4.2 (J/gm x o C) and ice cube = 50 gm, Ti=

-10 (o C), Tm= 0 (o C). (Lm) for water = 334 Joules / gm. So, 16,700 additional Joules are necessary to melt the ice cube of 50gm. Tv = vaporization temperature, (100 o C),

[14] Aka called "Fluence" Units of fluence are 1 J/cm2 =104 J/m2 and 1 W /cm2 = 104 W/ m2

[15] The effect of area can be better understood by looking at the energy delivery from the two atom bombs delivered against Hiroshima and Nagasaki. (Glasstone, 1977) Both weapons had yields of about 20kT, they released about 8 x 1013 Joules of energy. At a range of z of 0.1 mile (= 1.6 x 104 cm), the energy density would be approximately 8 x 1013 Joules / 4πz2 = 2.5 x 104 J /cm2 or fluence. So, when spreading of the blast energy is accounted for, the result is consistent with other weapon types. Our damage energy density sufficiency is 10,000 J / cm2 or fluence.

[16] Thermal conductivity varies for materials. Copper (good conductor) = 4.2 J/cm sec deg whereas Air (thermal insulator) has a value of 0.00042 J /cm sec deg. (Nielsen, 2012) Thermal conductivity is not just a simple single order equation. Other effects are observed changes in regional temperatures, effects of thermal conductivity, thermal diffusion, / diffusivity, temperature propagation v time.

[17] Black Body radiation is a mathematical ideal surface that absorbs all radiation incident upon it. In equilibrium it would radiate more energy than any other object. (Nielsen, 2012)

[19] Definitions

Electronic warfare (EW) is defined as the art and science of preserving the use of the electromagnetic spectrum (EMS) for friendly use while denying its use by the enemy. (Adamy D. , 2001) The EMS is from DC to light and beyond. EW covers the full radio frequency spectrum, the infrared spectrum, and the ultraviolet spectrum.

Nichols (2000) defines Cybersecurity in terms of cyber-conflict. (Nichols R. K., 2008) Alford (2000) authored effective definitions for the DoD. These will illustrate the bigger picture of Information Operations (IO) and the subset known as Electronic Warfare (EW).

Cybersecurity (in the context of Cyber conflict) is defined as, "the broad tree of investigation and practice devoted to cybercrimes, Computer Forensics (CF), Information Assurance (IA), Information Security (INFOSEC), Communications Security (COMSEC), and especially Cyber Counterintelligence (CCI)." (Nichols R. K., 2008)

"Cyber Warfare (CW / CyW). Any act intended to compel an opponent to fulfill our national will, executed against the software controlling processes within an opponent's system. CyW

includes the following modes of cyber-attack; cyber infiltration, cyber manipulation,

Cyber assault, and cyber raid." (DAU, 2018) (DAU, 2018)

"Cyber Infiltration (CI / CyI). Penetration of the defenses of a software-controlled system such

that the system can be compromised, disabled, manipulated, assaulted, or raided." (DAU, 2018) (DoD, 2018)

"Cyber Manipulation (CM / CyM). Following infiltration, the control of a system via its software which leaves the system intact, then uses the capabilities of the system to do damage.

For example, using an electric utility's software to turn off power." (DAU, 2018) (DoD, 2018)

"Cyber Assault (CA / CyA). Following infiltration, the destruction of software and data in the system, or attack that compromises system capabilities." (Alford, 2000) Includes viruses and system overloads via e-mail (e-mail overflow)." (DoD, 2018; DoD, 2018)

"Cyber Raid (CR / CyR). Following infiltration, the manipulation or acquisition of data within the system, which leaves the system intact, results in transfer, destruction, or alteration of

data. For example, stealing e-mail or taking password lists from a mail server." (DAU, 2018) (DoD, 2018)

Cyber-Attack. See CyI, CyM, CyA, or CyR.

Cybercrime (CC / CyC). Cyber-attacks without the intent to affect national security or to further operations against national security." (Alford, 2000)

"C4ISR. The concept of Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance." (DoD, 2018) (Kaye, 2001) See Figure 9-15 (C4ISystems, 2013)

Electronic Warfare (EW) is defined as the art and science of preserving the use of the Electromagnetic Spectrum (EMS) for friendly use, while denying its use by the enemy. (Adamy D. , 2001)

"Information Assurance (IA). Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities." (Barker, 2003) (Kaye, 2001)

"Information Operations (IO). The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision-making process, information, and information systems while protecting our own." (Barker, 2003) (Kaye, 2001)

"Information Superiority (IS). The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. A newer form of this is that: degree of dominance in the information domain which permits the conduct of operations without effective opposition." (Alford, 2000) (Kaye, 2001)

"Information Warfare (IW). Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary. IW is any action to Deny, Exploit, Corrupt or Destroy the enemy's information and its functions, protecting those actions and exploiting our own military information functions." (Alford, 2000) (Kaye, 2001)

"Intentional Cyber Warfare Attack (ICWA). any attack through cyber-means to intentionally affect national security (cyber warfare) or to further operations against national security.

Includes cyber-attacks by unintentional actors prompted by intentional actors. (Also

see "unintentional cyber warfare attack.") IA can be equated to warfare; it is national policy at the level of warfare. Unintentional Attack(UA) is basically crime. UA may be committed by a bungling hacker or a professional cybercriminal, but the intent is self-serving and not to further a national objective. This does not mean unintentional attacks cannot affect policy or have devastating effects.

Intentional Cyber Actors (I-actors). Individuals intentionally prosecuting cyber warfare (cyber

operators, cyber troops, cyber warriors, cyber forces)." (Alford, 2000)

"Network Centric Operations (NCO). NCO involves the development and employment of mission critical packages that are the embodiment of the tenets of Network Centric Warfare (NCW) in operations across the full mission spectrum. These tenets state that a robustly networked force improves information sharing and collaboration, which enhances the quality of information, the quality of awareness, and improves shared situational awareness. This results in enhanced collaboration and enables self-synchronization improving sustainability and increasing speed of command, which ultimately result in dramatically increased mission effectiveness. (Kaye, 2001)" (MORS, 2018) (Kaye, 2001)

OPSEC. (Operations Security) (DoD-01, 2018) "Determining what information is publicly available in the normal course of operations that can be used by a competitor or enemy to its advantage. OPSEC is a common military practice that is also applied to civilian projects such as the development of new products and technologies.

OPSEC – The Official Definition

(From JP 1-02, Department of Defense Dictionary of Military and Associated Terms, www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.) Operations Security (OPSEC) is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to:

1. Identify those operations that can be observed by adversary intelligence systems,

2. Determine what indicators adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries, and

3. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation." (DoD-01, 2018)

"Psychological Operations (PO) Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign entities." (Alford, 2000) (Kaye, 2001)

"Psychological Warfare (PW / PSYWAR) The planned use of propaganda and other psychological actions to influence the opinions, emotions, attitudes and behavior of hostile foreign groups." (Kaye, 2001)

"Unintentional Cyber Actors (U-actors). Individuals who unintentionally attack, but affect

national security and are largely unaware of the international ramifications of their actions.

Unintentional actors may be influenced by I-actors, but are unaware they are being

manipulated to participate in cyber operations. U-actors include anyone who commits

CyI, CyM, CyA, and CyR without the intent to affect national security, or to further

operations against national security. This group also includes individuals involved in

CyC, journalists, and industrial spies. The threat of journalists and industrial spies

against systems including unintentional attacks caused by their CyI efforts should be considered high.

Unintentional Cyber Warfare Attack (UCWA/ UA). Any attack through cyber-means, without the intent to affect national security (cybercrime)." (Alford, 2000)

[21] Skyjack Drone hack. Drone that flies around seeking Seeks wireless signal of any other drone in area. Forcefully disconnects wireless connection of true owner of target drone. Authenticates with target drone pretending to be its owner. Feeds commands to it and all other zombie drones SkyJack primarily a Perl application which runs off a Linux. Detect drones by seeking out wireless connections from MAC addresses.

[22] Aircrack-ng© To put wireless device into monitor mode to find drones and drone owners. De-authenticate true owner of drone. Once de-authenticated, connect as drone waiting for owner to reconnect.

[23] Snoopy is Software that can hack into Wi-Fi and steal data – attached to drones. Comprised of various existing technologies. Uses Distributed tracking and profiling framework. Runs client-side code on any device that has support for wireless monitor mode. Collects probe-request and uploads to a central server. Exploits handsets looking for wireless signal. Most leave their device Wi-Fi setting on Spoof network available to Wi-Fi searchers to use. Once connected to rogue network, data is stolen. Differs from other rogue access points in way data is routed. Traffic is routed via an OpenVPN connection to a central server. Able to observe traffic from all drones in field at one point. Traffic manipulation only done on server. Allows basic data exploration and mapping.

[24] Special thanks and credit to my co-author Dr. Julie J.C.H. Ryan and Dan J. Ryan, Esq who were pioneers in the field information security and its associated risks. (Randall K. Nichols, 2000)

[25] Adamy sets the standards for EW instruction. Moir summarizes the topic with respect to military operations, UAS, and military avionics systems. (Moir I. a., 2006) (Toomay, 1982) and (Burch, 2015) bring Radar to the non-specialist reader. A Google search on the key = RADAR yields 296,000,000 results (0.49 seconds). There is substantial material on the subject. The challenge is determining the UAS applicability.

[26] Legacy EW definitions- EW was classically divided into: (Adamy D. , 2001)

ESM – Electromagnetic Support Measures – the receiving part of EW;

ECM – Electromagnetic Countermeasures – jamming, chaff, flares used to interfere with operations of radars, military communications and heat-seeking weapons;

ECCM -Electronic Counter-Counter Measures – measures taken in design or operation of radars or communications systems to counter the effects of ECM.

Not included in the EW definitions were Anti-radiation Weapons (ARW) and Directed Energy Weapons (DEW).

USA and NATO have updated these categories:

ES – Electronic warfare Support (old ESM)

EA – Electronic Attack – which is the old ECM but also includes ASW and DE weapons;

EP – Electronic Protection – (old ECCM) (Adamy D. , 2001)

ES is different from Signal Intelligence (SIGINT). SIGINT is made up of Communications Intelligence (COMINT) and Electronic Intelligence (ELINT). All these fields involve the receiving of enemy transmissions. (Adamy D. , 2001)

COMINT receives enemy communications signals to extract intelligence.

ELINT uses enemy non-communications signals for determining the enemy’s EMS signature so that countermeasures can be developed. ELINT systems collect substantial data over large periods to support detailed analysis.

ES/ESM collects enemy signals, either communication or non-communication, with the object to do something immediately about those signals or the weapons associated with those signals. The received signals might be jammed, or the information sent to a lethal responder. Received signals can be used to type and locate the enemy's transmitter, locate enemy forces, weapons, distribution, and electronic capability. (Adamy D. , 2001)

[27] This a main theme of this book. In addition, this section started off with the answer – Low Probability of Intercept (LPI) as a countermeasure to reduce risk of EA to the UAS missions. (Adamy D. , 2009)

[28] Any number expressed in dB is logarithmic base 10. dB mathematical concepts with examples may be found in Chapter 2 of Adamy, D., (2001) EW 101. A value expressed in dB is a ratio converted to logarithmic form. A linear number is converted to dB form by the formula: N(dB) = 10 log (base 10) [N]. dB values are converted back to linear format by the formula N = 10 **N (dB/10). dB numbers are usually reference to some standard with constant value. A common example is signal strength expressed in dBm = dB value of Power / 1 milliwatt, used to describe signal strength. For example, 4 watts power level = 4000 mw. Divide by 1 mw standard then convert 4000 to dB = 10 log (4000) = 36.02 dBm. dB forms are used because of the wide range of numbers and orders of magnitude for the EMS.

[29] dBi = dB value of antenna gain relative to the gain of an isotropic antenna (perfect antenna). 0 dBi is the gain of an omnidirectional (isotropic) antenna.

[30] Video Report, Quote by Amy Hu. Data Expert Technology LTD, https://www.youtube.com/watch?v=o057LmNGsJA DLA 07312018

[31] *Source*: Tri-band Anti Drone Rifle KWT-FZQ/DG10-A
Manufacturer: Globaldroneuav.com https://globaldroneuav.com/Product/Police-drone-jammer-effective-drone-controller.html

[32] DE weapons are technically kinetic weapons with non-kinetic interfaces. The author has included them because they are very cool and represent a huge amount of classified advanced research for C-UAS purposes.

[33] FM 3-38 (2014)

[34] Askin, O., Irmak, R, and Avseyer, M. (14 May 2015)

[35] CEA aka Cyber electronic warfare

[36] Student will research CEA and its parallels to EW (start with FM 3 – 38 Cyber Electromagnetic Activities in CANVAS or use Google to find the free PDF) How do these intersections support both friendly and hostile actions on UAS systems in all classes? Develop a PowerPoint presentation with your answers for class submission. Look for tools like cyber offensive weapons against key UAS systems and cyber defensive weapons/countermeasures that can be used to thwart the cyber weapons that you have found in Open Source literature (Non- CLASSIFIED). Try to develop a taxonomy around your findings.

PART III

SECTION 3: COUNTER C-UAS

Chapter 10: When the Other Side Fights Back - Cyberwarfare, Directed Energy Weapons, Acoustics,Integrating C-UAS into Planning

R. K. NICHOLS

Student Objectives

All the C-UAS systems described in this chapter are known by USA and friendly forces and, in general, by other countries (China, Russia, terror states under CNKI, etc.) So, the object of this chapter is to understand the lethal use of the EMS by:

- Study four classic direct energy weapons (DEW, Laser, Microwave, Particle Beams) technologies
- Learn about acoustic countermeasures and their effects on MEMS
- Sample real-world advanced UAS systems deployed in the field. These UAS are able to fight back via EW and have both kinetic and non-kinetic countermeasures against friendly C-UAS systems.

What Happens When the Enemy Decides to Fight Back?

There needs to be plans /policies in place. The UK Government has developed one and presented it to Parliament in October 2019. In the UK Counter-Unmanned Aircraft Strategy we read the following objectives: (Norbiton, Oct 2019)

1 The objective of the strategy is to *reduce risk posed by the highest-harm illegal use of drones*,

2 The government's strategy is to mitigate the malicious, criminal use of drones, including threats to the UK's national security and critical infrastructure,

3 To develop a comprehensive understanding of the evolving risks posed by the malicious and illegal use of drones,

4 To take a full spectrum approach to deter, detect and disrupt the misuse of drones

5 To build strong relationships with industry to ensure products meet the highest security standards

6 To empower police and other operational responders through access to counter-drone capabilities and effective legislation, training and guidance.[1]

(Norbiton, Oct 2019) document considers highest-harm risks resulting from malicious use of drones:

- Facilitating terrorist attacks
- Facilitating crime, especially in the UK prisons
- Disrupting Critical National Infrastructure (CNI)
- Potential use by hostile state actors

The two departments that are responsible for strategy and policy associated with the illegal use of drones are Department of Transport(DT) (responsible for the safe and lawful use of drones within UK airspace) and the Home Office (HO) which has overall responsibility for domestic counter-drone activity as part of its wider security remit. (Norbiton, Oct 2019)

First Actions

Following the Gatwick drone sightings in December 2018, the DT and the Center for Protection of National Infrastructure (CPNI) put in place policies to reduce the vulnerability of sensitive sites to drone incursions:

- Guidance for CNI operators, including airports on how to assess drone risks and vulnerabilities, and training on available counter -drone technologies.
- Standardized signage to clearly designate areas where drone flights are prohibited, and providing information to the public on how to report drone sightings,
- Setting security requirements for manufacturers and end-users of counter-drone equipment to safely test and refine their equipment,
- Put in place significant additional classified steps to ensure that UK airports are prepared to detect, deter, and disrupt drone incursions.(Norbiton, Oct 2019)

Regulations

The Air Navigation Order (ANO) of 2016 established a number of offenses regarding the irresponsible use of drones. (National Archives, 2019) This is an extensive order much like the FAA multiple instructions / regulations / drafts for flight certifications, suitability, guidance and penalties for illegal use. APO 2016 was updated to include more offenses after the Gatwick 2018 incidents. On 30 November 2019, all sUAS drones must be registered and owners / pilots must undertake competency testing.

The DT, in its 2018 consultation, *Taking Flight: The Future of Drones in the* UK, (Transport, 2019) announced its intention to give police new powers to enforce drone offenses under ANO 2016 by:

- Giving police the power to require a drone to be grounded,
- Giving police the power to require operators to produce

evidence of registration and competency and provide the identity of the operator

- Improving police powers to investigate where an offense has been committed,
- Making an expansion to "no-fly zones" around airports from 1km to 5 km, effective March 2019,
- Improved Stop and Search power for offenses relating to flying a drone in a restricted zone of an aerodrome.[2]

Compare this approach to the ineffectual California police handling a drone operator misusing his drone during a huge and dangerous wildfire. The drone forced rescue helicopters to avoid critical areas and to be grounded. (Norman, 2019)

Practical Aviation Security in USA

An Airport Cooperative Research Project (ACRP), *Unmanned Aircraft Systems at Airports*: A *Primer* researched the potential use and impact of ATC systems, airport facility standards, environmental impact, safety management systems and community outreach. (K. Neubauer, 2015) Unfortunately, the report failed to envision the security threats posed by UAV operations away from an airport.

Security Implications of UAV Operations (5 major threats)

The security threats from current enemy drone operations are multiple:

1. A UAV can be used to conduct surveillance on airports or other high-value targets (HVT)
2. A UAV can be purposely flown into a passenger aircraft.(Example Figure 3-1 in (Nichols, et al., Unmanned Aircraft Systems in the Cyber Domain, 2019)
3. A UAV can be weaponized with a gun, DEW, Sonic systems, lasers, IEDs, to attack a high-value targets, passing quietly over the heads of security personnel and any security fencing or

barriers

4. A UAV could combine weapons and surveillance and flown into a number of specific targets
5. A UAV can be equipped with CBR element and dispense the agent over an open-air assembly, stadium, ball park, mall or concert. (Forrest, 2016)

Most of the authors' 2nd edition was devoted to expanding the threat landscape and countering the risks so determined. (Nichols, et al., Unmanned Aircraft Systems in the Cyber Domain, 2019) In this text, the authors assume the enemy fights back. All the risks remain and must be considered viable scenarios at some level of exposure and mitigation. Several Russian and Chinese competitive systems are discussed later in this chapter.

Important Changes in Electronic Warfare

The authors agree with Commander Malte von Spreckelsen, DEU N, NATO Joint Electronic Warfare Core Staff that modern conflicts will be fought in all dimensions possible and that Electronic Warfare (EW) will be the key for modern conflict. (Commander Malte von Spreckelsen, 2018)[3]

The modern "father" of Electronic Warfare technology is David L. Adamy. In his textbook (Adamy D. L., 2015) he points out important changes in EW (especially after the Iraq wars and the expansion of UAS in the battlefield):

- The recognition of the electronic environment as a distinct battlespace;
- New and extremely dangerous electronically guided weapons;
- New technologies that impact both the accuracy and lethality of weapons.

Adamy defines radio emissions associated with threats as "threats."

This is not technically correct because things that explode or can cause great damage are also threats. Adamy refers to signals as threats, especially radar and radar-controlled weapons:

- Search and acquisition radars;
- Tracking radars;
- Radio links between radar processors and missiles

The other significant area defined by Adamy is communication threats which include:

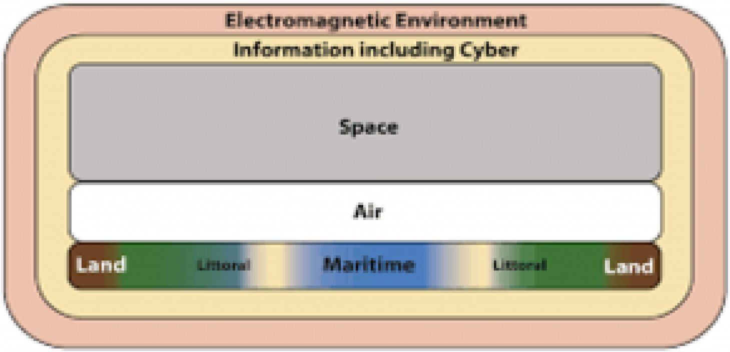
- Command and control communications;
- Data links between components of integrated air defense systems;
- Command and data links connecting UAVs with their control stations;
- Cell phone links when used for military purposes.(Adamy D. L., 2015)

Adamy essentially focuses on ADS. Cmd. von Spreckelsen considers integration of the EMS the entire battlespace to insure effectiveness of IADS suppression. (Stathopoulos, 2018) See Figure 10-1.[4]

NATO has a pretty decent view on the threats it may encounter on land, on and below sea, in the air, and in space. Furthermore, cyberspace is increasingly considered by NATO as critical risk – determinative. (Commander Malte von Spreckelsen, 2018)

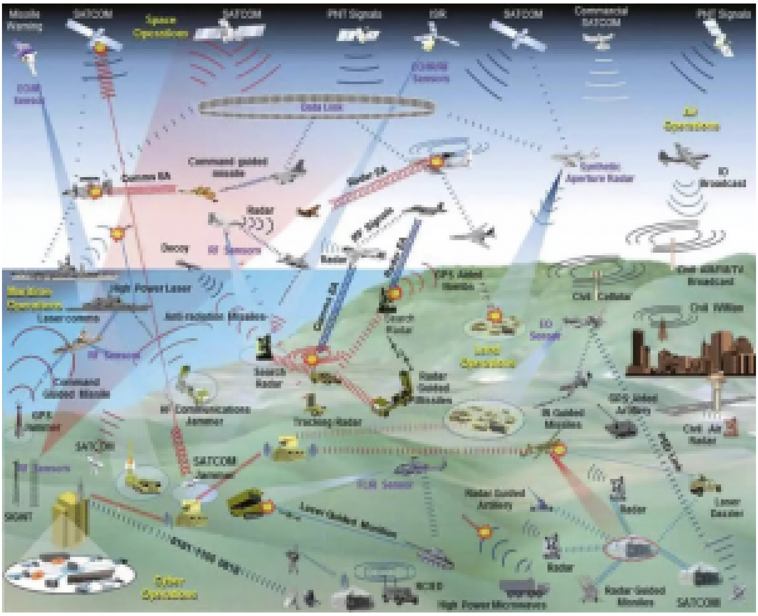
"In its EW policy[5], NATO defines Electronic Warfare as 'a military action that exploits electromagnetic energy, both actively and passively, to provide situational awareness and create offensive and defensive effects'. It is warfare within the Electromagnetic Spectrum (EMS) and (shown in Figure 10-2) involves the military use of electromagnetic energy to prevent or reduce an enemy's effective use of the EMS while protecting its use for friendly forces."

Figure 10-1 Integration of the Electromagnetic Spectrum (EMS) into Every Operating Domain



Source: (Stathopoulos, 2018)

Figure 10-2 Electronic Warfare in today's military environment

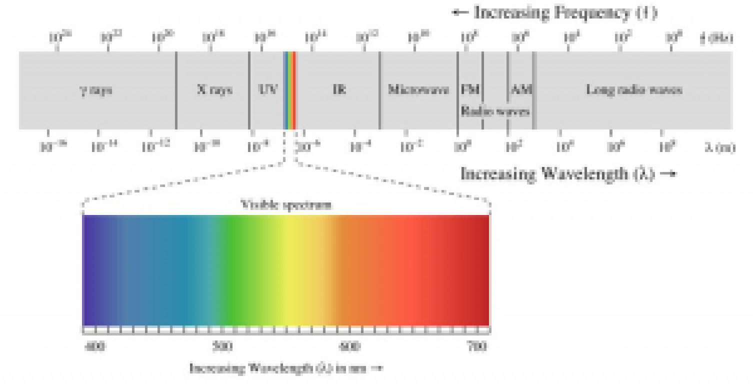


Source: (Commander Malte von Spreckelsen, 2018)

Figure 10-2 is a complex reality. Study this in detail. Recognized the importance of communications, cybersecurity, and EW components. EW can have significant mission impact – even in the simplest possible scenario. "For example, having an adversary monitor one's communications or eliminate one's ability to communicate or navigate can be catastrophic. Likewise, having an adversary know the location of friendly forces based on their electronic transmissions is highly undesirable and can put those forces at a substantial disadvantage." (Commander Malte von Spreckelsen, 2018)

Recall from (Nichols, et al., Unmanned Aircraft Systems in the Cyber Domain, 2019) the EMS purview in Figure 10-3:

Figure 10-3 EMS Purview



Source: (TRS, 2018)

Now integrate the EMS information with the Battlespace Dimensions in Table 9-3 from previous chapter (Nichols, et al., Unmanned Aircraft Systems in the Cyber Domain, 2019):

The point is that the security environment has changed necessitating a refocus on EW, especially integrated with Cyber capabilities. Russia and China have significantly upgraded their capabilities to operate in the EMS. (Commander Malte von Spreckelsen, 2018) These are not threats to be ignored.

Revisit Figure 9-21 showing the intersection of Cyber, EW, and Spectrum Warfare designated as Cyber Electromagnetic Activities (CEA).[6]

Cyberwarfare Purview

When our authors think *Cyberwarfare*, the consensus is that cyber refers to information moved from computer to computer over the Internet, within the network of computers comprising the Internet. In Chapter 4 of the 2nd edition textbook (Nichols, et al., Unmanned Aircraft Systems in the Cyber Domain, 2019) the authors expanded this definition to measures on the information superhighway to gain military advantage by gathering military significant information from the enemy or interfering with the enemy's ability to move its own information over the Internet or other networks or to process information within a computer or finally to be able to make command decisions faster than the enemy in all the domains. In Chapter 1 of this textbook, the authors consider the role of information technologies (automated decisions, artificial intelligence (weak and strong), communications, networking, remote sensing) and later in Chapter 4 the authors consider issue of resiliency, i.e. planning for resiliency and robustness expecting pushback, when secrecy is needed, how to shield operations. In Chapter 9, the authors introduced SCADA attacks and vulnerabilities and how important they were in terms of UAS operations.

The uninitiated would see cyber warfare as conducted by the use of malware. This is first level software whose purpose is destruction. The tools in this view are simply viruses, worms, Trojan Horses, spyware, rootkits, attacks on service, protocols storage or data in transit. All these are useful. But the real meat especially for UAS, satellite, ground stations and mobile deployment units is SCADA and its vulnerabilities.[7] This would be like calling Stuxnet just a virus! Stuxnet was an exquisitely designed cyberweapon with vectoring in on multiple zero-day vulnerabilities, specific manufacturer OS / maintenance SCADA attacks, multiple coordinating vectors of attack, secret target acquisition in Iran. It had the huge effect of delaying Iran's nuclear buildup by destroying their centrifuge processes from within by inducing cavitation and turning off operator controls / alarms without detection. (Zetter, 2014) The only property that Stuxnet didn't have was self-destruction upon discover or self-encryption for protection against countermeasures. Stuxnet was not discovered by Iran but information was released publicly by commercial interests for unknown reasons.

Cyber vs EW Battlespace (Parallels)

EW in *legacy* terms has three major subfields and another closely related field:

- Electronic warfare (EW) support (ES), which involves hostile intercept of enemy transmissions
- Electronic Attack (EA) in which enemy electronic sensors (radars and communications; receivers) are degraded either temporarily or permanently by transmission of signals designed for that purpose;
- Electronic protection (EP), which is a set of measures designed to protect friendly sensors from enemy EA actions;
- Decoys, which act as bait to cause enemy missile and gun systems to acquire and track invalid targets.(Adamy D. -0., 2015)

Cyber warfare (CW) involves attacks on military assets through networks, including the internet. Electronic Warfare involves attacks on military assets through electromagnetic propagation.

Table 10-1 continues the *legacy* definitions comparison of CW and EW functions.

Table 10-1 Comparison of EW and CW Functions in legacy terms

Operational Function	**EW**	**CW**
Collect information from enemy	EW support, listens to enemy signals to determine enemy capabilities and operating mode	Spyware, causes information to be exported to a hostile location (or friendly depending on the side employed)
Electronically interfere with enemy's operational capability	EA, either covers received information or causes processing to give inaccurate outputs	Viruses, reduce available operating memory or modify programs to prevent proper processing outputs
Protect friendly capabilities from enemy's electronic interference	EP, prevents enemy jamming from impacting operational capabilities	Passwords, firewalls, VPNs, hardware modifications, cryptography,[8] steganography [9],2-factor authentication, digital signatures, prevent malware from penetrating a computer and breaching information security protocols
Cause enemy systems to initiate undesired actions	Decoys, look and act like valid targets, when acquired by missile or gun systems point away from the real target	Trojan Horses, rootkits, are hostile software accepted by the enemy computers because they appear valid and have acceptable credentials (Adamy D. -0., 2015)
Direct damage or destruction	DEW, Acoustic grenades, lasers, anti-satellite weapons all hit the UAS target from outside and destroy it by delivering focused energy in real time on a small slice of the target	Advanced Cyberweapons attack SCADA and internal subsystems causing them to act in unplanned actions (fatal) to either over or under perform a critical function or subfunction, lose energy, destabilize, or prevent operator action on a critical fault (Nichols, et al., Unmanned Aircraft Systems in the Cyber Domain, 2019)

EMS Environment

It can be deduced from Table 10-1 that the difference between cyber warfare and EW has to do with how the hostile function is introduced into the enemy's systems. Historically, EW dealt with the electromagnetic spectrum (EMS) as it was related to kinetic threats. Radars that locate targets guide missiles to those targets and detonate warheads. EW was purposed to make missiles unable to hit those targets. This meant disrupting a receipt of a return signal or preventing the missile uplink from delivering guidance information. Enemy communications relate to command and control (CC). Historically, this referred to kinetic attack protocols. The purpose of EW was to prevent CC by the enemy. (Adamy D. -0., 2015)

Computers and software are an integral part of almost every aspect of modern warfare, and cyber warfare attacks on those computers directly impacts kinetic attacks and the defenses against those attacks. The new reality is that the EMS itself has become a target of enemy actions. By denying USA use of the EMS, the enemy can inflict significant economic damage upon society, put our military forces at a disadvantage without firing a single shot or dropping a single bomb.

The EMS environment is becoming more complex, congested, and contested, making it imperative for Defense agency and organizations to continually improve EW capabilities to enable reliable use of the EMS.

NATO – EME, EMO

NATO, like DoD, is evolving how it conducts operations and support of emerging technologies. The focus has shifted away from isolated EW operations to joint Electromagnetic Operations (EMO) in the electromagnetic environment (EME). (Commander Malte von Spreckelsen, 2018).

The EMS is defined as the entire distribution of electromagnetic radiation according to frequency or wavelength (Figure 10-3).[10] Electromagnetic waves (EMW) travel at speed of light in a vacuum, they do so across a wide range of wavelengths and corresponding frequencies. EMS comprises the span of all electromagnetic radiation (ER) and consists of many subranges called spectral bands such as visible light or ultraviolet radiation. EME is the geophysical environment influenced by terrain, weather and atmospheric conditions, which supports the radiation, propagation and reception of ER across the entire EMS. (Commander Malte von Spreckelsen, 2018)

Within NATO, EMO is the deliberate transmission and reception of EM energy in EME for military operations. This includes communications, navigation, attack, battlespace awareness, and targeting. Figure 10-4 demonstrates that EMO not only enables operations in each domain but also provides the thread which links and integrates military forces across domain, and in cyberspace and information environments. EMO is conducted by both friendly and enemy forces. EMO often leads to contested, overlapping, congested or interference with neutral actors in the EME. (Commander Malte von Spreckelsen, 2018)

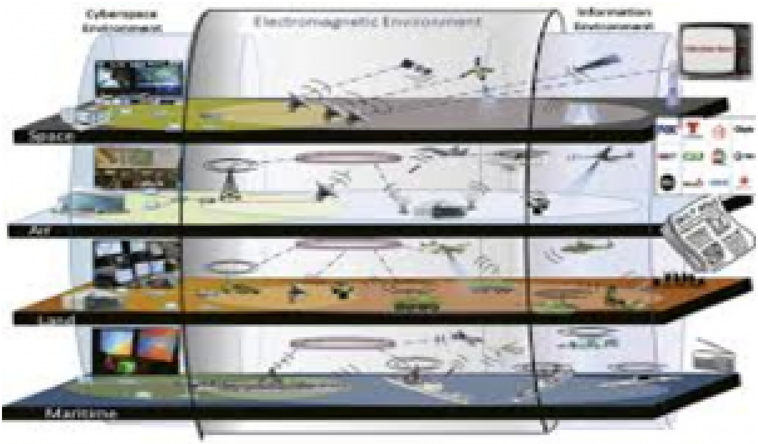
DE Weapons

In Chapter 9, the authors looked at the basic principles of DE weapons. UAS in flight (SWARMS or other configuration) are subject to destruction by deployment of DE weapons. DE weapons are in a class by themselves and represent huge portion research budgets in USA, China and Russia. All military and large commercial UAS are potential targets for DEW deployment. There are four types of DE weapons, kinetic energy, lasers, microwave and particle beams. (Nielsen, 2012) The approach taken is to discuss fundamental concepts, then propagation (travel) towards the target, and lastly, interaction with the target and the mechanisms by which the target is destroyed.

Kinetic Energy Weapons (KEW)

Kinetic energy (KE) weapons fir the definition of DEW because their energy is aimed or directed at a target and intercepts a small fraction of the target's surface area. 10,000 Joules is a magic number because it is close to the energy delivered by a wide range of DEWs. 10,000 Joules is sufficient energy to vaporize about one cubic centimeter of anything! (Nielsen, 2012)

Figure 10-4 EMO in EME



Source: (Commander Malte von Spreckelsen, 2018)

We need some understanding of the parameters and units affecting target response and damage. Table 10-2 shows key parameters, units, definitions, and comments

KEW damage targets with their energy of motion. This energy is proportional to a projectile's mass and the square of its velocity. In space, projectile motion is determined by the gravitational force of earth, along with the forces from the projectile's launcher or on-board engine. Gravitational forces dominate a projectile's trajectory, and KE far exceed damage criteria. Stress in the target exceed its internal strength, and it responds like a dense gas. Details of projectile and target construction are of minor importance. In the atmosphere, ranges are shorter and energies less due to atmospheric drag. At lower energies forces internal to a target are important. The target's response depends on its construction and end engagement scenario. Projectile design for efficient propagation and interaction is a priority and may be a compromise with optimization for target interaction. (Nielsen, 2012)

Table 10-2 Parameters , Units affecting Target Response and Damage

Parameter	Symbol	Units	Definition	Comments
Kinetic Energy	K	Joules (J)	K= Mv2 / 2	M,v = Projectile mass, velocity
Momentum	ρ	Kg m/ sec	Mv	K and ρ are conserved when particles collide
Force	F	Newtons (Nt)	M dv/dt	Also, F= dp/dt
Pressure	P	Nt/m 2	Force / Area	Force/ Area = Energy / Volume
Impulse	I	Nt sec	Force x time	
Fluence[11]	F or	Joules / cm 2	KE /area	Concentrated KE density necessary to damage a target measured as an output of a radiation field or laser beam
Or Intensity	I	Watts / cm 2		

Source: (Nielsen, 2012)

The finite speed of KEW (10 km/sec or less) means that the time to engage goes up with increasing distance and moving targets can be engaged only if they are "led"[12] with computer calculations made in advance on how to bring the weapon and target together. There are three truths that hold for all types of DEW.

1. "Propagation in a vacuum follows well defined physical laws. These account for adequate energy placement on the target by the weapon. Long ranges associated with engagements in space place severe constraints on the energy that the weapon launcher requires to ensure lethal energies are brought to bear on the target. Orbital motion counts for much of the energy in

space. This energy is not free and comes from the energy in the rocket engines which placed the weapons in orbit.(Nielsen, 2012)

2. In the atmosphere, ranges are much less than in space and interactions results in greater energy losses. Therefore, weapon characteristics / parameters (bullet shape, laser pulse width, etc.) must be tailored to minimize these energy losses. (Nielsen, 2012)
3. When a weapon encounters a target, energy must be efficiently absorbed for damage to occur. This places constraints on weapon parameters which may be conflict with those necessary for efficient propagation. (Nielsen, 2012)

Lasers

A Laser is fundamentally nothing more than a device that can produce an intense, or highly energetic, beam of light.[13] Light is an EM band in the EMS and is subject to Maxwell's wave equations. (David H. Staelin, 1998) Here are the basic ideas about lasers as weapons from (Nielsen, 2012):

1. Lasers are intense sources of ER with wavelengths from 10 to 0.4 μm and frequencies from about 3 x 10 13 to 8 x 10 14 Hz.

2. The materials with which lasers might interact are characterized by an index of refraction, n, and the attenuation coefficient, K. When light passes regions of different n, it is bent according to the Law of Refraction. When light propagates a distance, z, through a region whose attenuation coefficient is K, its intensity is decreased by a factor of e (-Kz).

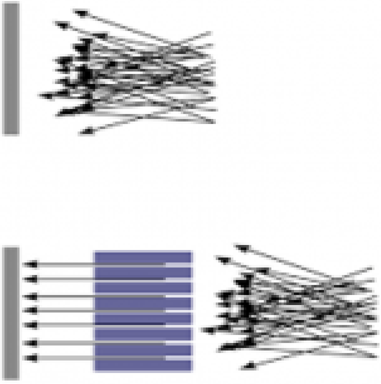
3. A laser with a wavelength, λ, emerging from an aperture of diameter, D, can propagate a distance on the order of D2 / λ, as a collimated beam.[14] Beyond this distance, it will diverge at

an angle of θ ≈ λ / D. Figure 10-5 shows Collimated light for Laser.

4. Decreases in intensity result from both diffraction and attenuation. This results in a fraction of the beam's energy being reduced and reduces the amount of energy that can be brought to bear on the target. Compensating parameters to reduce this effect are energy level, pulse width, wavelength, and diameter of the beam.

5. In the atmosphere, K, is highly dependent, made up of contributions from absorption and scattering from both molecules and particles.[15] If a beam becomes too intense, free electrons in the atmosphere will multiply and breakdown, forming an ionized *plasma* which will absorb the beam. Following the breakdown, plasmas propagate toward the source of laser light as combustion or detonation waves.[16]

Figure 10-5 Collimated light for Laser



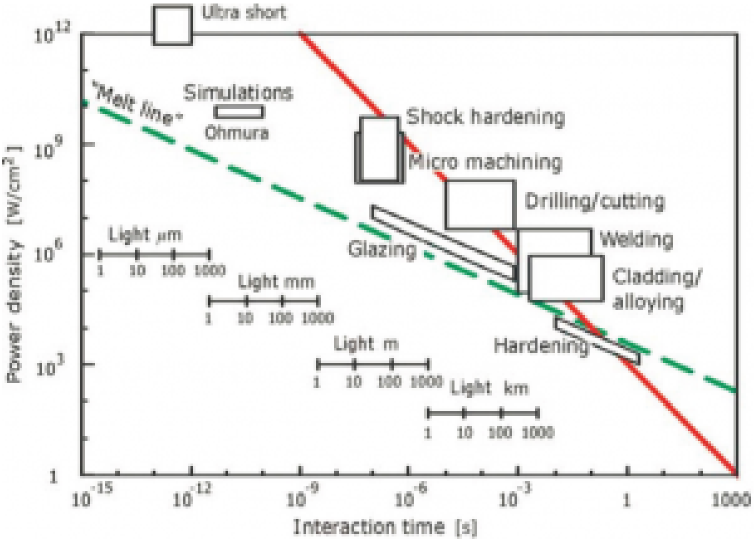
Source: (Jackson, 2017)

6. In the atmosphere, n, the index of refraction, can vary through turbulence or through expansion induced by absorption of laser light. The second effect results in beam expansion (thermal blooming) or bending. These effects must be compensated for in real time through adaptive optics.

7. When laser light encounters a target , a fraction of the light is absorbed in the target surface, and manifests as heat. Thresholds for melting and vaporization are established by the criterion that energy is deposited so rapidly that it cannot be carried away within the pulse width of the laser. Targets can be damaged by erosion (thermal melting) or through momentum transferred to the target surface by the evolving vapor jet (mechanical damage).[17]" (Nielsen, 2012)

Actually, the torch cutting process is a good example of laser optimization of intensity versus pulse width concept. Such optimum considers propagation and interaction effects as they work together to constrain the available operating parameters. Figure 10-6 Laser technology processing activities used in manufacturing.[18]

Figure 10-6 laser processing activities as a function of the laser pulse width



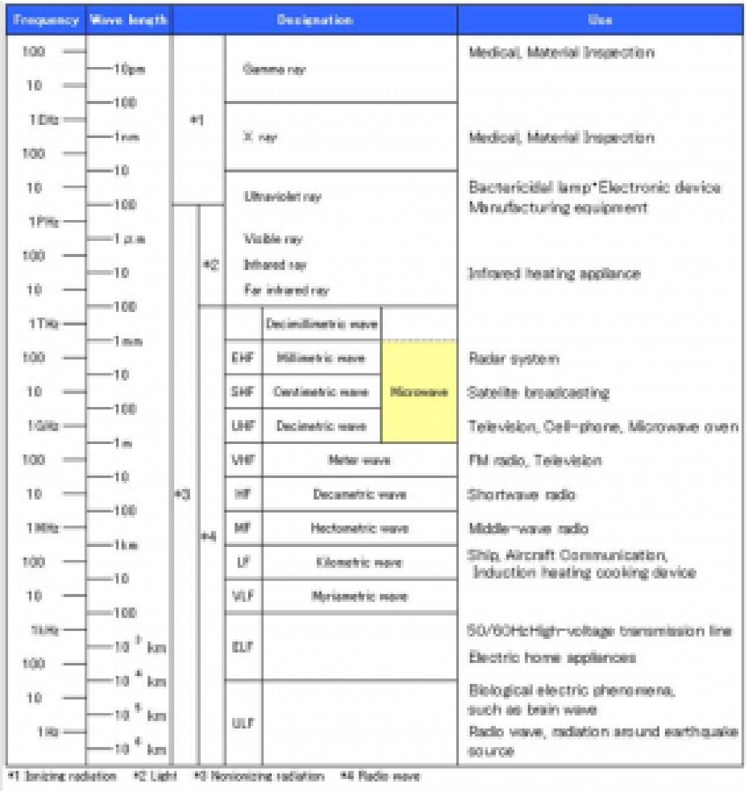
Source: (National Academies of Sciences, 2018)

It may be concluded (extending the torch thinking) that there is very little opportunity to damage targets in the atmosphere without operating at intensities where potentially deleterious propagation effects must be handled. Even melting through targets in times less than seconds will be influenced by thermal blooming. If mechanical damage is needed, the full range of propagation effects could constrain the interaction between laser and target. [19]

Microwaves

Like lasers, microwaves travel through space, carrying energy and are characterized by specific frequencies. Microwaves are another form of ER, having a much longer wavelength and much lower frequency than light. Microwaves have wavelengths of about 1 cm, and frequencies on the order of 1010 Hertz, or 10 GHz. (See Figure 10-7) Microwaves have a long history of use in commercial devices.

Figure 10-7 Microwave portion of the EMS


Frequency
100
10
1EHz
100
10
1PHz
100
10
1THz
100
10
1GHz
100
10
1MHz
100
10
1kHz
100
10
1Hz
Wave length
10pm
100
1nm
10
100
1 μm
10
100
1mm
10
100
1m
10
100
1km
10
100
10 3 km
10 4 km
10 5 km
10 6 km

Designation				Use
*1		Gamma ray		Medical, Material Inspection
*1		X ray		Medical, Material Inspection
*2		Ultraviolet ray		Bactericidial lamp・Electronic device Manufacturing equipment
*2		Visible ray		
*2		Infrared ray Far infrared ray		Infrared heating appliance
*3 *4		Decimillimetric wave		
	EHF	Millimetric wave	Microwave	Radar system
	SHF	Centimetric wave		Satellite broadcasting
	UHF	Decimetric wave		Television, Cell-phone, Microwave oven
	VHF	Meter wave		FM radio, Television
	HF	Decametric wave		Shortwave radio
	MF	Hectometric wave		Middle-wave radio
	LF	Kilometric wave		Ship, Aircraft Communication, Induction heating cooking device
	VLF	Myriametric wave		
	ELF			50/60Hz High-voltage transmission line Electric home appliances
	ULF			Biological electric phenomena, such as brain wave Radio wave, radiation around earthquake source

*1 Ionizing radiation *2 Light *3 Nonionizing radiation *4 Radio wave

Source: (Micro Denshi Co.,Ltd., 2019)

Microwaves travel at the speed of light, c, (=3 x 108 m/sec) in a vacuum. They have frequency, v, and wavelength, λ, related by the expression v = c / λ. Microwave frequencies lie in the range of 0.1 – 100 GHz, and the associated wavelengths lie in the range 100 – 0.1 cm. Microwaves are unique in that their wavelengths are similar in size to the physical objects they interact with. (Micro Denshi Co.,Ltd., 2019)

Microwave Target Interaction

Microwaves are likely to damage targets through the soft kill mechanisms (*similar to cyber-attacks on* SCADA *systems*) – those that exploit inherent target vulnerabilities. There are two types of soft-kill: in-band and out-of-band. (Nielsen, 2012)

1. With in-band damage, microwaves enter target through its antenna.(Adamy D. , 2009) This requires that the attacking microwaves be of the same frequency as those the target is tuned to receive. Damage occurs when the target's circuits are loaded beyond their design capacity. (Nielsen, 2012) The best-known example of in-bound microwave attack is EW jamming, a staple of CEA. (Adamy D. , 2009) Although there are shielding methods in military UASs to reduce this microwave jamming vulnerability, damage may still occur.

2. In out-of-bounds damage, microwaves enter the target through the back door – apertures (*again similar to some cyber-attacks*) which were not designed for entry. Damage occurs as the microwaves are absorbed in thin, sensitive electronic components, heating them to the point of exhaustion and damage. (Nielsen, 2012)

Particle Beams

The fourth (DEW, Lasers, Microwaves and Particle Beams (aka PB)) type of DEW that may be used against UASs are Particle Beams. Particle beams are large numbers of atomic or sub-atomic particles moving at relativistic velocities. [20] There are a large number of particles in these beams. Their interactions among themselves is as important as their interactions with the atmosphere and with targets. Below are the main concepts as we delve into the propagation and interaction forest of charged and neutral particle beams. (Nielsen, 2012)

1. There are two types of PB: charged and neutral. Charged PB consist of particles such as electrons and photons which have an electrical charge. Charged PB tend to spread because of mutual repulsion of their particles. Neutral PB consist of electrically neutral particles such as hydrogen atoms.(Nielsen, 2012)

2. A PB is characterized by the current it carries, the energy of its particles, and its radius. These quantities are related to more weapon related parameters such as intensity, through relationships shown in Table 10-3. (Nielsen, 2012)
3.

Table 10-3 Quantities Used to Characterize Particle Beams (PB)

Fundamental Physics	Beam Engineering	Weaponeering
Particle charge, q	Current, I	Beam intensity, S
	I = nqvπw2	S= nKv
Beam radius, w		
Particle density, n	Kinetic Energy, K	Beam Fluence, F
	ϒ =1/(1-v2 /c2) 1/2	F= Stp
Particle velocity, v	K= (ϒ-1)mc2	
	Pulse width, tp	Pulse width, tp

Source: (Nielsen, 2012)

3. Real PB deviate from perfection, in which all the particles propagate in the same direction with the same velocity. Lack of perfection is expressed in PB *brightness* (current/area/per

solid angle); *divergence* (angle which the PB envelope makes as it expands); or *temperature* (small random fluctuations in energy about the average value). (Nielsen, 2012)

4. Neutral PB can propagate only in a vacuum at altitudes greater than about 100 km. Charged PB can propagate only in the atmosphere at altitudes less than about 200 km.(Nielsen, 2012)

5. In propagating through the atmosphere, particles in the PM lose energy by ionization of the background gas and radiation. Further, if the PB contains heavy particles (photons or atomic nuclei), it loses current from collisions. These negative effects are reduced in magnitude as the atmospheric density is reduced. PB can also become unstable and cease to propagate when internal perturbations occur and grow. (Nielsen, 2012)

6. PB interact with targets just as they do with the atmosphere – through ionization, bremsstrahlung,[21] and nuclear interactions. The energy deposited into the target is a function of its density. Energy losses from a PB propagating through the atmosphere to a target are less than those within the target itself.(Nielsen, 2012)

7. For PB in the atmosphere, the total time it takes to destroy a target may be greater than the time required for a constant beam to deposit sufficient energy on it, because of “hole-boring” and suppression of instabilities.

PB Target Implications (especially large UAS)

In principle, PB should be ideal as DEW. Unlike lasers or microwaves, their propagation is *unaffected by weather*, clouds, rain, which add very little to the mass a PB might encounter on the way to the target. PB are an all-weather weapon. Once the PB encounters the target, the long penetration range of relativistic particles ensures that critical components on the interior of the target will be rapidly engaged. Time is not wasted on eroding protective layers of matter on the target surface. Shielding targets against PB as a defensive countermeasure (CM) is not practical.

In practice, PB are not technologically "there" yet. Difficulties in achieving stable propagation in the atmosphere has caused the research funds to focus on space based neutral PB, where physical problems of atmospheric propagation are replaced by engineering problems of deployment into space and maintaining large constellations of particle accelerators. (Nielsen, 2012)

So, of four DEW, it appears that only Lasers, Microwaves are viable and cost-effective approaches. However, a new EMS team player has joined the C-UAS fray. Sound. Sound has some very nice properties and is useful as both a countermeasure and an identifier in IFF systems. *Sound* as a CM was introduced in *Chapter 19: Audiology, Acoustic Countermeasures against Swarms and Building IFF Libraries* of (Nichols, et al., Unmanned Aircraft Systems in the Cyber Domain, 2nd Edition, 2019) [22] A summary of findings of this previous work follows.[23]

Acoustic Countermeasures and Building Identify Friend or Foe (IFF) Acoustic Libraries –Revisiting the C-UAS Problem

The Risk of success of Terrorist Attacks on US Air Defense Systems (ADS) via sUAS / UAS is higher and improving because of commercial capabilities and accessibility. Advanced small drones capable of carrying sophisticated imaging equipment, significant (potentially lethal) payloads and performing extensive Intelligence, Surveillance, and Reconnaissance (ISR) missions are readily available to civilian market. **They pose a significant threat to civilian and military UAS operations and safety in the NAS. The highest threats to ADS are presented by hostile UAS SWARMS.**

Problem Solution

The author's research suggests that UAS SWARMS can be both

identified (IFF) and destabilized / mitigated /eliminated / countered in the air by applying harsh acoustic countermeasures at resonance frequencies. UAS (in any formation – especially SWARMS) present *detectable acoustic signatures* that can be collected in an IFF sound libraries and like fingerprints or DNA they are unique to the make, model and origin manufacturer. Once identified as hostile, UAS (SWARM units) may be destabilized by harsh – explosive amplitude acoustic countermeasures to the MEMS or rotor base of the UAS's causing destabilization of the UAS and grounding. Emergency and waypoint recovery functions do not work under this approach.

Sound as a Weapon and Countermeasure

Next, we add *sound* to the group of DEWs. The approach taken is to discuss fundamental concepts, then propagation (travel) towards the target, and lastly, interaction with the target and the mechanisms by which the target is destroyed.

Essentials of Audiology

The question is why would hitting a UAS going at 100+ mph or more be susceptible to a loud noise hitting the MEMS under the rotors or the rotors themselves? Why would this same noise or variation thereof be capable of characterization of the UAS's of a hostile or friendly power? It is not something we can just take for granted without understanding the essentials of audiology underlying the process.

Detection Signatures

(Nichols, et al., Unmanned Aircraft Systems in the Cyber Domain, 2nd Edition, 2019) found that UAS / UAVs are detected by their ***signatures***: noise (acoustic), optical (visible), infrared (thermal) and radar (radio). "These acoustic or electromagnetic emissions occur at the following wavelengths: (Austin, 2010)

1. A) Noise (acoustic) [16 m-2 cm, or 20 – 16000 Hz]

2. B) Optical (visible) [0.4 – 0.7 um]
3. C) Infrared (thermal) [0.75 um – 1 mm]
4. D) RADAR (radio) [3 mm – 3 cm]" (Austin, 2010)

"If the designer is to reduce the vehicle detectability to an acceptable risk level, it is necessary to reduce the received emissions or reflection of the above wavelengths (expressed as frequencies) below the threshold *signature* value. A good portion of the UAS signatures are a function of the operating height of air vehicle." (Austin, 2010) The concept of frequency as a fifth realm can be elucidated in terms of targets, battlespace, and wavelengths. (Nichols, et al., Unmanned Aircraft Systems in the Cyber Domain, 2nd Edition, 2019) One of the parameters, range was a serious limitation on performance. Range has a significant impact on radio transmission. Depending on the environment, the strength of a received signal, T, is a function of the square or fourth power of a distance, d, from the transmitter. (Adamy D. -0., 2015)

In Chapters 8 and 14 of (Nichols, et al., Unmanned Aircraft Systems in the Cyber Domain, 2nd Edition, 2019), EMS was presented with emphasis on sound frequencies, many out of human hearing range. The author's experiments were performed using DJI Phantom 4 at 400 ft. This is not a tactical distance for a C-UAS countermeasure. However, the LRAD 1000X made by LRAD Corporation is effective to a 1.864 miles. See Figure 10-8. Appendix 10-2 gives the LRAD 1000X specifications. (LRAD Corporation, 2019) Longer-range models are in pipeline. The upper end of noise – Stealth acceptability is 17,150 Hz. The Stealth range is 20 Hz – 17,150 Hz. (Austin, 2010)

Figure 10-8 LRAD 1000x C-UAS

Source: (LRAD Corporation, 2019) [24]

Designing a UAS for Stealth

Stealth means "to resist detection." Stealth applies to the air vehicle and materials visible to the enemy plus the internal SAA systems that control / create noise, heat, electromagnetic emanations, and changes in light. For ISR platforms and missions, it is essential the UAS systems be undetected in operation. "It is desirable not to alert the enemy (military) or criminals (police) to the ISR operation." It can be assumed that the enemy is using counter-UAV operations and weapons. Stealth design protects the air vehicle from these counter – UAV measures. Stealth in civilian operations results in minimal environmental disturbances. (Austin, 2010)

From a personal privacy standpoint or in civil airspace it is desirable to have the UAV stealth features turned off. [It should be as if we had flicked a switch.] (Austin, 2010) Thinking again about a team or swarm of UAS, the low-hanging fruit target is US communications. We depend on connectivity in everything we do: daily lives, social interactions, business, manufacturing, government, transportation, computers and warfare to name just a few in the extensive list. *Connectivity is any technique for the movement of information from one location or player to another.* Consider the economic impact of having our critical infrastructure (banking, air transportation, etc.) shut down. Damaging the connectivity of system is real damage. We measure connectivity in terms of information flow. In warfare, this is called Information Operations (IO). Fundamental to IO is the *frequency* at which the information is transmitted or received. Returning to stealth with respect to UAS design, we note that the intelligence, surveillance, reconnaissance and weapons payload-delivery functions of UAS. These are all IO operations and frequency is at the heart of their success against or denial by the enemy. (Adamy D. -0., 2015)

Acoustic Signature Reductions

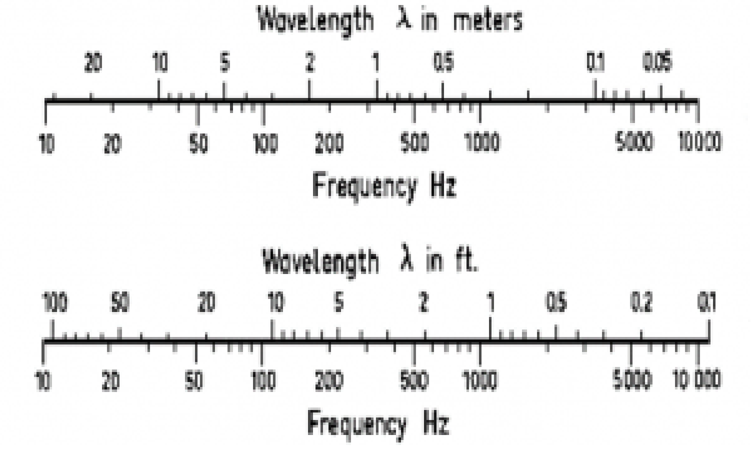
"Aircraft noise may be the first warning of its presence; however, it may not immediately be directionally/locatable for detection." "UAS noise emanates predominantly from vortices, tips of wings, rotors, or propellers. Lowering wingspan or blade span enhances acoustical stealth." Conventional propulsion systems are a concern because of the noise of combustion. Electric motors develop virtually no noise. "Reducing mass and aerodynamic drag of the UAS reduces noise generation." (Austin, 2010) The human ear is a problem for the designer. "It is most sensitive to frequencies around 3500 Hz and can hear sound down to a practical threshold of 10 dB. For a given sound pressure level, attenuation of sound with distance in air and insulating material varies as the square of the sound frequency. Low frequency sound presents a greater problem for UAS stealth design." (Austin, 2010)

Audiology Fundamentals

1. The science of sound is called *acoustics*, which a branch of physics. Appendix 10-1 displays the principal physical quantities in MKS, cgs, and English units. It is the starting point of a trip uphill to resonance frequencies. Sound is small portion of the EMS.

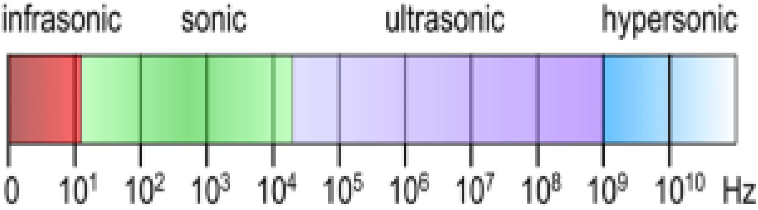
Figure 10-9 shows the conversion for sound and acoustic wave period to frequency and back. (Adamy D. -0., 2015) Figure 10-10 shows the Sound EMS regions (Adamy D. -0., 2015)

Figure 10-9 Conversion for sound and acoustic wave period to frequency and back



Source: (TRS S. , 2018)

Figure 10-10 Sound EMS Regions



Source: (TRS S. , 2018)

Acoustic waves and Sound Waves in Air

2. Sound waves are EMS waves which propagate vibrations in air molecules. The 1986 standard speed of sound, **c**, is 331.3 m/s or 1125.33 ft/s at a temperature, T = 0 degrees Celsius."(TRS S. , 2018) "The formulas and equations for sound are

$$\mathbf{c = L \times f;\ L = c\ /f = c \times T;\ f=c\ /L} \qquad \textbf{Equation 10-1}$$

Where:

T = time- period or cycle duration and T = 1/ f and f = 1 / T.

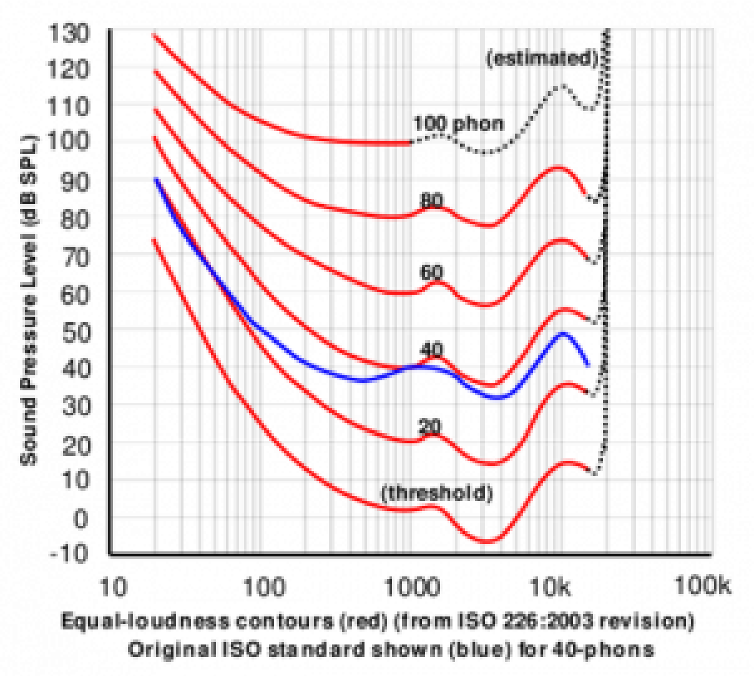
The unit for frequency is Hertz = Hz =1/s. The unit for wavelength, L is meters, m. The time-period or cycle duration, T is sec, s. The wave speed or speed of sound, c, is meters/sec, m/s." (TRS S. , 2018)

(Austin, 2010) states that the design limit for UAS Stealth for acoustic (noise) or sound waves is "[16 m-2 cm, or 20 – 16000 Hz]." **The Stealth range is 20 Hz – 17,150 Hz.** [25]

3. Hearing range describes the range of frequencies that can be heard by humans, (aka range of levels). The human range is commonly given as 20 to 20,000 Hz, there is considerable variation between individuals, especially at high frequencies,

and a gradual loss of sensitivity to higher frequencies with age is considered normal. Sensitivity also varies with frequency, as shown by equal loudness contours. (Rosen, 2011) See Figure 10-11.[26]

Figure 10-11 Equal Loudness Contours



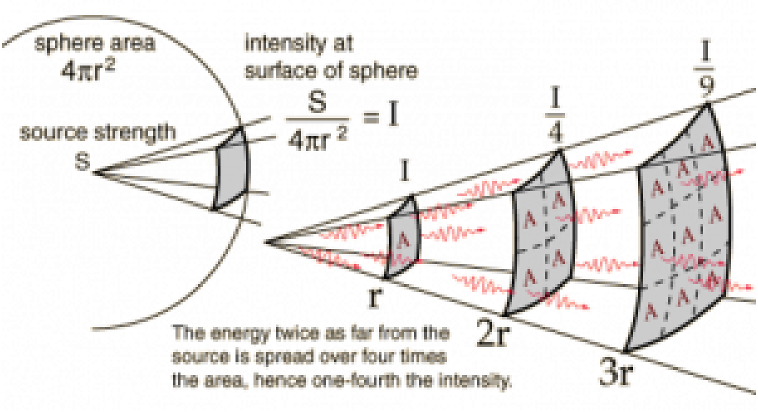
Source: Equal -Loudness Contours (Fletcher, 1933) (Rosen, 2011)

Intensity and Inverse Square Law

4. "Sound radiates outward in every direction from its source. This constitutes a sphere that gets larger and larger with

increasing distance from the source."(Entokey, 2019) Figure 10-12 shows the relationship between Intensity and the Inverse Square Law.(Uni-wuppertal, 2019) Intensity (I) (power divided by area) decreases with distance from the original source because of finite amount of power is spread over increasing surface area. (Entokey, 2019) Proportionately less power falls on the same unit of area with increasing distance from the source. (Gelfand, 2004) [27] [28]

Figure 10-12: Inverse Square Law, Sound Intensity



Source: (Uni-wuppertal, 2019)

5. Figure 10-13 shows common decibel and Intensity levels within the hearing range. This does not consider environment, frequency differences or noise (discussed presently). It does show the ease of which decibels may be used to rank the sound intensity levels which vary greatly in magnitude. Hearing aids are effective from about 6 –90 decibels. Above 90 dB, they can dampen but not eliminate the very loud sounds

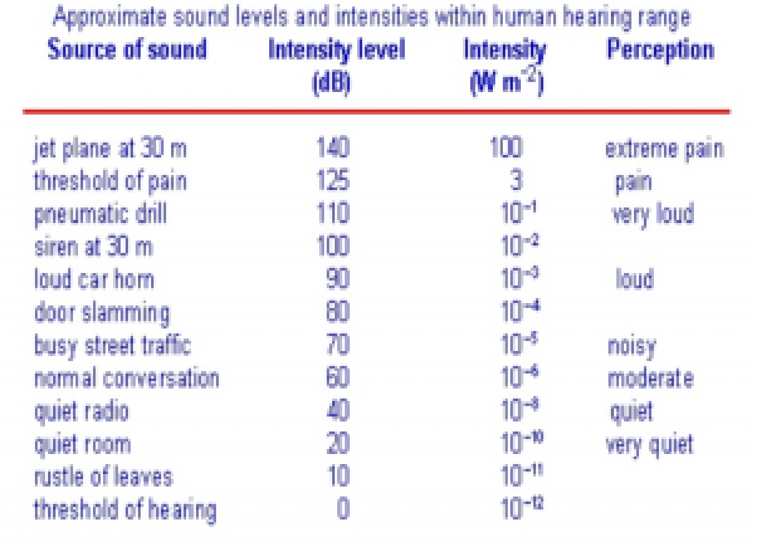
unless there is complete loss of hearing.

The Nature of Sound

6. *Sound is defined as a form of vibration that propagates through the air in the form of a wave. Vibration is the to-and-fro motion (aka oscillation) of an object.* Some examples are playground swing, tuning fork prong, air molecules and UAS rotor blades [circular motion]. The vibration is called *sound* when it is transferred from air molecule to air molecule. This transfer may be simple like a tuning fork or a very complex pattern like the din in a school cafeteria. Naturally occurring sounds are very complex. (Entokey, 2019) UAS sounds are not natural and supported by machinery, hardware and software. Three weaknesses of the UAS are the MEMS, gimbal assembly and rotors. Although stealth mechanisms may be employed to reduce noise emissions, the former parts are exposed. They do produce discernable signatures.

7. A tuning fork illustrates the oscillations of sound. After being struck, the tuning fork vibrates with a simple pattern that repeats itself over time. (Entokey, 2019) Figure 10-14 shows that the tuning fork when struck exerts a force on the air molecules which alternatively exerts a high pressure (compression) and a low pressure (rarefaction) zones. The zones exhibit wave amplitude and wavelength as a function of air pressure and distance. The sound wave is distributed in 360 degrees through the air.

Figure 10-13 Shows common decibel and Intensity levels within the hearing range.



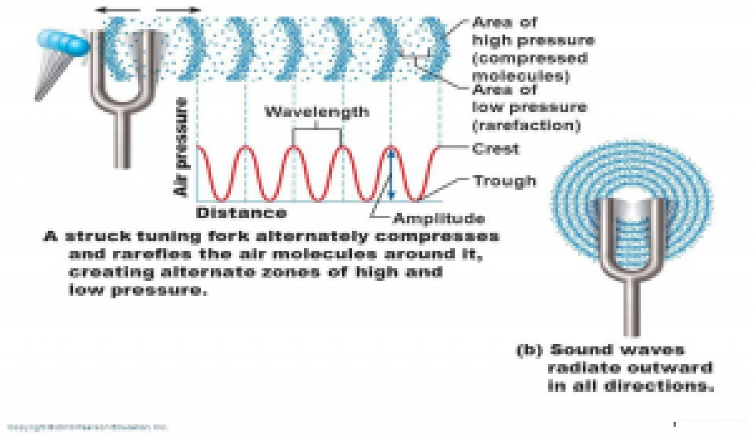
Approximate sound levels and intensities within human hearing range

Source of sound	Intensity level (dB)	Intensity ($W\ m^{-2}$)	Perception
jet plane at 30 m	140	100	extreme pain
threshold of pain	125	3	pain
pneumatic drill	110	10^{-1}	very loud
siren at 30 m	100	10^{-2}	
loud car horn	90	10^{-3}	loud
door slamming	80	10^{-4}	
busy street traffic	70	10^{-5}	noisy
normal conversation	60	10^{-6}	moderate
quiet radio	40	10^{-8}	quiet
quiet room	20	10^{-10}	very quiet
rustle of leaves	10	10^{-11}	
threshold of hearing	0	10^{-12}	

Source: (Carter, 2012)

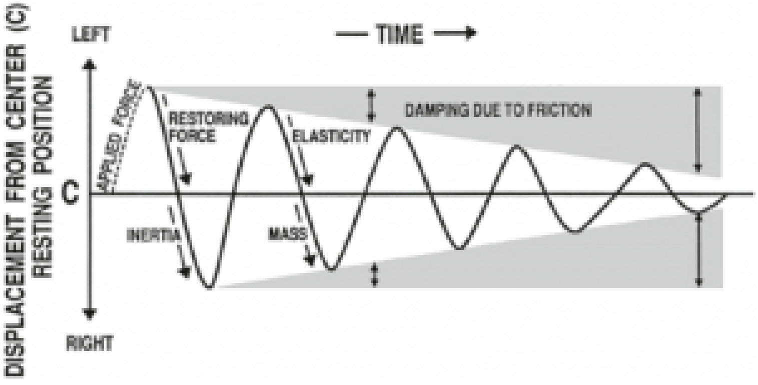
Figure 10-14 diagrams tuning fork oscillations over time. Sounds that are associated with simple harmonic motion are called pure tones. Vertical displacement amount of the tuning fork prong displacement around its resting position. Distance from left to right represents progression of time. One complete round-trip or replication of an oscillating motion is called a cycle. The number of *cycles* occurring in one second is the *frequency*. The duration of one cycle is called its *period*. This form of motion occurs when a force is applied to an object having properties of elasticity and inertia. Simple harmonic motion (SHM) shows the same course of oscillations as in Figure 10-15 because they repeat themselves at the same rate until friction causes dampening of the waveform. (Entokey, 2019) and (Gelfand S. A., 2009)

Figure 10-14: Tuning for Oscillations


Area of high pressure (compressed molecules)
Area of low pressure (rarefaction)
Wavelength
Air pressure
Crest
Trough
Distance
Amplitude
A struck tuning fork alternately compresses and rarefies the air molecules around it, creating alternate zones of high and low pressure.
(b) Sound waves radiate outward in all directions.

Source: (Pierson, 2019)

Figure 10-15: Tuning fork oscillations over time



Source: (Entokey, 2019)

Other Parameters of Sound waves

8. Probably the most useful SHM waveform is the sinusoidal wave or sine wave.[29]

The number of times a waveform repeats itself in one second is known as the frequency or cycles per second (CPS). (Gelfand S. A., 2009)Two useful relationships are: f = 1/ t or t = 1/f; where f is the frequency in cps and t is the period in seconds. A*mplitude* denote the magnitude of the wave. The *peak- to – peak* amplitude is the total vertical distance between negative and positive peaks. The peak amplitude is the distance from the baseline to one peak. The magnitude of sound at any instant is the *instantaneous amplitude.* Wavelength (λ) is the distance traveled between one peak and the next. (Gelfand, 2004) Wavelength formula is: λ = c / f, where c is the speed of sound in air (344 m/s. f is the frequency of sound in Hz. Similarly, frequency is inversely proportional to wavelength or f = c / λ. (Gelfand S. A., 2009) Another interesting sound parameter is *Pitch.* Pitch is the quality of sound and especially a musical tone governed by the rate of vibrations producing it. It is the degree of highness or lowness of sound. (Merriam-Webster, 2019)

Complex waves

9. When two or more pure-tone waves are combined, the result is *a complex wave*. (Gelfand, 2004) They may contain any number of frequencies. Complex periodic waves have waveforms that repeat themselves. If they don't, they are *aperiodic*. Combining waves may reinforce themselves or cancel themselves whether they are in phase or out. The lowest frequency component of a complex periodic wave (like a combination of sign waves) is called its *fundamental frequency. (Gelfand,* 2004)

10. *Harmonics* are whole number or integral multiples of the fundamental frequency. Waveforms show how amplitude changes with time. (Gelfand, 2004) Fourier's Theorem shows

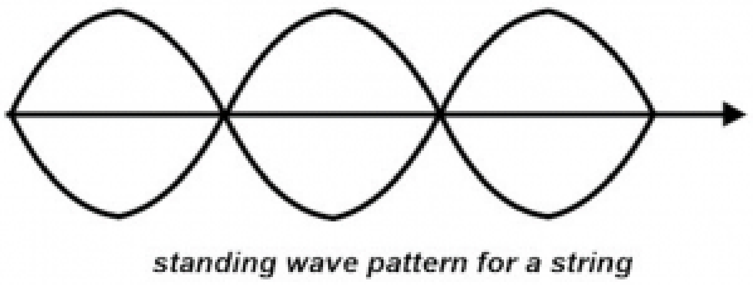
that complex sound waves can be mathematically dissected into its pure tones. Of more interest to UAS designers are aperiodic sounds which are made up of components that are not harmonically related and do not repeat themselves over time. The extreme cases of aperiodic sounds are transients and random noise. A *transient is an abrupt sound* that is very brief in duration. *Random noise* has a completely random waveform, so it contains all possible frequencies in the same average amplitude over the long run. *Random noise* is also called white noise like white light because all possible frequencies are represented.

Standing Waves and Resonance

11. *We have arrived at the crux of the acoustic* CM *discussion, the natural or resonating frequency. "The frequency(ies) at which a body or medium vibrates most readily is called its natural or resonant frequency(ies)."*(Gelfand S. A., 2009) Differences in resonance frequency ranges enable different devices to act as filters by transmitting energy more readily for certain high, low, or band-pass frequencies. UAS with multiple rotors circulate the rotors to gain lift and / or hold steady / or descend in altitude. Four, six, eight – rotor UAS maintain control via internal SCADA systems and send critical information through a MEMS component located at the bottom of rotors. Rotor frequencies are coordinated, monitored, and position -controlled through the MEMS and in-board computers. Even though the rotor(s) motions are spinning in circular fashion, the sound wave generation is not curvilinear, or aperiodic but transferred up through the Y axis and back again to its base as it ascends in altitude. There is a tendency to maintain equilibrium in terms of position of the UAS.

12. The author contends that the UAS rotor systems act like vibrating strings and resonance frequency information can be approximated by this approach. An example of a vibrating spring is when you "pluck" a guitar. The waves initiated move outward toward the two tied ends of the string. The waves are then reflected back, and they propagate in the opposite directions. The result is a set of waves that are moving toward each other, resulting in a perturbation sustained by continuing reflections from the two ends. The superimposed waves interact and propagate and appears as a pattern that is standing still. Peaks (maximum displacement) and no displacement (baseline crossings occur at fixed points along the string.[30] Places along the spring where zero displacement in the standing wave pattern are called nodes. (Gelfand, 2004) Locations where the maximum displacement occurs are called antinodes. See Figure 10-16.

Figure 10-16: Standing Wave



(Administrator, 2015)

13. "The *fundamental frequency* is defined as the lowest frequency of a periodic waveform. It is generally denoted as 'f'. The lowest

resonating frequency of a vibrating object is called as fundamental frequency."(Administrator, 2015)

14. "*Harmonic is a frequency, which is an integer multiple of the fundamental frequency*. The forced resonance vibrations of an object are caused to produce standing waves. At the natural frequency it forms a standing wave pattern. These patterns are created at specific frequencies, they are called Harmonic Frequencies or Harmonics."(Administrator, 2015)

15. "The sound produced by a wave form at its harmonic frequency is very clear, and at other frequencies we get noise, and cannot hear the clear sound of waves. Harmonics may occur in any shaped wave forms, but mostly they occur in sine waves only. Non – sinusoidal wave forms, like triangular and saw tooth wave forms are constructed by adding together the harmonic frequencies. The word harmonic is generally used to describe the distortions caused by different un- desirable frequencies called noise, of a sine wave."(Administrator, 2015)

16. "Node and antinodes occur in a wave form. So, the waves have harmonic frequency in them. The fundamental frequency is the smallest frequency in a harmonic. Hence there is only a single anti-node occurs between them. This Antinode is middle of the two nodes. So, from this we can say that the guitar string produces longest wavelength and the lowest frequency."(Administrator, 2015)

17. "The lowest frequency produced by any instrument is called the *fundamental frequency*. This is also known as first harmonic of the wave. In words of fundamental frequency, harmonics are the integer multiples of the fundamental frequency." (Ex: f,2f,3f,4f, etc…. are harmonics.) (Administrator, 2015)

18. "Because of multiple integers of fundamental frequency, we

will have n number of harmonics like 1st harmonic, 2nd harmonic,3rd harmonic, and so forth."(Administrator, 2015) "The fundamental frequency is also called as *First harmonic*. In the first harmonic, we have two nodes and one antinode. he numbers of antinodes are equal to the integer multiples of specific harmonics. i.e., for 1st harmonic we have 1 antinode, for 2nd harmonic we have 2 antinodes etc."(Administrator, 2015)

MEMS

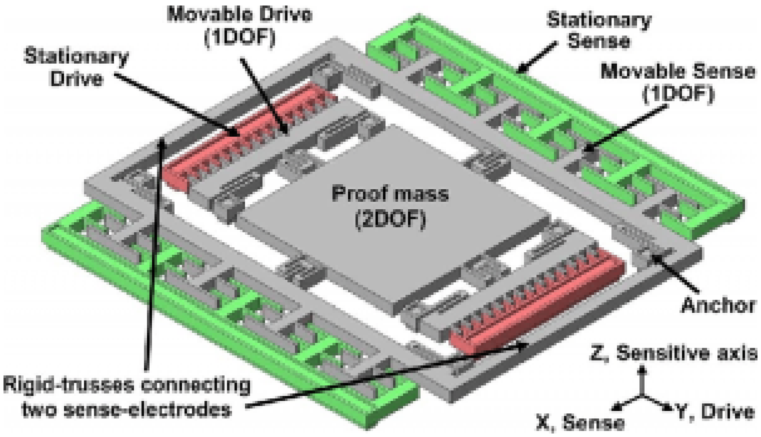
19. What is a MEMS and how does it relate to the UAS gyroscope? As shown in Figure 10-17 MEMS Gyroscope, MEMS (Micro-Electro-Mechanical-Systems) gyroscopes are located in the rotor systems of most drones. Visualization of a MEMS gyroscope is a single proof mass suspended above a substrate The proof mass is free to oscillate in two perpendicular directions, the drive and sense direction.(Said Emre Alper, December 2008)

Resonance Effects on MEMS

20. Achieving resonance frequencies can have a significant effect for countering hostile UAS:

- ***MEMS Gyroscope can be degraded using harsh acoustic noise***
- ***MEMS Gyroscope has a resonant frequency that is related to the physical characteristics of its structure* (Usenix.org, 2019)**
- **MEMS Gyroscopes have resonant frequencies much higher than can be heard (audible and ultrasonic ranges)**
- ***Unexpected resonance output caused from an attack will cause the rotor system to malfunction***
- ***Rotors will spin at differing speeds causing the drone to become unstable and crash***

Figure 10-17: MEMS Gyroscope



Source: (Said Emre Alper, December 2008)

Resonance Tuning

21. In the operation of MEMS gyroscopes, the bending changes the capacitance between the sensing mass and the sensing electrode, and this capacitance change is sensed as the output of the gyroscope By using an additional feedback capacitor connected to the sensing electrode, the resonant frequency and the magnitude of the resonance effect can be tuned Resonance can be induced by a malicious attacker, if resonant frequencies exist in gyroscopes.(Nichols R. K., Hardening US Unmanned Systems Against Enemy Counter Measures, 2019)

What is the "so what" for Acoustics?

22. "Passive detection is much cheaper and cost effective to operate vs a complex radar system for a single installation

(limited by detection range ~350ft).MEMS gyroscopes contained in rotor systems are very susceptible to malfunction when struck with rough noise that resonates inside the MEMS. Offensive acoustic systems are currently mounted, could become man portable. Offensive systems are not detected by National ELINT assets not looking for acoustic energy signatures, enemy can remain hidden from detection when using acoustics."(Nichols R. K., Hardening US Unmanned Systems Against Enemy Counter Measures, 2019)

23. What is an Acoustical attack on the UAS Gyroscope?

There are two possibilities: compromising the sound source or drone on drone attack:

Compromising the Sound Source

- UAM with speakers (consider police and military operations or search-and-rescue operations)(Usenix.org, 2019)
- Counter the source of the sound from the speaker with different frequency sound
- Jamming attack aims to generate ultrasonic noises and cause continuing vibration of the membrane on the sensor, which make the measurements impossible
- Level of noise causes performance degradation

Drone on Drone Attack

- Taking a picture of a moving object from UAM
- An adversary drone equipped with a speaker could steer itself toward a victim drone and generate a sound with the resonant frequency of the victim's gyroscope to drag it down(Usenix.org, 2019)

What are Countermeasures for Acoustic attack on Gyroscope

24. Countermeasures for attacks on gyroscope include: Physical

Isolation – provide physical isolation from the sound noise; Surrounding the gyroscope with foam would also be a simple and inexpensive countermeasure; using a differential comparator; using an additional gyroscope with a special structure that responds only to the resonant frequency so the application systems can cancel out the resonant output from the main gyroscope and improving detect and cancel out analog sensor input spoofing against CIEDs.(Nichols R. K., Hardening US Unmanned Systems Against Enemy Counter Measures, 2019)

In terms of UAS Countermeasures, why are Acoustics so important? (Nichols R. K., Hardening US Unmanned Systems Against Enemy Counter Measures, 2019)

25. They are important because:

- Offensive systems use ultrasonic frequency resonance
- Cannot be heard by humans when used to intercept a drone
- Passive systems are difficult, if not impossible, to detect
- Able to identify and track drone based on acoustic and/or visual signature
- Acoustic detection systems are limited in range ~ 350 ft to 500 ft due to environmental variables BUT commercial companies like LRAD, Corporation have developed long range acoustic devices which can detect a UAS up to a mile away at altitude.
- Can be a cost-effective way to defend a small area –especially against SWARM Attack

What are the Acoustic Detection Issues?

26. Detection relies on uniqueness of the UAS and hearing capabilities at low frequencies:

- Detects drones by recognizing the unique sounds produced by their motors

- Rely on a library of sounds produced by known drones, which are then matched to sounds detected in the operating environment, however,
- The human ear is a problem for the designer
- It is most sensitive to frequencies around 3500 Hz and can hear sound down to a practical threshold of 10 dB
- For a given sound pressure level, attenuation of sound with distance in air and insulating material varies as the square of the sound frequency
- Low frequency sound presents a greater problem for UAS stealth design
- The greater noise problem is posed by smaller UAS using piston engines
- Sound comes from their internal combustion and exhaust systems
- Sound emission can be reduced with sound-absorptive materials, silencers and mufflers and by directing the intake and exhaust manifolds upward
- Level of sound detected depends on the level of background noise for sound contrast
- Limited range to 500 feet (experimental and research – not commercial or military)
- Noisy backgrounds (airports, city downtown) limit detection & interdiction
- Drone tuning (changing the stock propellers) limits detection / Interdiction

Is Acoustic Quieting possible?

27. "Yes, under certain conditions:

- Disguise sounds from sensors to eliminate its noise and passive echoes
- "Acoustic superiority" used by the Navy to mask detection of U.S. submarines

- Acoustic technology is "passive," meaning it is engineered to receive pings and "listen" without sending out a signal which might reveal their location to an enemy
- Increased use of lower frequency active sonar and non-acoustic methods of detecting."(Nichols R. K., Hardening US Unmanned Systems Against Enemy Counter Measures, 2019)

28. **How has the Long-Range Acoustic Device (LRAD) used as a sonic weapon**?(LRAD, 2019)

It has been used primarily for denying GPS navigation:
GPS Denied Navigation

- GPS navigation relies on measuring the distance or delay, to several known transmitters in order to triangulate the mobile receiver's position
- GPS-denied environment presents navigation challenges for UAV and UAM
- These areas include urban canyons, forest canopy, etc.
- Strike Resonance frequency – which disrupts balance (vehicles tilt, orientation & rotation)

UAS Collaboration – SWARM

A UAS SWARM as a uniform mass of undifferentiated individual's w/o Chief at automation level 4 or 5. SWARMs exhibit the following advantages:

- Efficient based on numbers, emergent large group behaviors, and reactions
- Not controllable or automated, decentralized intelligence
- Think shoal of fish w/ evolving local rules; highly resistant form
- Not changing based on survivability of members, no hierarchy

SWARM Countermeasures include disruption, i.e. changing the Strategic Global View of SWARM (its only real vulnerability), complete Defender collaboration with multiple kinetic and non-kinetic countermeasures, and use of Acoustic Countermeasures for identification as friend or foe (IFF) based on a library of manufacture detection signatures and complete , abrupt rotor disablement by attacking the SWARM units with resonant, loud (100-140 dB) sound noise aimed directly at the MEMS gyroscopes or close by on the unit. [Think of glass breaking at resonance frequency or a submarine under depth charge attack. The former breaks by super-excited molecules in the glass and literally shakes apart. The latter is destroyed by violent shaking of the submarine so that its parts break and flooding ensue. It is not necessary to hit the submarine directly because explosions in water, hence sound waves and explosive forces, carry very far and effectively to the target.]

South Korean experiment

A paper by Yunmonk son, et. Al. From the Korean advanced institute of science and technology (KAIST), in the authors judgement, is the seminal paper on taken down drones using sound noise on gyroscope sensors! (Yunmonk Son, 2015) It is required reading for my students.

(Yunmonk Son, 2015) describes the relationship between *Sound Pressure Level* (SPL) and *Sound Amplitude* and derives the attack distance, d as (in dB):

$$\mathbf{SPL = SPLref + 20 \log (A / Aref)} \qquad \textbf{Equation. 10-2}$$

Where SPL = sound pressure level, SPLref is the reference, A and Aref are the amplitudes of the source and reference point. Using real-world experiments (Yunmonk Son, 2015) found that:

$$\mathbf{SPL = SPLref - 20 \log (d / dref)} \qquad \textbf{Equation. 10-3}$$

Where d, dref are the attack scenario distances.

KAIST under (Yunmonk Son, 2015) primary conclusions are:

- “Many sensing and actuation systems trust their measurements and actuate according to them. Unfortunately, this can lead to security vulnerabilities that cause critically unintended actuations.
- The sound channel can be used as a side channel for MEMS gyroscopes from a security point of view.
- 15 kinds of MEMS gyroscopes were tested, and seven of them were found vulnerable to disruption using intentional noise.
- The output of the vulnerable MEMS gyroscopes was found using a consumer-grade speaker to fluctuate up to dozens of times as a result of the sound noise.
- Authors found that an attacker with only 30% of the amplitude of the maximum sound noise could achieve the same result (disruption) at the same distance.
- At 140 decibels, it would be possible to affect a vulnerable drone up from around 40 meters away,
- Some drone gyroscopes have resonant frequencies in both the audible and ultrasonic frequency ranges, making them vulnerable to interference from intentional sound noise.
- Authors found that accelerometers integrated with MEMS gyroscopes were also affected by high-power sound noise at certain frequencies.”(Yunmonk Son, 2015)[31]

Noise

Loud and abrupt sound as a countermeasure also brings the problem of exposure and loss. Chapter 17 of (Gelfand S. A., 2009) discusses the effects of noise and hearing conservation. Chapter 20 of (Gelfand S. A., 2009) discusses occupational standards. Safety is an important topic but outside the scope of this writing.

Real World C-UAS

Time to move from the theoretical into the practical. The balance of this chapter will be devoted to a sample of deployed ADVANCED UAS / C-UAS multi-mission systems globally. They can fight back!

Chinese CH7

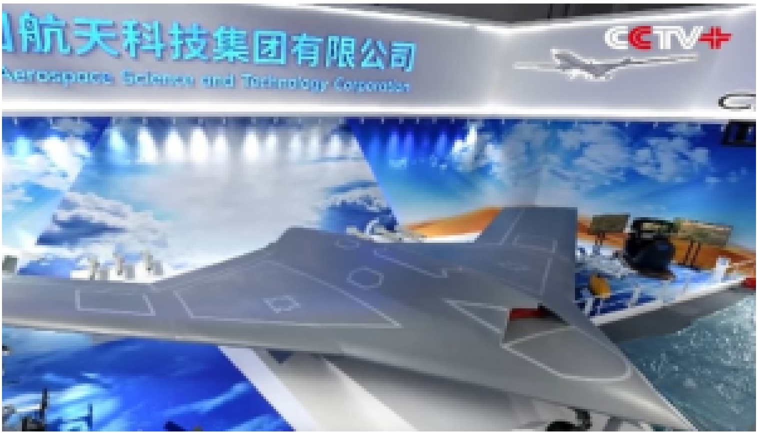
At the air show China 2018 in Zhuhai, South China, The UAV – CH7 was unveiled. The CH7 is China's new generation stealth combat unmanned aerial vehicle. The CH7 makes China the second country, followed by the US, to produce HALE combat vehicles with advanced penetration capabilities. The CH7 has internal weapons bays, making it capable of launching anti-radiation missiles, air-to-ground (ATG) or anti-ship missiles and long -distance precision guided bombs. Its missions favor high altitude, stealth capacity and endurance under dangerous conditions such as C4ISR or launching missiles at HVTs. The CH7 is 10m long and has a wingspan of 22 m. It weighs 13,000 kg, cruises at 0.5-0.6 Mach and can fly for 15 hours. The CH7 can intercept radar electronic signals and simultaneously detect, verify and monitor HVTs such as US command stations, missile launch sites and navy vessels. (Defense Editor, 2018) See Figure 10-18.

Russian Okhotnik aka "Hunter Drone"

Just as General Michael Hayden and Roger N. McDermott predicted in their report, *Russia's Electronic Warfare Capabilities to 2025: Challenging* NATO *in the Electromagnetic Spectrum* (McDermott, September 2017), along comes the Russian Okhotnik drone. Flying with the fifth generation Su-57, the Okhotnik, or "Hunter," drone which is able "to broaden the fighter's radar coverage and to provide target acquisition for employing air-launched weapons." (Pickrell, 2019)

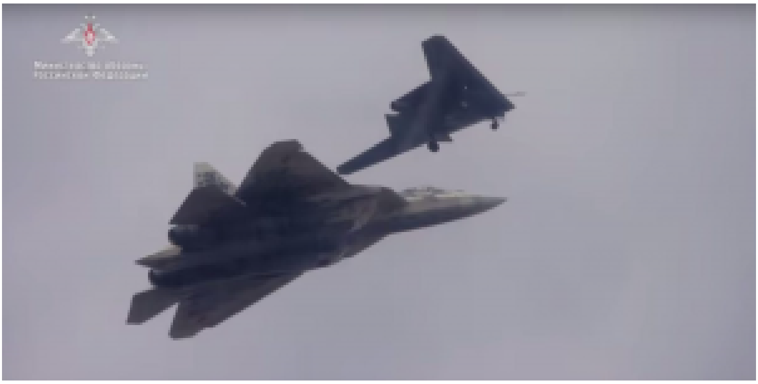
Figure 10-19 shows the Okhotnik drone flying next to the SU-57, Russia's most advanced stealth fighter. The latest flight appears to confirm suspicions that the drone was designed to fight alongside and provide critical battlespace information to Russia's newest fighters. (Pickrell, 2019)

Figure 10-18 Chinese CH7 – UAV



Source: (Defense Editor, 2018)

Figure 10-19 Okhotnik drone flying next to the SU-57, Russia's most advanced stealth fighter



Source: (Pickrell, 2019)

The Iranian Shahed 129

The Shahed 129 (Persian for Eyewitness) is an Iranian single-engine MALE (UCAV) designed by Shahed Aviation Industries for the (IRGC). The Shahed 129 is capable of combat and reconnaissance missions and has an endurance of 24 hours; it is similar in size, shape and role to the American MQ-1 Predator and is widely considered the most capable drone in Iranian service. (Taghvaee, 2017) See Figure 10-20.

General characteristics from (Taghvaee, 2017)

- Crew: none
- Capacity: 400 kg payload
- Length: 8 m (26 ft 3 in)
- Wingspan: 16 m (52 ft 6 in)
- Height: 3.1 m (10 ft 2 in)
- Powerplant: 1 × Rotax 914 four-cylinder, four stroke Ac engine
- Propellers: 3-bladed

Performance

- Cruise speed: 150 km/h (93 mph, 81 kn)
- Combat range: 1,700 km (1,100 mi, 920 nm)
- Ferry range: 3,400 km (2,100 mi, 1,800 nm)
- Endurance: 24h
- Service ceiling: 7,300 m (24,000 ft)

Armament

- Bombs: 4 × Sadid-345 PGM

Avionics
Oghab-6 electro-optical/infrared sensor
Laser range finder

Figure 10-20 The Iranian The Shahed 129

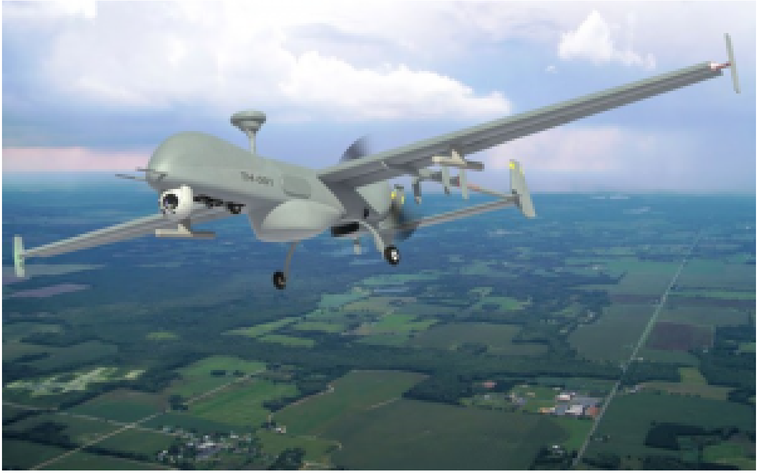
Source: (Taghvaee, 2017)

In June, U.S. Air Force F-15Es shot down two Iranian UAVs in Syria—both Shahed 129s operated by Iran's Islamic Revolutionary Guard Corps. These were rare incursions between U.S. and Iranian aircraft in the Middle Eastern country, which Iran has used as a testing ground for the Shahed, one of the most advanced armed UAVs in the Iranian Revolutionary Guard's Air & Space Force (IRGC-ASF) drone unit. It will continue to be a mainstay of the Iranian fleet for the foreseeable future. (Taghvaee, 2017)

The Israeli Tactical Heron

The Tactical Heron, joins drones that have "hundreds of thousands of operation flight hours." Designed for missions on the battlefield, the tactical Heron is used by ground troops or coast guards. The new Heron can fly up to 7.3 km. with payloads of 180 kg. (Frantzman, 2019) The Heron is used for ISTAR missions. Figure 10-21 shows the Tactical Heron.

Figure 10-21 Israeli Tactical Heron



Source: (IAI, 2019)

"According to IAI, T-Heron is the best of the best of Heron line, with all its sensors, cameras, intelligence and attack capabilities, but for the "local" tactical level. Only UAV in the world with the abilities of super drones but for tactical levels (according to the ISI). It has a versatile design and is all-weather day and night. It is 30% smaller than the standard Heron, and most importantly, cheaper. It's for the Brigade tactical level, specifically ground and mechanized forces, and can even be operated by them (without having to bring specialized drone operators). It can be brought to its required location with two trucks and can lift off and land back on very short paved low-level runways. Because it's mobile and tactical, it can travel with front-line forces with no logistical long tail headaches. It can carry multiple payloads, up to 180 KG, and its gross weight up to 600 KG. It has a flight time of 24 hours, 300 KM range, 23000 ft altitude and has a 10-meter wingspan." (IAI, 2019)

According to Moshe levy, VP of Aircraft division at IAI, "We are proud to introduce the most recent UAS developed by IAI. Our T-Heron tactical UAS rounds up the range of operational UAS solutions IAI offers to all forces on the battlefield: marine, air, ground, and intelligence. IAI preserves its leadership position in UAS's with a continuous stream of solutions for the challenges posed by the field." (IAI, 2019)

IAI doesn't foresee much maturity problems as it has the same materials and components as the other Heron's, only in smaller amounts. (IAI, 2019)

USA Predator C Avenger

The General Atomics Avenger (formerly Predator C) is a developmental UCAV built by General Atomics Aeronautical Systems for the US military. Its first flight occurred on 4 April 2009. Unlike the previous MQ-1 Predator and MQ-9 Reaper (Predator B) drones, the Avenger is powered by a turbofan engine, and its design includes stealth features such as internal weapons storage, and an S-shaped exhaust for reduced infrared and radar signatures. The Avenger will support the same weapons as the MQ-9 and carry the Lynx SAR and a version of the F-35 Lightning II's electro-optical targeting system (EOTS), called the Advanced Low-observable Embedded Reconnaissance Targeting (ALERT) system. The Avenger will use the same ground support infrastructure as the MQ-1 and MQ-9, including the GCS and existing communications networks. (Staff, General Atomics Avenger, 2019)

Predator C Avenger can carry Hellfire missiles and guided bombs and ammunition. The Predator C Avenger is a remotely piloted aircraft developed by GA-ASI. The first flight of the aircraft was conducted in April 2009. The combat drone has a maximum take-off weight of 8,255kg.It is capable of carrying multiple sensor payloads attached to its wing hard-point mountings while its internal weapons bay can carry precision mutations and large sensors up to 1,588kg. The total payload capacity of the aircraft is 2948kg. Its weapon payload includes Hellfire missiles, guided bomb unit (GBU)-12/49 laser-guided bombs, GBU-31 GBU-32, GBU-38 38 joint direct attack munitions (JDMA) and GBU-39 and GBU-16/48 bombs. The Predator C Avenger offers greater operational and transit speeds than Predator B aircraft. Powered by Pratt and Whitney PW545B turbofan engine, the combat drone is capable of reaching altitudes up to 50,000ft. It has a maximum speed of 400k and endurance of 20 hours. (Army, The world's top combat drones, 2019) See Figure 10-22.

Conclusions

There are five DE systems (DEW, Laser, Microwave, Particle Beams, Acoustic) which use the EMS to attack and defend against hostile UAS. Acoustic systems have the secondary advantage that their resonance frequencies may be used not only to knock out UASs but also characterize and identify friend or foe (IFF) UASs. All these EMO technologies have varying success rates against SWARMS.

Acoustical defenses show promise in they represent a two-for. Not only can they disrupt the MEMS with explosive sound at resonance frequencies, but every UAS has a unique acoustical signature. These acoustic signatures can be cataloged and used for challenge – response in an Identify Friend or Foe (IFF) algorithm.

The sampling of advanced attack capability UAV from around the world, at the end of this chapter *are targets that have the ability to fight back* – either with ISTAR, missiles, precision guided bombs (PGB) / (PGM) / missiles or EW countermeasures. They are able to identify the defender's transmitters. They can put a world of hurt on opposing forces.

Figure 10-22 Predator C Avenger

Source: (Staff, General Atomics Avenger, 2019)

Discussion Questions

- This chapter explores the use of acoustic countermeasures against UAS. The authors contend that every manufactured UAS has unique sound detection signatures. Further these can be libraried and used in a search algorithm to IFF the UAS group or SWARM. At the DoD 7th Annual Summit, (Nichols R. K., Hardening US Unmanned Systems Against Enemy Counter Measures, 2019) the author found that several contractors are actually doing this and building databases. BUT they refuse to share their data because it is proprietary. Assuming this situation cannot be changed, suggest two ways to get around this problem not involving legal actions. What type of research project would you propose to meet an 85% detection criteria that would suffice as an initial IFF database for evaluation?
- Along with attacking the MEMS gyroscopes to disable the UAS rotor, propose an experiment to use acoustic countermeasures

on the UAS internals, such as SCADA, payload, navigation, internal clocks, internal computer, battery, etc. Perhaps loud noise can disrupt additional UAS features?

- This chapter has discussed sound in the in the extended hearing ranges from 10 Hz to 20,000 Hz. Many UAS are designed for higher frequencies, i.e. ultrasonic and hypersonic. Propose an experiment to test sound disruption effects at the higher frequencies. (Drones, 2017) Quad Star Drones has some interesting "takes" on hypersonic flight and Mach 0.8 speeds.
- There was a fascinating story in the 4 November 2019 web-issue of *Popular Mechanics* about drones being launched from submarines. (Mizokami, 2019) See: https://hmg.h-cdn.co/videos/missle-rc-illustration-1572620289.mp4 The article is critical of carrier warfare and suggests that submarine launched drones would change the way carriers are deployed.

Assignment: read the article. Then you be the designer to tie it all together. How would you do it?

Much of the tech needed to develop drone-launching submarines—such as creating a large submersible or controlling drones at sea—has already been mastered. When someone ties it all together, we could see (or rather, not see) a naval event where carriers from both sides are totally underwater.

Now that you have it tied together and plan to bring this new form of warfare, now defend against it. What technologies would you use from this chapter?

REFERENCES

Adamy, D. -0. (2015). EW 104 EW *against a New Generation of Threats.* Boston: Artech House.

Adamy, D. (2001). EW 101 A *First Course in Electronic Warfare.* Boston, MA: Artech House.

Adamy, D. (2009). EW 103 *Tactical Battlefield Communications Electronic Warfare.* Boston, MA: Artech House.

Adamy, D. L. (2004). EW 102 A *Second Course in Electronic Warfare.* Boston: Artech House.

Adamy, D. L. (2015). EW 104 EW *Against a New Generation of Threats.* Boston: Artech House.

Adamy, D.-9. (1998, Jan). Lesson 4: the basic link for all EW functions. (electronic warfare)(EW Reference & Source Guide). *Journal of Electronic Defense, Jan 1998 Issue.*

Administrator. (2015, June 15). *Standing Wave and Fundamental Frequency.* Retrieved from Electronics Hub: https://www.electronicshub.org/?s=fundamental+frequency

Alford, L. (2000). Cyber Warfare: Protecting Military Systems. *Acquisition Review Quarterly.*

Angelov, P. (2012). *Sense and avoid in UAS research and applications.* Hoboken: NJ.

Army, U. (1992, November 23). US Army Field Manual FM 34-40-7. *Communications Jamming Handbook.*

Austin, R. (2010). *"Design for Stealth", Unmanned Aircraft Systems* UAVS *Design Development and Deployment.* New York: John Wiley and Sons.

Barker, W. (2003, August). SP 800-59 *Guidelines for Identifying an Information System as a National Security System.* Retrieved from NIST: https://csrc.nist.gov/publications/detail/sp/800-59/final

Barnhart, R. K. (2012). *Introduction to Unmanned Aircraft Systems.* New York: CRC Press.

Beason, D. (2005). *The E-Bomb: How America's new directed energy weapons will change the way future wars will be fought.* Cambridge, MA: Da Capo Press.

Beaudoin, L. e. (2011). Potential Threats of UAS Swarms and the Countermeasures Need. ECIW.

Boutros, D. (2015, May 15). *US Navy War College.* Retrieved from Operational Protection from Unmanned Aerial Systems: http://www.dtic.mil/dtic/tr/fulltext/u2/a621067.pdf

Brenner, J. (2011). *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare.* New York: Pilgrim Press.

Burch, D. (2015). *RADAR for Mariners*. New York: McGraw-Hill.

C4ISystems. (2013). *basics-of-information-operations.* Retrieved from Blogspot: http://c4isys.blogspot.com/2013/11/basics-of-information-operations-24.html

Carter, A. (2012, May 24). *EEWeb.* Retrieved from The Sound Intensity: https://www.eeweb.com/profile/andrew-carter/articles/the-sound-intensity

Chairman, U. (2012, March 23). Countering Air and Missile Threats, final coordination, JP 3-01. CJCS.

Clothier, R. (2017, April 02). *The Smart Skies Project: Enabling Technologies for UAS Operations in Non-segregated Airspace.* Retrieved from QUT ePrints: http://eprints.qut.edu.au/40465/3/40465.pdf

Clothier, R. F. (2010). *The Smart Skies Project: Enabling technologies for future airspace.* . Clothier, R.A., Frousheger, D., Wilson, M., (2010). The Smart Skies Project: Enabling technologies for future airspace. Australian Research Center for Aerospace Automation, Commonwealth Scientific and Industrial Research Organization, Boeing Research an. Australian Research Center for Aerospace Automation, Commonwealth Scientific and Industrial Research Organization.

Clothier, R. R. (2011). The Smart Skies project. *IEEE Aerospace and Electronic Systems Magazine.*

Collins-Dictionary. (2019, November 3). *Fluence Definition.* Retrieved from Collins Dictionary: https://www.collinsdictionary.com/us/dictionary/english/fluence

Commander Malte von Spreckelsen. (2018, January). *Electronic Warfare – The Forgotten Discipline:Why is the Refocus on this Traditional Warfare Area Key for Modern Conflict?* Retrieved from JAPCC Journal 27: https://www.japcc.org/electronic-warfare-the-forgotten-discipline/

DAU. (2018, July 2). *Cyber Table Top Guidebook.* Retrieved from DOD / DAU: https://www.dau.mil/cop/test/_layouts/15/WopiFrame.aspx?sourcedoc=/cop/test/

DAU%20Sponsored%20Documents/The%20DoD%20Cyber%20Table%20Top%20Guidebook%20v1.pdf&action=default&DefaultItemOpen=1

David H. Staelin, A. W. (1998). *Electromagnetic Waves*. Upper Saddle River, NJ: Prentice Hall.

Defence, P. (2014, May 7). *China's Pterodactyl drone*. Retrieved from defence.pk: https://defence.pk/pdf/threads/saudi-arabia-signs-deal-for-chinas-pterodactyl-drone.312761/

DoD. (2018). *Dictionary of Military Terms*. Retrieved from JCS.Mil: http://www.jcs.mil/doctrine/dod_dictionary/

DoD-01. (2018). *JP 1-02*. Retrieved from Department of Defense Dictionary of Military and Associated Terms: www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

DoD-02. (2018). *Information Operations (IO) in the United States*. Retrieved from JP 3-13 : http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf

DoD-03. (2015). *Unmanned Systems Roadmap 2013 to 2038*. Retrieved from DTIC: http://www.dtic.mil/dtic/tr/fulltext/u2/a592015.pdf

Drones, Q. S. (2017, July 11). *quadcopters-have-hit-the-sound-barrier/*. Retrieved from quadstardrones.com: https://quadstardrones.com/2017/07/11/quadcopters-have-hit-the-sound-barrier/

DTRA. (2019, October 18). Private Communication re Aviation Vulnerabilities. (Nichols, Interviewer) Retrieved from https://www.dtra.mil/

Editor. (2012, April 22). *RT Question More*. Retrieved from Iran starts cloning of American spy drone: https://www.rt.com/news/iran-spy-drone-copy-667/

EIA. (2019, June 20). *The Strait of Hormuz is the world's most important oil transit chokepoint*. Retrieved from EIA – US Energy Information Administration: https://www.eia.gov/todayinenergy/detail.php?id=39932

Entokey, a. G. (2019, May 16). *entokey.com/acoustics-and-sound-measurement/*. Retrieved from entokey.com/acoustics-and-sound-measurement/: https://entokey.com/acoustics-and-sound-measurement/

Eshel, T. (2019, September 14). *AFRL to Test a Drone-Swarm Killer HPM.* Retrieved from Defense Update: https://defense-update.com/20190923_hpm.html

FAA. (2018, February 1). *Part 107 Rule for sUAS.* Retrieved from Fly under the Special Rule for Model Aircraft: https://www.faa.gov/uas/getting_started/model_aircraft/

Filbert, F. &. (2014, (July – August). *Joint Counter Low, Slow, Small Unmanned Aircraft Systems Test. Fires PB644-14, no 4.* Washington: DoD.

Fitts, R. (1980). *The Strategy of Electromagnetic Conflict.* Los Altos, CA: Peninsula Publishing.

Fletcher, H. a. (1933). Loudness, its definition, measurement and calculation. *Journal of the Acoustical Society of America* , 5, 82-108 .

Foley, W. S. (March, 1979). Ancient Catapults. *Scientific American,* 240, 150.

Forrest, J. C. (2016). *Practical Aviation Security: Predicting and Preventing the Future Threats.* Cambridge, MA: BH.

Gallagher, S. (2019, September 16). *Missiles and drones that hit Saudi oil fields: Made in Iran, but fired by whom?* Retrieved from Arstechnica.com: https://arstechnica.com/tech-policy/2019/09/missiles-and-drones-that-hit-saudi-oil-fields-made-in-iran-but-fired-by-whom/

Garcia, M. (2006). *Vulnerability Assessment of Physical Protection Systems.* Albuquerque: Sandia National Laboratories,BH.

Gelfand. (2004). *"Physical Concepts", Hearing an Introduction to Psychological and Physiological Acoustics, 4th ed.* New York City.

Gelfand, S. A. (2009). *Essentials of Audiology, 3rd Edition.* Stuttgart, DE: Thieme.

Glasstone, S. &. (1977). The Effects of Nuclear Weapons, 3rd Edition. In S. &. Glasstone, *Chapter V, Figures* 5.20, 5.22 *&* 5.23. Washington, DC : UGPO.

Greenburg, H. (2015). *Hackers Remotely Kill a Jeep on the Highway—With Me in It.* Retrieved from Wired :

https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Halsam, C. M.-S. (1982). *Small Arms and Cannons.* Oxford: Brassey's Publishers.

Hartman, K. a. (2013). The Vulnerability of UAVs to Cyber Attacks – An Approach to the Risk Assessment. 2013 5*th International Conference on Cyber Conflict* . Tallin: NATO CCD COE Publications.

Heinman, C. (2019). *Hearing Loss Tests Patrient D v*-105. Carlisle, PA: Brown Optical Hearing Aid Service.

Horowitz, M. C. (2014). *Droning On: Explaining the Proliferation of Unmanned Aerial Vehicles.* University of Pennsylvania and Texas A&M Universities. University of Pennsylvania and Texas A&M Universities.

Howard, C. (2019, June 21). *What is the Strait of Hormuz, where Iran shot down* US *Navy drone*? Retrieved from Fox News: https://www.foxnews.com/world/whats-the-strait-of-hormuz-iran-shot-us-navy-drone

Hubbard, R. K. (1998). *Boater's Bowditch.* Camden, MA: International Marine.

ITU. (2019, July 19). *ARTICLE 2 – Nomenclature – Section I – Frequency and Wavelenght Bands.* Retrieved from ITU Radio Communication Edition 2008: https://web.archive.org/web/20111001005059/http://life.itu.int/radioclub/rr/art02.htm

Jackson, B. (2017, August 7). *UCF and UT win $400k for micro 3D printed light-bending research.* Retrieved from 3dprintingindustry.com/news: https://3dprintingindustry.com/news/ucf-ut-win-400k-micro-3d-printed-light-bending-research-119864/

1. Neubauer, D. F. (2015). *Unmanned Aircraft Systems at Airports: A Primer.* Washington: ACRP.

Kania, E. (2017, July 6). Swarms at War: Chinese Advances in Swarm Intelligence. China Brief Volume: 17 Issue 9. *China Brief Volume: 17 Issue 9.*

Kaye, T. a. (2001, September 30). ACHIEVING INFORMATION DOMINANCE:. Retrieved from DODCCRP-Space and Naval Warfare Systems Center San Diego: http://www.dodccrp.org/events/2002_CCRTS/Tracks/pdf/026.PDF

Kilman, D. &. (2003). *Framework for SCADA Security Policy.* Albuquerque, NM: Sandia National Laboratories. Retrieved from Energy.gov: https://www.energy.gov/sites/prod/files/Framework%20for%20SCADA%20Security%20Policy.pdf

Kim, A. G. (2012, June). *Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles.* Retrieved from Infotech@Aerospace.com: https://www.researchgate.net/publication/268571174_Cyber_Attack_Vulnerabilities_Analysis_for_Unmanned_Aerial_Vehicles

Kirk, J. (2015, August 5). *sounds-can-knock-drones-sky.* Retrieved from www.computerworld.com.au/article/581231: https://www.computerworld.com.au/article/581231/sounds-can-knock-drones-sky/

Lister, T. (2019, September 16). *Attack is a game-changer in Gulf confrontation.* Retrieved from CNN: https://www.cnn.com/middleeast/live-news/saudi-oil-attack-dle-intl/h_3e647100fa720927c962d7643472b12d

Liteye. (2018, August 25). *AUDS.* Retrieved from Liteye Corporation: http://liteye.com/products/counter-uas/auds/

LRAD. (2019, May 189). *LRAD 450XL Datasheet.* Retrieved from LRADX: http://www.lradx.com/wp-context/uploads/2015/05/LRAD_datasheet_450XL.pdf

LRAD Corporation. (2019, October 18). *Product sheet LRADS 1000x.* Retrieved from LRAD Corporation : https://lradx.com/lrad_products/lrad-1000xi/

Marshall, D. M. (2016). *Introduction to Unmanned Aircraft Systems, 2nd Edition.* New York: CRC Press.

Merriam-Webster. (2019, May 17). Merriam-Webster Online Dictionary.

Merrick, K. (2016). Future Internet. 10.3390/fi8030034 *Review*, 8(3), p. 34.

Micro Denshi Co.,Ltd. (2019, November 3). *Introduction to Microwaves.* Retrieved from Microdenshi company: https://www.microdenshi.co.jp/en/microwave/

Military & Aerospace Electronics. (2019, October 14). *Air Force researchers to test high-power microwave weapon to destroy or disable swarms of unmanned aircraft.* Retrieved from Military & Aerospace Electronics: https://www.militaryaerospace.com/unmanned/article/14068535/high-power-microwave-unmanned-aerial-vehicle-uav-swarms

Moir, I. &. (2006). *Military Avionics Systems.* New York City, NY: Wiley.

Moir, I. a. (2006). *Military Avionics Systems.* New York: Wiley Aerospace Series.

Monahan, K. (2004). *The Radar Book: Effective Navigation and Collision Avoidance.* Anacortes, WA: Fineedge Publications.

MORS. (2018). *Military Operations Research Society* . Retrieved from http://www.mors.org/meetings/oa_definition.htm

Myer, G. (2013, May-June). *Danger Close Definition.* Retrieved from US Army Magazine: www.benning.army.mil/infantry/magazine/issues/2013/May-June/Myer.html

NASA. (2018). *Unmanned Aircraft Systems (UAS) Integration in the National Airspace System (NAS) Project.* Retrieved from NASA: https://www.nasa.gov/feature/autonomous-systems

National Academies of Sciences, E. a. (2018, November 3). *Opportunities in Intense Ultrafast Lasers: Reaching for the Brightest Light.* Washington: The National Academies Press. doi: https://doi.org/10.17226/24939

National Archives. (2019, August 25). ANO 2016, UK *Statutory Instruments* 2016 # 675. Retrieved from legislation.gov.uk: http://www.legislation.gov.uk/uksi/2016/765/contents/made

Naval Technology Team. (2019, June 11). *feature-the-top-10-maritime-patrol-aircraft/.* Retrieved from https://www.naval-technology.com: https://www.naval-technology.com/features/feature-the-top-10-maritime-patrol-aircraft/

Naval Technology Team. (2019, October 18). *MQ-4C Triton Broad Area Maritime Surveillance (*BAMS) UAS. Retrieved from Naval Technology: https://www.naval-technology.com/projects/mq-4c-triton-bams-uas-us/

Nichols, R. K. (1996). *Classical Cryptography Course, Volume I.* Laguna Hills, CA: Aegean Park Press.

Nichols, R. K. (1999). *The ICSA Guide to Cryptography.* New York, NY: McGraw Hill.

Nichols, R. K. (2008, September 05). Counterintelligence & Sensitive Compartmented Information Facility . (SCIF) *Needs – Talking Points.*

Nichols, R. K. (2019, March 14). Hardening US Unmanned Systems Against Enemy Counter Measures. *7th Annual Unmanned Systems Summit.* Alaxandria, VA, USA: PPTX presentation , self.

Nichols, R. K., Mumm, H. C., Lonstein, W. D., Ryan, J. J., Carter, C., & and Hood, J.-P. (2019). *Unmanned Aircraft Systems in the Cyber Domain.* Manahattan, KS: New Prairie Press. Retrieved from https://newprairiepress.org/ebooks/27/

Nichols, R. K., Mumm, H. C., Lonstein, W. D., Ryan, J. J., Carter, C., & and Hood, J.-P. (2019). *Unmanned Aircraft Systems in the Cyber Domain, 2nd Edition.* Manhattan, KS: NPP eBooks. 27. Retrieved from www.newprairiepress.org/ebooks/27

Nichols, R. (Nov 28-30, 2006). Cyber Terrorism, Critical Infrastructure, & SCADA Presentation. In R. Nichols (Ed.), *Defense Threat Reduction Agency Conference.* Shirlington VA: Utica College, Utica NY.

Nichols, R.-0. (2016, March 29). NCIE UAS SAA Final Rev 4. 2016 INFOWARCON *conference presentation April* 4-7, Nichols, R.K. et. al. (3-29-2016) Presentation to INFOWARCON April 4-7 on NCIE UAS SAA Final Rev 4, presented to 2016 INFOWARCON conference, Memphis TN. Available as PPTx presentation download from author or in CANVAS. Memphis, TN, USA: INFOWARCON16.

Nielsen, P. E. (2012). *Effects of Directed Energy Weapons*. Middletown, DE: CreateSpace Independent Publishing Platform.

Norbiton, R. H. (Oct 2019). *UK Counter-Unmanned Aircraft Strategy*. London: APS Group on behalf of the Controller of Her Magesty's Stationary Office. Retrieved from www.gov.uk/official-documents

Norman, G. (2019, November 1). *California police rip drone pilot as device gets in way of wildfire relief efforts*. Retrieved from www.Foxnews.com: https://www.foxnews.com/us/california-drone-pilot-wildfire-relief

NTSB. (2009, September 16). *National SCADA testbed Documents and Media*. Retrieved from National SCADA Testbed Fact Sheet: https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/NSTB_Fact_Sheet_FINAL_09-16-09.pdf

Osborn, K. (2019, October 15). *Swarm Hell: Can the U.S. Army Stop Hundreds of Drones Armed with Explosives*? Retrieved from National Interest: https://nationalinterest.org/blog/buzz/swarm-hell-can-us-army-stop-hundreds-drones-armed-explosives-88206

Pettit, R. (1982). *ECM and ECCM Techniques for Digital Communication Systems*. Belmont, CA: Lifetime Learning Publications .

Pierson. (2019, May 16). *tuning-fork-waves-sound*. Retrieved from airfreshener.club – Pierson Education: https://airfreshener.club/quotes/tuning-fork-waves-sound.html

radiotechnika – Republic of Belarus. (2019, October 20). *Computer modeling of sophisticated radio electronic systems*. Retrieved from http://radiotechnika.by/: http://radiotechnika.by/en/products/radar/computer_model_difficult_systems/

Randall K. Nichols, D. J. (2000). *Defending your digital Assets against hackers, crackers , spies and thieves*. New York, NY: RSA Press & McGraw-Hill.

Randall K. Nichols, D. J. (2000). *Defending Your Digital Assets against Hackers, Crackers, Spies and Thieves*. New York: RSA Press.

Rani, C. M. (2015). Security of unmanned aerial vehicle systems against cyber-physical attacks. *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology.*

Raytheon. (2019, October 23). *Raytheon announces delivery of first laser counter-*UAS *system to U.S. Air Force.* Retrieved from Defense Blog: https://defence-blog.com/news/raytheon-announces-delivery-of-first-laser-counter-uas-system-to-u-s-air-force.html

Rogoway, T. (2018, September 5). *Global Hawk.* Retrieved from www.thedrive.com: https://www.thedrive.com/the-war-zone/23383/exclusive-u-s-air-force-rq-4-global-hawk-drone-crashed-off-spain-last-june

Rosen, S. (2011). *Signals and Systems for Speech and Hearing (2nd ed.).* New York City: BRILL. p. 163.

Said Emre Alper, Y. T. (December 2008). ACompact Angular Rate Sensor System Using a Fully Decoupled Silicon-on-Glass MEMS Gyroscope. JOURNAL OF MICROELECTROMECHANICAL SYSTEMS, VOL. 17, NO. 6.

Schneiner, B. (1996). *Cryptography.* New York, NY: John Wiley.

Shapiro, J. (2006, February 14). *Slideplayer.com.* Retrieved from Cybersecurity: http://slideplayer.com/slide/4545982/

Sheena McKenzie, M. W. (2019, September 17). *Saudi attacks send oil prices soaring.* Retrieved from CNN: https://www.cnn.com/middleeast/live-news/saudi-oil-attack-dle-intl/h_1ab7e8469e98525f887c3a4e588dde8a

Signia. (2019, May 16). *Signia Hearing Aids.* Retrieved from Signia Hearing Aids – Hear across America: www.signiausa.com

Singer, P. W. (2010, February 25). Will Foreign Drones One Day attack the US? . N*ewsweek.*

slideshare.net. (2019, May 16). *ProudParas/sound-waves-loudness-and-intensity, slide* 12. Retrieved from slideshare.net: https://www.slideshare.net/ProudParas/sound-waves-loudness-and-intensity

Sood A.K. & Enbody, R. (2014, December 19). *https://www.georgetownjournalofinternau-s-military-defense-systems-the-anatomy-of-cyber-espionage-by-chinese-hackers.* Retrieved from georgetownjournalofinternationalaffairs.org/

online-edition: https://www.georgetownjournalofinternationalaffairs.org/online-edition/u-s-military-defense-systems-the-anatomy-of-cyber-espionage-by-chinese-hackers

Staff. (2016, April 17). *Equal Loudness Contours*. Retrieved from Gutenberg Organization: http://central.gutenberg.org/article/WHEBN0001046687/Equal-loudness%20contour

Stathopoulos, C. J. (2018). *Challenges of Future SEAD Operations: An Insight into SEAD in 20 Years*. Retrieved from JAPCC | Journal Edition 27 | 2018 | Transformation & Capabilities: https://www.japcc.org/wp-content/uploads/JAPCC_J27_screen.pdf

Stratfor. (2019, October 20). *strait-of-hormuz-chokepoints*. Retrieved from https://www.stratfor.com: https://www.stratfor.com/sites/default/files/styles/wv_small/public/strait-of-hormuz-chokepoints.jpg?itok=xSgx6Hhi

Studios, D. D. (2017). Boaters Ref. USA.

Toomay, J. (1982). *RADAR for the Non – Specialist. London; Lifetime Learning Publications*. London: Lifetime Learning Publications.

Transport, S. o. (2019). *future-of-drones-in-uk-consultation-response-web.pdf*. Retrieved from assets.publishing.service.gov.uk/government: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/771673/future-of-drones-in-uk-consultation-response-web.pdf

TRS. (2018, July 10). *Tontechnic-Rechner-Sengpielaudio Calculator*. Retrieved from Tontechnic-Rechner-Sengpielaudio (TRS): www.sengspielaudio.com/calculator-wavelength.htm

TRS, S. (2018, July 10). *Tontechnic-Rechner-Sengpielaudio*. Retrieved from Tontechnic-Rechner-Sengpielaudio Calculator: www.sengspielaudio.com/calculator-wavelength.htm

Uni-wuppertal. (2019, May 15). *Inverse Square Law, General*. Retrieved from hydrogen.physik.uni-wuppertal.de/hyperphysics/: http://hydrogen.physik.uni-wuppertal.de/hyperphysics/hyperphysics/hbase/forces/isq.html

Usenix.org. (2019, 6 9). *MEMS, Drones, & Sound Sourcing.* Retrieved from Usenix.org: www.usenix.org

Vernard Foley, G. P. (January, 1985). The Crossbow. *Scientific American*, 252, 104.

Weise, E. (2017, August 23). *could-hackers-behind-u-s-navy-collisions.* Retrieved from USATODAY: https://www.ruidosonews.com/story/tech/news/2017/08/23/could-hackers-behind-u-s-navy-collisions/594107001/

Wiki-E. (2018, August 26). *Equal Loudness Contours.* Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Equal-loudness_contour

Wikipedia. (2018, August 26). *Human Hearing Range.* Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Hearing_range

Wikipedia. (2019, November 3). *Collimated Definition.* Retrieved from Wikipedia: https://www.google.com/search?client=firefox-b-1-d&q=collimated+definition

Wikipedia. (2019, November 3). *Plasma Weapons.* Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Plasma_weapon

Wiley, R. G. (1993). *Electronic Intelligence: The Analysis of Radar Signals, 2nd ed.* Norwood, MA: Artech House.

Wilson, M. (2012). The Use of Low-Cost Mobile Radar Systems for Small UAS Sense and Avoid. *Sense and Avoid in UAS Research and Applications.*

Yan. (2017, December 23). *China's commercial drone market to top 9 bln USD by 2020.* Retrieved from Xinhuanet: http://www.xinhuanet.com/english/2017-12/23/c_136847826.htm

Yu, X. &. (2015). Sense and avoid technologies with applications to unmanned aircraft systems: Review and prospects. *Progress in Aerospace Sciences*, 74, 152-166.

Yunmonk Son, H. S. (2015, August 12-14). Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors. *Proc. 24th Usenix Security Symposium.* Washington, DC: USENIX. Retrieved from https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/son

Zaharia, M. D. (2012). *Discretized Streams: An Efficient and Fault-*

Tolerant Model for. Retrieved from UNIX Org: https://www.usenix.org/system/files/conference/hotcloud12/hotcloud12-final28.pdf

Zetter, K. (2014, November 3). *An Unprecedented Look at Stuxnet, the World's First Digital Weapon.* Retrieved from Wired: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

Zwijnwenburg, W. (2014, October 8). *ZwijnwenbDrone-tocracy? Mapping the Proliferation of Unmanned Systems.* Retrieved from Sustainable Security.org.

Appendix 10-1: Standard Acoustic Principal Physical Properties

Quantity	Formula	MKS (SI)Units	Cgs Units	Comments	English Units
Mass (M)	M	kilogram (kg)	gram (g)	1kg = 103 g 1kg = 2.2046 lbs	pounds (lbs)
Time (t)	t	seconds, (s)	s		s
Area (A)	A	m2	cm2	1 m2 = 104 cm2	ft2
Displacement (d)	d	meter (m)	centimeter (cm)	1m = 102 cm	ft
Velocity (v)	v = d/t	m/s	cm/s	1 m/s = 102 cm/s	ft/s
Acceleration (a)	A = v/t	m/s2	cm/s2	1 m/s2 = 102 cm/s2	ft/s2
Force (F)	F = MA = Mv/t Mv = Momentum	kg x m/ s2 newton (N)	g x cm2 dyne	1N = 105 dynes	1lbf = 1 lb x 32.174049 ft -lbs /s2 = 9.80665 m/s2
Pressure (p)	p = F/ A	N /m2 Pascal (Pa)	dynes /cm2 microbar (µbar)	20 µPa = 2 x 10-5 N/ m2 reference value	Psi = lbf /in2 1 N/m2 = 0.000145 psi
Work (W)	W =Fd	N x m Joule	dyne x cm erg	1 j = 107 erg/s Energy -capability to do Work. Potential energy for a body at rest and kinetic energy for a body in motion.	BTU [British Thermal Unit] 1 BTU = 1055.056 joules

Power (P)	P = W/t = Fd/t =Fv	Joules/s watt (w)	erg/s watt (w)	1 w = 1 J/s = 107 erg/s	1 watt = 3.412 BTU/hr
Intensity (I)	I = P/A I = P / 4?r2 Based on sphere radius	w/m2	w/cm2	10-12 *w/m2* *reference value*	

Sources: (Entokey, 2019) & (Studios, 2017) & (Nielsen, 2012)

Appendix 10-2 LRAD 1000X, Source: (LRAD Corporation, 2019)

Communicate Even Further with Longer Range AHD

The LRAD 1000Xi is a power efficient, long distance communication system designed for applications ranging from critical infrastructure protection to territorial water, border and port security, and large vessel and vehicle installations.

Featuring a rugged carbon fiber emitter head integrated with electronics and amplification, the LRAD 1000Xi comes standard with an MP3 Control Module for playing recorded messages and an all-weather microphone for live broadcasts. The MP3 Control module also enables remote operation of the device from safe locations.

Superior voice intelligibility and an extended frequency range ensure broadcasts are clearly heard and understood over wind, engine and background noise. The LRAD 1000Xi provides a long-range communications capability to issue authoritative voice commands and attention-commanding deterrent tones to determine intent, safely enhance response capabilities, modify behavior, and scale the use of force if necessary.

Features

1. Rugged, military tested construction
2. Low power requirements
3. All-weather use

4. Easy to use
5. Increased coverage with single operator
6. Safer alternative to non-lethal deterrent measures
7. HD Camera (optional)

Directionality, Power Efficiency & Range

1. Highly intelligible communication up to 3,000 meters (1.864 miles)
2. Safely communicates beyond standoff distances to determine intent
3. Variable beam width for extended coverage
4. Clear, long range, directional communication
5. Establishes instant acoustic standoff perimeter

LRAD 1000Xi Specifications

Acoustic Performance

- Maximum Continuous Output: 153 dB SPL @ 1 meter, A-weighted
- Sound Projection +/- 15° at 1 kHz
- Communications Range: Highly intelligible voice messages over distances up to 3,000 meters; max range of 1,250 meters over 88 dB of background noise.
  6+ dB above background noise is based on field trials conducted by independent sources.

Environmental Performance

- Hot Operating Temperature: MIL-STD-810G, Method 501.5, Procedure II, Design type Hot, 60°C
- Cold Operating Temperature: MIL-STD-810G, Method 502.5, Procedure II, Design type Basic Cold, -33°C
- Hot Storage Temperature: MIL-STD-810G, Method 501.5, Procedure I, 70°C

- Cold Storage Temperature: MIL-STD-810G, Method 502.5, Procedure I, -40°C
- Operating Humidity: MIL-STD 810G, Method 507.5, Procedure II – Aggravated Cycle
- Rain: MIL-STD-810G, Method 506.5, Procedure I, Blowing rain
- Salt Fog: MIL-STD-810G, Method 509.5
- Shipboard Vibration: MIL-STD-167-1A
- Shipboard Shock: MIL-S-901D, Class I, Shock grade B
- Random Vibration: MIL-STD-810G, Method 514.6, Wheeled vehicles
- SRS Shock: MIL-STD-810G, Method 516.6, Procedure I, (Functional shock)

Tested by National Technical Systems (NTS) *following* MIL-STD-810G, MIL-STD-167-1A & MIL-S-901D

Mechanical

- Dimensions: 36" ACOUSTIC PERFORMANCE x 40" ACOUSTIC PERFORMANCE x 13" D (91cm x 102cm x 33cm)
- Weight: 87 lbs. without accessories (39.4kg)
- Construction: Molded low smoke composite, 6061 Aluminum, 316 Stainless hardware

Electrical Requirements

- Typical Power Consumption: 720 Watts (With tone)
- Normal Power Consumption: 190 Watts (With voice content)
- Power Input: 90-260VAC 50/60Hz Typical Power with warning tone. Normal Power Consumption: with voice content, sound projection is wide and voice boost is off.

Safety

MIL-STD-1474D

MIL-STD-1474D standard establishes acoustical noise limits and prescribes testing requirements and measurement techniques for determining conformance to the noise limits specified therein.

Electromagnetic Compatibility (EMC)

FCC Part 15 class A radiated emissions, CE

Requirements for the control of electromagnetic interference characteristics of subsystems and equipment.

Endnotes

[1] "Drone" in this document refers to small unmanned aircraft, remotely piloted or autonomous, fixed-wing or rotary blade, controlled remotely or use satellite navigation systems, or RTF or tethered or RC models.

[2] In 2018, the Home Office ran a public consultation, Stop and search: extending police powers to cover offences relating to unmanned aircraft (drones), laser pointers, and corrosive substances. The result was published in 2019

[3] A fascinating study by NATO on *Transforming Joint Air and Space Power* via The Journal of the Joint Air Power Competence Center (JAPCC) available for download at: https://www.japcc.org/wp-content/uploads/JAPCC_J27_screen.pdf

[4] In Chapter 14: Exposing UAS Vulnerabilities via Electronic Warfare (EW) and Countering with Low Probability Intercept Signals (LPI), EW, CYBER and LPI in modern communications systems is covered in detail. (Nichols, et al., Unmanned Aircraft Systems in the Cyber Domain, 2019)

[5] MC 64/11, 4 Jul. 2018

[6] Student assignment end of Chapter 9.

[7] SCADA systems, functions, configurations, and their vulnerabilities are covered in detail in (Nichols, et al., Unmanned Aircraft Systems in the Cyber Domain, 2019) Chapter 3: Understanding Hostile Use and Cyber-Vulnerabilities of UAS:

Components, Autonomy v Automation, Sensors, SAA, SCADA and Cyber Attack Taxonomy. The purpose of this textbook is to move forward not rehash materials previously presented. Some Tables in Chapter 3 have been republished here for convenience. The reader is reminded that *UNMANNED AIRCRAFT SYSTEMS IN THE CYBER DOMAIN: PROTECTING USA'S ADVANCED AIR ASSETS, 2nd Edition* by Nichols, R. K., Ryan, J., J.C.H., Mumm, H.C., Lonstein, W.D., Carter, C., Hood, J.P. is available for **FREE** at www.newprairiepress.org/ebooks/27

[8] In the authors' ancient textbook (Nichols R. K., The ICSA Guide to Cryptography, 1999) *Cryptology* is the study of creating codes and ciphers (*cryptography*) and decoding or deciphering codes and ciphers (*cryptanalysis*) when the system is not known. There are far better books available. Consider the classic by guru and one-time competitor, Bruce Schneier, simply entitled *Cryptography*. (Schneiner, 1996)

[9] The general term for the art and science of concealment ciphers is *steganography*. This includes null, ciphers and image / pixel deceptions (hiding in plain sight or in a massive amount of storage) (Randall K. Nichols D. J., 2000).

[10] If the reader is really interested in pain and all things Maxwell (James Clerk), consider the textbook Electromagnetic Waves by Staelin, et.al. (David H. Staelin, 1998). Prepare for hours of math and difficult reading.

[11]Fluence – particle density or energy density, used to describe the output of a radiation field or of a laser beam (Collins-Dictionary, 2019)

[12] Think skeet shooting.

[13] Laser stands for Light amplification through simulated emission of radiation.

[14] A collimated beam of light or other electromagnetic radiation has parallel rays, and therefore will spread minimally as it propagates. A perfectly collimated light beam, with no divergence, would not disperse with distance. … Perfectly collimated light is sometimes said to be focused at infinity. (Wikipedia, Collimated Definition, 2019)

[15] This effect is referred to as *aerosols*.

[16] Plasma weapons are very cool and are more sci-fi than reality, certainly against UAS systems. A plasma weapon is a type of" ray gun" that fires a stream, bolt(s), pulse or toroid of plasma (i.e. very hot, very energetic excited matter). The primary damage mechanism of these fictional weapons is usually thermal transfer; it typically causes serious burns, and often immediate death of living creatures, and melts or evaporates other materials. Fictional plasma weapons are often visually analogous to real-life plasma torches that cut into materials for industrial use purposes; however, said torches currently only produce a plasma jet of several inches at most. (Wikipedia, Plasma Weapons, 2019) Amazon sells a Star Wars Nerf Captain Plasma Blaster for a mere $34.57 +tax and shipping. Six-year old's can now melt down a droid.

[17] Aside from author's comments in note 19, the ignition of plasmas at a target surface, and their subsequent propagation as detonation or combustion waves, can greatly enhance the thermal and mechanical coupling of a laser to a target, either in a vacuum or air.

[18] Laser material processing is now a major component of the manufacturing process. Lasers accomplish tasks ranging from heating for hardening, melting for welding and cladding, and the removal of material for drilling and cutting. Typical intensities required for such tasks include heat treating at 103 – 104 W/cm2, welding and cladding at 105 – 106 W/cm2, and material removal 107 – 109 W/cm2 for drilling, cutting, and milling. (National Academies of Sciences, 2018)

[19] These conclusions may be big jump from real earth to atmosphere. A better picture of the thermal, mechanical damage, stimulated Rama scattering (SRS), vaporization, melting as a function of intensity and pulse width is provided by (Nielsen, 2012) in Chapter 3, p 191, Figure 3-76. No matter how we dissect the laser weapon use concepts, UASs are not cost-effective targets for this cool technology.

[20] Relativistic velocities – Velocities approaching speed of light.

[21] Bremsstrahlung -radiation loss of energy induced by the acceleration of particles they suffer in collisions in the PB. (Nielsen, 2012)

[22] Another related chapter was *Chapter 8: Designing UAS Systems for Stealth.* (Nichols, *et al.*, *Unmanned Aircraft Systems in the Cyber Domain*, *2nd Edition*, 2019)

[23] Refer to Appendix 10-1 for standard acoustical properties and units.

[24] https://lradx.com/lrad_products/lrad-1000xi/

[25] Use the bottom of the page converter. Basis: Speed of sound c = λ × f = 343 m/s at 20°C} for 16 m L = 21.4375Hz. This compares to the Austin value of 20 Hz. For the 2 cm = 0.02 m, the resulting valued for f = 17650 Hz. This is above the 16,000 Hz limit from Austin. This might be due to the 20-degree Celsius basis difference. This tells the UAS designer that the upper end of noise – Stealth acceptability 17,150 Hz.

[26] "An equal-loudness contour is a measure of sound pressure (Db SPL) over the EMS spectrum, for which a listener perceives a constant loudness when presented with pure steady tones. The unit of measurement for loudness levels is the phon and is arrived at by reference to equal-loudness contours. Two sine waves of differing frequencies are said to have equal-loudness level measured in

phons if they are perceived as equally loud by the average young person without significant hearing impairment." (Staff, Equal Loudness Contours, 2016)

[27] "Four important relationships to note are that power is equal to pressure squared, P = p2, pressure is equal to the square root of power, p = √ P, intensity is proportional to pressured squared,
I ≈ p2 and pressure is proportional to intensity, p ≈ √I. This makes it easy to convert between sound intensity and sound pressure." (Entokey, 2019) These relations yield a few more to relate sound pressure, sound intensity and distance r. Given to pressures p1 and p2 at distance r1 and r2, they are proportional: p2 / p1 = r1 / r2; and factoring in intensities at I1 and I2, gives I2 / I1 = (r1 /r2)2. Finally, r2 / r1 = p2 / p1 = √I1 / I2. (TRS S. , 2018)

[28] Decibels (Adamy D. , 2001) (Gelfand S. A., 2009) Sound magnitudes, intensities, and pressures vary over an enormous range. We use decibels (dB) to express sound values. Decibels takes advantages of ratios and logarithms. Ratios are used so that physical magnitudes can be stated in relation to a reference value that has meaning to us. The reference point chosen is the softest sound that can be heard by normal people. The reference value has an intensity of 10-12 w/m2 (10-16 w/cm2). In terms of sound pressure, the reference value is: 2 x 10-5 N/m2 or 20 µPa (2 x 10-4 dynes/ cm2). An interesting Geek bar bet is what is the logarithm of all 2:1 ratios, 8:4, 20, 20:10, 100:50, etc.? Even though the distance between absolute numbers gets wider, 1,4,10, 50…, the logarithms of the 2:1 ratios are the same at 0.3. Another interesting factoid about ratios is the units generally cancel out.

The general decibel formula in terms of power level (PL) is as follows (Gelfand, 2004):

$$\mathbf{PL = 10 \log P / Po}$$

Equation 10-4

Where P = power of the sound measured, and Po is the reference power to be compared.

The general decibel formula in terms of power level (IL) is as follows (Gelfand, 2004):

$$\mathbf{IL = 10 \log I / Io}$$

Equation 10-5

Where I = intensity of the sound measured, and Io is the reference intensity to be compared. Io is given as 10-12 w/m2 .

The general decibel formula for sound pressure level (SPL) is obtained by replacing all of the intensity values with the corresponding values of pressure squared because (I ≈ p2).

$$\mathbf{SPL = 10 \log p2 / po2}$$

Equation 10-6

Where p is the measured sound pressure (in N/m2) and po is the reference sound pressure of

2 x 10-5 N/m2 . A more convenient form of this equation recognizes that log x2 = 2 log x. (Gelfand, 2004)

$$\mathbf{SPL = 20 \log p / po.}$$

Equation 10-7

Equation 10-7 is the common formula for SPL. A couple of observations a positive decibel value means that the sound pressure level is greater than the reference. The decibel value of the reference is 0 because reference value / reference value = 1 and 10 log 1 = 0. This does not mean no sound; it just means the sound measured is equal to the reference point. A negative value of decibels means that the sound magnitude is lower than the reference. (Gelfand S. A., 2009)

[29] It is left to the reader to obtain any standard trigonometry text to see all the parameters of the well-known sine wave.

[30] The formula for the string's resonant frequency Fo is:

$$\mathbf{Fo = 1 / 2L \; x \; \sqrt{T} \; /M}$$

Equation 10-8

Where Fo is resonance frequency in Hz, T is Tension, M is Mass, $L = \lambda /2$ and $f = c / \lambda$ and c = speed of sound. L = length of the string. (Gelfand, 2004) The strings lowest resonant frequency is $f = c / 2 L$ but Eq 10-8 considers that the speed of sound is different for a vibrating string than it is for air.

[31] Author's note although not specified in (Yunmonk Son, 2015), according to chapter author research and experimentation, the frequencies turn out to be the resonance frequencies. So agrees Dr. Kim at KAIST. "You would think that the gyroscopes used in unmanned aircraft systems (UAS) would have been designed to have resonant frequencies above the audible spectrum – i.e., above 20 kHz – but Kim and his team found that some have not." (Yunmonk Son, 2015) In the case of a gyroscope, "you can get it to spit out very strange outputs, as researcher Yongdae Kim, a professor in the electrical engineering department of the Korea Advanced Institute of Science and Technology (KAIST), told ComputerWorld" (Kirk, 2015) An example of resonance frequency and breaking glass can be found on youtu.be at https://youtu.be/BE827gwnnk4

Chapter 11: Thinking Like the Enemy: Seams in the Zone

W.D. LONSTEIN

Student Learning Objectives

The student will gain knowledge of the balance between effective C-UAS strategy and the many ways that technological and non-technological attack vectors can be implemented to defeat even the most robust Counter Unmanned Aircraft Systems ("C-UAS") tactics and strategies. Designing and new technology to respond to and counteract new, and rapidly developing technologies presents a daunting challenge. The C-UAS student must recognize that they are placed at an inherent disadvantage if only by the nature of their mission, responding to and addressing known and unknown threats.

Students Will Be Able To:

Understand the challenges confronting those who research, design and implement C-UAS systems, tactics, and strategies.

Acquire a historical understanding of C-UAS systems, their strengths, weaknesses, and lessons learned from prior successes and failures.

Describe how to "think like the enemy" and incorporate the thought process in the development of C-UAS Technology and strategy.

Understand the importance of ensuring that the physical security of C-UAS systems, personnel and data is often the first step in an attacker's playbook.

Develop a healthy skepticism of new technologies that claim to be able to address most or all threats posed to the public, assets, and personnel by Unmanned Systems.

Establish as a foundational underpinning of any C-UAS analysis that every technology or strategy has inherent vulnerabilities and so must have robust and rapid failure response.

Preliminary Statement

It is assumed those who may read this chapter do so with the intent of learning to benefit not harm upon innocent citizens and lawful combatants engaged in conflict under the modern rules of warfare. Drone and other unmanned automated technology provides a vehicle to weaponize payloads once thought impossible to transport and efficiently disperse upon targets. A delicate balance exists between what is appropriately disclosed and discussed in the educational realm against supplying information to those who intend or be inclined to inflict great harm upon innocents. The prospect of using UAS to efficiently and economically deliver weaponized chemical, biological and radioactive agents is of constant concern. It would be foolish to assume that scenarios discussed in this text are incapable of being independently created by those who seek to inflict harm, yet it is all of our duty to do our utmost to prevent such a reality.

Although the balance must always tip in favor of using information for education and defense of freedom-loving nations and citizens, we must also be mindful that other eyes are reading, and ears are listening to the information contained in this book. The fact that this text and its prior works printed by this group of authors and the works of many others are freely available in various formats online. To pretend that only those who seek to benefit mankind will access the information would be folly. While we will be discussing various scenarios that exploit vulnerabilities in C-UAS systems and strategies, let us remain vigilant to prospect and re-double our efforts to ensure that by critical thinking and analysis we remain a step ahead of adversaries.

Keeping it Simple

To fully examine C-UAS vulnerabilities across the spectrum of civilian, commercial, homeland security, and military applications these pages would number in the thousands and the content become impossible to digest. No matter what the strategy or technology, inherent vulnerabilities will always exist. In recognition of the in-depth information proved by many of the co-authors of this textbook, we will limit our examination to the civilian-hobbyist realm. I believe that there are universal truisms of C-UAS vulnerabilities which can serve as the foundational underpinnings of the broader study and implementation of effective processes and technology to mitigate their risk.

Vulnerability evaluation must be a dynamic process since as UAS technology rapidly evolves, so too must C-UAS strategy and technology. Students and professionals should develop robust and continual processes, similar to those common to IT best practices. Focus points should include, but not be limited to, penetration testing, hacking, physical access exploitation, and social engineering attack simulations.

We will examine one multi-part scenario which is quite simple and use it to explain how C-UAS students and professionals might address challenges and vulnerabilities one might encounter in a C-UAS framework. The scenario and sub-parts will be simplistic and generic, it is for the reader to expand on the base assumptions and consider how they might affect their ability to develop C-UAS strategies, deploy or develop technologies and prepared for response based upon vulnerabilities which may be inherent therein.

History as a Guide

In the 1930s, before the outbreak of World War II, a system known as Radio Detecting and Ranging, commonly referred to today by the acronym RADAR was successfully deployed to detect an aircraft. This feat was accomplished by Sir Robert Winston Watt in 1935 and by 1937 a network deployment of this technology was deployed across Britain called Chain Home.

During the early years of WW II, it was a particularly effective technological advantage for Britain against the air raids of the German Luftwaffe. (Foley, 2019)

Sadly, the same type of radar system was present on the Hawaiian island of Oahu on December 7, 1941, known as the Opana Radar site. Two lightly trained privates were operating the unit when, just shortly after 7 am, a return was received which they interpreted as squadrons of inbound aircraft. They immediately called Fort Shafter where superiors were stationed to express their concern. They were allegedly told “don’t worry about it,” if anything it was an approaching group of B-17’s expected from San Diego. (Bureau, 2019)

Though the technology deployed in both locations was largely the same, it provides an all too painful reminder that no matter how good the technology or strategy, there will always be vulnerabilities. These vulnerabilities may be human, mechanical, environmental or even unexplainable, yet their exploitation often has consequences that are real and deadly. History has witnessed numerous examples of seemingly impenetrable defenses, even those employing state-of-the-art technology and strategy, failing under attack for a variety of reasons.

For example, a seemingly impenetrable defense based on lessons learned during World War I was constructed by France to prevent similar invasions, most particularly from its then constant adversary Germany. Sadly, when Germany sought to once again invade France during WWII, the Maginot line failed. Why? Because an apparent frontal attack, which in actuality was an intentional distraction delayed French troops from responding to two larger Axis forces. One, attacking through Belgium and the Ardennes forest and another acting as a pincer from the north from Poland. These are just two historical examples of why defense is never static, and adversaries are always on the hunt for vulnerabilities in the defenses of their prey.

Figure 11-1: Opana Radar Site

Figure 11-1 Opana Radar site (Courtesy Pearl Harbor Chamber of Commerce)

Source: (Bureau, 2019)

The latter example has led some in the cybersecurity industry to caution “Don’t let your cybersecurity become another Maginot Line.” (Mirza, 2019)

Always be mindful of the truism no matter how perfect the plan or “foolproof” the strategy or technology risk of failure or circumvention is a constant. For any C-UAS technology or strategy to be truly robust, it must assume the inevitability of failure and therefore incorporate responsive capability.

The threats posed by UAS are broader and far more complex (and therefore unpredictable) than any other technology mankind has ever encountered. Acknowledging vulnerabilities are inherent, and that adversaries will constantly probe any defensive system for them, failure must be engineered into C-UAS technology and responsive best practices are of primary importance, not an afterthought.

Figure 11-2 Battle of Constantinople

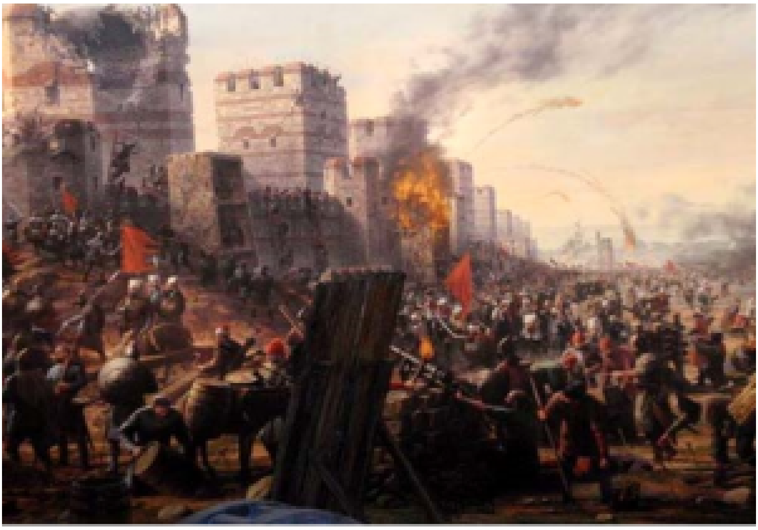


Figure 11-2 (Courtesy medievalwarfare.info)

Source: (medievalwarfare.info, 2019)

Improved technology has led to more effective weapons from the dawn of mankind. See Figure 11-2 Siege of Constantinople in 1453 for all out use of new weapons. Historians have documented such occurrences as early as 400,000, BC when humans used spears as a tool of warfare, defense, and hunting. This is a historical continuum where more mobile, lethal and functional weapons progress over time. Spears evolved into the atlatl, a type of dart, to the bow and arrow, the boomerang and eventually the sword. Between 800 and 1300 AD, primarily related to the invention of gunpowder by the Chinese, led to the cannon, hand cannon, and other forms of artillery.

Over time, hand weapons, once requiring a match to ignite gunpowder during the Ming Dynasty between 1368 and 1644 eventually evolved to better and faster ignition technology such as the matchlock and then the wheel lock. (PBS, 2014) With the dawn of the modern age rocket technology evolved and forever changed warfare in the mid-1700s. Rapid-fire artillery and automatic machine and handguns developed in the mid-1800. Through the 19th century and two World Wars during the early 20th accelerated the creation of a broad spectrum of weaponry culminating with nuclear warfare which debuted in 1945 with the bombings of Hiroshima and Nagasaki Japan. Delivery systems also improved to where nuclear ordinance could be delivered efficiently, rapidly and using land and sea-based missiles, aircraft, submarines, surface vessels, and even space-based platforms. Later laser, acoustic, stealth, space, and cyber weapons presented a dizzying array of threats that confront today's security and defense professionals.

As the millennium came and went vast improvements in using rapid data and information processing technology led to the widespread implementation of automated, unmanned intelligent weapons systems. Drone warfare almost immediately went from theoretical to and actual and present tool of warfare. (Marshall, 2009)

Unmanned technology has gained rapid acceptance by the military as well as being deployed in a myriad of civilian uses from transportation, to logistics and hundreds of other applications in everyday life. Therein lies the challenge facing C-UAS students and professionals alike, the need to differentiate and distinguish drones being used innocently versus with malice. Even the harmless use of UAS in recreational applications presents a risk to everything from civilian aviation, governmental functions, critical infrastructure and even inhabiting one own private domicile. With history as a guide, we will examine how best to predict and discover risks from this rapidly evolving, asymmetric technology.

Hiding in Plain Sight; Distinguishing the Attacker from the Hobbyist

Generally speaking, one of the biggest challenges confronting C-UAS professionals lies in the prediction and defending against risks associated with UAS technology in daily life as well its use as an attack vector in hostile activity. When considering the multitude of possibilities of threats from UAS differentiating between what is normal versus what is not, it is essential if we are to have any ability to predict, detect, deter and defend against UAS threats.

Scenario:

A single UAV hovers over an elementary school playground during recess. (Andrews, 2017) See Figure 11-3 Talking Drone. Children are loud playing and seemingly happy carnival-style calliope music is broadcast from above with the voice of Sponge Bob, Square Pants saying “follow me, kids! Once a sight that would cause alarm, has now become somewhat “normal” considering the increased popularity of UAV’s ranging from aerial photography to educational and other STEM programs.

Figure 11-3: Talking Drone

Ohio school: Beware of talking drone trying to lure kids off the playground

Figure 11-3 (Courtesy Washington Post/ Mike Stewart/AP/YouTube)

Source: (Andrews, 2017)

The need to instantly identify the capability, payload, operator, and mission has become far more complex. The more popular and affordable drones become, the more faculty, students, parents, and authorities will tend to assume such sightings are regular and innocuous.

Not too long ago, it was a rarity to see multiple jet aircraft flying overhead. Today, especially near metropolitan areas the sights and sounds associated with modern have become part of the ambient environment. Think back to your first day of elementary school. Everything was new, faces, places, sounds, smells and experiences. With time environmental familiarity became part of the daily routine.

Vulnerability Axis 1: Familiarity

From a defense and security perspective familiarity and normality are major inherent vulnerabilities to any C-UAS deployment. As automation becomes more ubiquitous in our lives the vulnerability from attack proportionately increases. This vulnerability can be largely attributed to a decrease in "Situational Awareness." Situational awareness or situation awareness ("SA)" is generally defined as a perception of environmental elements and events concerning time or space, the comprehension of their meaning, and the projection of their future status. (Endsley, 1995)

It is now well accepted that as automation and routine increase situational awareness ("SA") decreases. "Situational awareness is very important, not just for personal security but as a fundamental building block in collective security." (STRATFOR, 2012)

Returning to the schoolyard the more students, staff, and authorities become acclimated to UAV's in everyday life the less likely they will perceive them as an abnormality or threat.

Attacker Perspective:

Once again it is important to note that the "Attacker Perspective" is included in terms of generalities only, not specifics. All of the concepts, information, and discussion is an open course, not classified and within the grasp of any reasonably astute person with or without specialized education or technical expertise. They are not intended to be a “How To” tutorial on C-UAS exploits, rather and general overview of the mindset and considerations an attacker might consider when considering an attack. The key is for the C-UAS student or professional to learn to “think like the enemy” to be prepared for their attacks and attempts to exploit C-UAS vulnerabilities.

Using VPNs and other anonymization techniques, research the most popular consumer UAS in the target region, check blogs, sales figures advertisements and enforcement information from news, police websites, the FAA, state and local authorities. Consider demographics including age of the local population, popularity of drone hobbyists locally, stores that sell UAV’s and their sales volumes. Are there farms or other industries that may use UAS in any capacity such as spraying, surveillance, powerline management, policing or education? Are there local photographers, surveyors, appraisers or realtors who advertise a UAS capability online or in online publications?

Vulnerability Axis 2: Environmental Concealability

A recent trend of many civilian UAV manufacturers in the introduction of smaller and lighter products. In many ways, their size, when coupled with distance can easily be mistaken for a bird, small airplane or simply fit in as another drone in an area. Open spaces such as farm fields, rivers, parks or other sparsely populated areas are often places where drone enthusiasts may practice UAV flight or in the case of farms, may see UAS use for spraying, surveying crops of other agricultural purposes.

Attacker Perspective:

Research features, payload, speed, altitude and price attributes of various UAS available to the attacker. Consider the affordability of mini swarms to various locations to leverage distraction and confusion. Remotely research line of sight issues or BLOS capability of UAV including live stream capability to avoid local detection and enable remote operation. Consider the attacker (s) capability to operate remotely and whether local assets are required. Are there cultural, linguistic or other factors that might enhance risk detection Consider ornithological and other wildlife factors that may hinder or aide in stealth operation and avoidance of detection by the public or C-UAS technology?

Vulnerability Axis 3: Conformity with Regulation.

UAV's under .55 pounds (250 grams) are currently exempt from FAA Part 107 registration licensure requirements. According to the latest FAA guidance:

"Drones being used for commercial purposes under the Part 107 regulations need to be registered with the agency, regardless of weight. "Only those drones flown under the Exception for Limited Recreational Operations and weighing less than .55 pounds, or 250 grams, do not require registration." (Mintz, 2019)

Attacker Perspective:

Researching laws to find UAS which have little or no regulatory and administrative footprint (i.e. not subject to registration). Learn nuances, train and develop proficiency in its operation Depending on type of planned attack research the most effective payload capable of being delivered (if employing swarm, consider lighter payload upon multiple UAS's in order to account for detection, C-UAS countermeasures, human and mechanical failure and risk of environmental factors upon types of agents. (Biologic, radioactive, chemical, SCADA, even EMP attack or other)

Vulnerability Axis 4: Adapting Appearance to Attract Susceptible Targets:

When the drone allegedly broadcast a message to children on the playground a message to "follow me" it is a social engineering tool designed to attract a curious and less skeptical target. The more an attacker can adopt a "wolf in sheep's clothing" appearance the less chance of onlookers expecting any sinister motive. The more begin the appearance the less likely to cause alarm and therefore inquiry by authorities.

Attacker Perspective:

Consider the objective. Locate targets for research which fit objective and capable of success using practical, affordable and technological factors as a guide. Scour news for reports of crime, public discontent with facility operations and staff. Employ satellite imagery, social media, live stream research to determine any actionable intelligence about physical features, recent improvement, and planned projects. Check the schedule for dates and times of operation. Research surround areas for airports, radar facilities, military bases and assets, times of day with highest and least traffic. Research local EMS, Police, and Military response times in the area. Research other federal, state and local law enforcement assets nearby. Will the use of multiple, swarms or even multiple swarms be possible to avoid C-UAS detection and disperse risk to total mission failure? Is there a heavy security presence? Depending on the type of attack will there be times when targets are out in the open instead of within a building. What are work shifts, class or other staffing schedules which can provide predictability and reduce the chance of detection?

Vulnerability Axis 5: Attraction – Distraction – Stealth:

When coupled with strobing, colored, anti-collision lights, the allure of the drone becomes even more powerful. The result? A simple yet effective blending of technology, social engineering, and legality which theoretically would allow a child predator to hide the nature of their intention in the open.

This type of attack is nothing new and has supposed origins as far back as the 12th Century in the age of the Iliad and Odyssey of Greek Mythology lore. See Figure 11-4 Trojan Horse.

Figure 11-4 Trojan Horse

Figure 11-4 (Rischgitz / Hulton Archive/Getty Images)

Source: (Rischgitz, 2019)

The Trojan horse was a seemingly “normal” occurrence in this myth as a form of boasting by Odysseus who was renowned for his architectural and construction prowess. (Remember its mythology so please suspend belief.) What was not expected, just like a hidden payload in a UAV today was a lethal brigade of the best warriors of the time, hidden within the hollow belly of the horse. (Maro, 2019)

Current UAS technology allows the average citizen, terrorists and military forces globally the ability to achieve a stealth attack capability simply by blending in, operating relatively quietly and out of the field of normal ground focused visual attention. Today’s Trojan horse is compact, remotely operated, stealthy and capable of acting with overwhelming force in large numbers creating lethal swarms.

Attacker Perspective:

Which normal activities in and around the target are capable of providing cover to the attack vector. For example, in loud industrial areas, there is usually more ambient noise and therefore rotor "whir" is less likely to be heard and therefore make detection less likely? Are there time, color, feature or other forms of concealing the UAS in the open to minimize the risk of detection? The greater the distance from the launch site increases the risk of the UAS being observed and therefore remediated. Consideration of signal emanation from the controller's location will also play a role in the risk of detection by C-UAS technology. Some UAS use multiple forms of communication for operational control. Can the UAV be rebranded to make it look more like a toy or hobby vehicle with bright colors or even relevant images to lessen suspicion and delay reporting?

Vulnerability Avis 6: A Studious Attacker

According to translation from the epic military strategy work, "The Art of War", its author Sun Tzu is reputed to have written "The general who wins the battle makes many calculations in his temple before the battle is fought. The general who loses makes but few calculations beforehand." (Sun-Tzu, 1964) C-UAS students must always assume that an attacker who seeks to inflict harm or worse using UAS must have done significant research and preparation before commencing an attack. It would make little sense for such an attacker to simply fly a drone to a target and attempt to inflict damage. Students must assume that an attacker is not going to remotely pilot a UAS to a location they are unfamiliar with.

Familiarity comes with study, research, even spies. Since so much information is available online one of the most concerning vulnerabilities inherent in all C-UAS deployments is ease of access to almost any information. Students must, therefore, assume an attacker is familiar with the target, the C-UAS systems if any which is in place as well as the size, nature, and location of any possible defensive and/or responsive force.

Attacker Perspective:

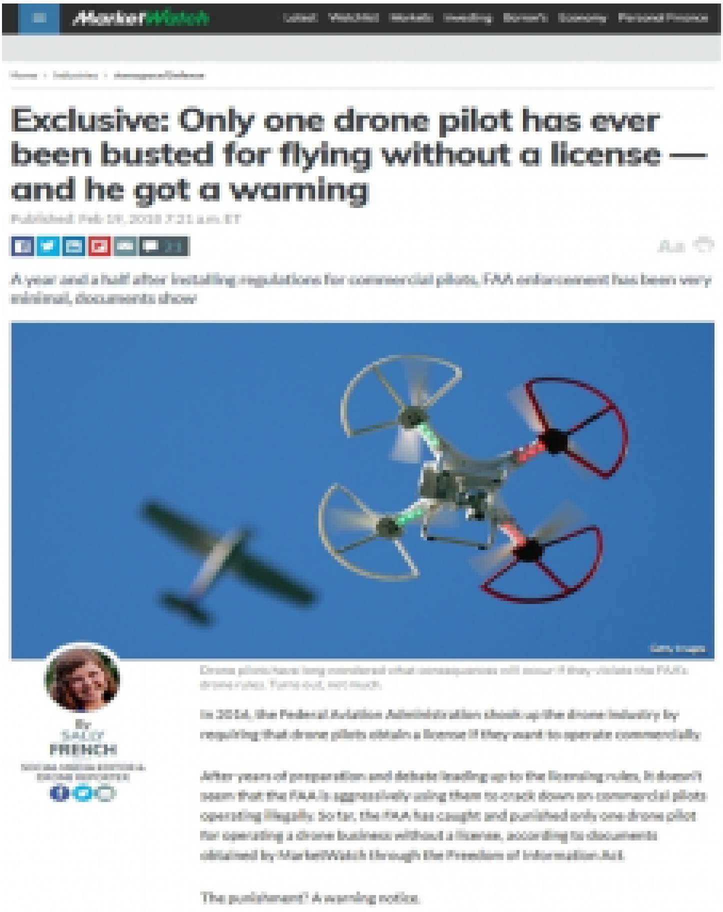
As we have discussed almost any type of information is available online. That which may not be available may be able to be acquired by compromising information systems (hacking), cultivating and recruiting spies or informants or engaging in cyber, in-person or even UAS reconnaissance of the target. A well prepared and research attack is created by patiently securing information without leaving an actual or digital footprint. Scouring budgets, work orders, new stories, building permits, business filings, and police blotter records are but a few of the areas the diligent attacker can acquire to prepare themselves to exploit C-UAS vulnerabilities.

Vulnerability: More Than a Seam – A Gaping-hole

Almost every roadway across the globe is subject to maximum speed restrictions it would seem that eventually full compliance would be achieved through education enforcement and penalties. Figure 11-5 Drone Enforcement. Nothing can be farther from the truth.

According to a 2018 study by the British Home Office, 2.2 million speeding tickets were issued in 2017, a 2.4% increase from the prior year and a 26% increase from 2011, all while automated speed enforcement technology was increasing in scope and coverage. (Office, 2018)

Figure 11- 5: Drone Enforcement



Exclusive: Only one drone pilot has ever been busted for flying without a license — and he got a warning

Published: Feb 19, 2018 7:21 a.m. ET

A year and a half after installing regulations for commercial pilots, FAA enforcement has been very minimal, documents show

Drone pilots have long wondered what consequences will occur if they violate the FAA's drone rules. Turns out, not much.

By SALLY FRENCH

SOCIAL MEDIA EDITOR & DRONE REPORTER

In 2016, the Federal Aviation Administration shook up the drone industry by requiring that drone pilots obtain a license if they want to operate commercially.

After years of preparation and debate leading up to the licensing rules, it doesn't seem that the FAA is aggressively using them to crack down on commercial pilots operating illegally. So far, the FAA has caught and punished only one drone pilot for operating a drone business without a license, according to documents obtained by MarketWatch through the Freedom of Information Act.

The punishment? A warning notice.

Figure 11-5 (Courtesy Market Watch / Getty Images)

Source: (French, 2018)

If drivers disobey a heavily monitored and enforced activity like driving, what is the likelihood that UAS operators, with little to no method to detect and enforce violations, will choose to comply? The takeaway when it comes to predicting vulnerabilities in any C-UAS deployment is to expect that many operators will not comply with the law. Whether innocent or intentional it does not matter since the interface of civilian or other UAS everyday activities can result in serious, if not tragic results.

An extensive review of public and court records search to fully grasp the vigor with which authorities are enforcing violations of UAS regulations in the United States. Not surprisingly I was hard-pressed to find more than a handful of prosecutions, and when they occurred the penalties enforced were warnings. (French, 2018) This begs a critical question, is there even an enforcement arm of the FAA or other law enforcement agencies capable of enforcing current UAS regulations? While many of the vast majority of operators will choose to comply with the law to the extent, they understand it, the fact that detection and enforcement are virtually non-existent is a fact that will not be overlooked by an attacker and is there a major vulnerability confronting any C-UAS professional.

The Information Age – A Tool for Attackers

According to a report issued by the General Accounting Office on October 17, 2019, three recommendations were made to the Ranking Member, Committee on Transportation and Infrastructure:

"GAO has three recommendations, including that FAA: (1) develop an approach to communicate to local law enforcement agencies expectations for their role in UAS investigations, and (2) identify and obtain data needed to evaluate FAA's small UAS compliance and enforcement activities, as the UAS environment evolves. FAA concurred with the recommendations." (GAO, 2019)

Facially, the GAO recommendations suggest the FAA's current strategy to regulate civilian UAS activity is one of the evaluation and development of tools and processes all while studying the best methods to enforce compliance with laws and regulations. The current UAS enforcement regime is a vulnerability in and of itself. As of October 2019, it appears that little or no coordinated monitoring, response, and enforcement mechanism is in place to address the growing risk of UAS attacks.

The United States Government Accounting Office ("GAO") issued a "Law Enforcement Guidance for Suspected Unauthorized UAS Operations", on August 14, 2018. According to the report, the FAA uses the acronym D-R-O-N-E to instruct State and Local Law Enforcement Agencies on how best respond to a suspected case of illegal or dangerous UAS operation within their jurisdictions: (GAO, 2019)

Ø DIRECT: attention outward and upward, attempt to locate and identify individuals operating the UAS.

Ø REPORT: the incident to the FAA Regional Operations Center (ROC).

Ø OBSERVE: the UAS and maintain visibility of the device.

Ø NOTICE FEATURES: Identify the type of device, whether it is fixed wing or multi-rotor, its size, shape, color, and payload, such as video equipment, and the activity of the device.

Ø EXECUTE appropriate action. Follow your policies and procedures for handling an investigation and securing a safe environment for the public and first responders." (FAA, Law Enforcement Guidance for Suspected Unauthorized UAS Operation – Version 5, 2018)

Criminals, terrorists, hostile nations and other bad actors can find and search the exact reports we have referenced above. To assume they are not using this information in planning UAS attacks is likely a dangerous if not deadly mistake. Even were the systems for monitoring and enforcing illegal UAS activity to fully exist, the sheer number of UAS operating legally or illegally will make pre-attack intervention a longshot. The solution? Create the best C-UAS technology and strategy possible but make responsive capability equally if not more robust.

Rapid Advancements in Technology -Amplified Vulnerability

In July 2018, a supplementary letter was issued updating a letter sent by the FAA Office of Airports Safety and Standards in October 2016, discussing the evaluation process for C-UAS technology deployments at major airports in the United States. Of prime importance was the following admonition which every C-UAS student, professional or educator must never lose sight of. “An additional and critical component of this finding is that technology rapidly becomes obsolete upon installation as UAS technology is rapidly changing.” (FAA, Airport Safety Media, 2018) To minimize the challenge from C-UAS vulnerabilities being exploited would not only be against the lessons taught to us by history but, also to ignore the reality of human ingenuity when it comes to circumventing the technology. The longer new technology remains in the market, the more motivated attacker can probe it for weakness, look to disable, circumvent, confuse or reverse engineer. The challenge facing C-UAS professionals is one of the endless cycle of point-counterpoint.

As this chapter is being written rest assured somewhere in the world motivated attackers are probing systems for vulnerabilities and likely examining ways to equip UAS with Anti- C-UAS technology. If the future of C-UAS is to be one of efficacy and reliability, all engaged in this noble work must take heed of the warning given by Albert Einstein to President Harry Truman. “I know not with what weapons World War III will be fought,” Albert Einstein warned President Truman, “but World War IV will be fought with sticks and stones.” As quoted by Rosa Brooks who continued: Certainly, history offers plentiful examples of escalating technological “measure, countermeasure, counter-countermeasure”. (Brooks, 2013)

Conclusions

While it is impossible to predict the future, what is possible to look to the past. Students must keep this in mind going as they embark on careers in this exciting, important and ever-changing field. If there is one takeaway that will benefit any current or future C-UAS technology it that no matter what the defensive technology or strategy, it is always best to “be prepared” for any contingency. In a field where only perfection will ensure safety sobriety and preparedness dictates that perfection will never be achievable and professionals and the public alike must be cognizant of this reality.

Questions:

1. Do you believe that an all-encompassing C-UAS system of technology and strategy will ever be a reality?

2. List 3 steps you would take to proactively discover possible C-UAS vulnerabilities both from a technological and strategic standpoint?

3. If you were responsible for crafting a C-UAS strategy and deploying technology what would be your top three objectives when beginning the process?

4. Do you believe civilian use of UAS not matter the size should be regulated as an inherently dangerous technology much like handgun laws?

References

Andrews, T. M. (2017, October 12). *ohio-school-beware-of-talking-drone-trying-to-lure-kids-off-the-playground.* Retrieved from www.washingtonpost.com/news/: https://www.washingtonpost.com/news/morning-mix/wp/2017/10/12/ohio-school-beware-of-talking-drone-trying-to-lure-kids-off-the-playground/

Brooks, R. (2013, April 4). *Why Sticks and Stones Will Beat Our Drones.* Retrieved from foreignpolicy.com:

https://foreignpolicy.com/2013/04/04/why-sticks-and-stones-will-beat-our-drones/

Bureau, P. H. (2019, October 22). *The History of the Opana Radar Site.* Retrieved from Pearl Harbor Visitors Bureau: Pearl Harbor Visitors Bureau. (2019, October 22). The History of the Op https://visitpearlharbor.org/the-history-of-the-opana-radar-site

Endsley, M. R. (1995). Measurement of Situation Awareness in Dynamic Systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 65-70.

FAA. (2018, July 20). *Airport Safety Media.* Retrieved from Federal Aviation Administration Office of Airports Safety and Standards: https://www.faa.gov/airports/airport_safety/media/attachment-1-counter-uas-airport-sponsor-letter-july-2018.pdf

FAA. (2018, August 14). *Law Enforcement Guidance for Suspected Unauthorized UAS Operation – Version 5.* Retrieved from Federal Aviation Administration: https://www.faa.gov/uas/public_safety_gov/media/FAA_UAS-PO_LEA_Guidance.pdf

Foley, S. (2019, October 20). *World War II Technology that Changed Warfare -Radar and Bombsights.* Retrieved from Scholars Archive at Johnson & Wales University, JWU: https://scholarsarchive.jwu.edu/cgi/viewcontent.cgi?article=1011&context=ac_symposium

French, S. (2018, February 19). *Only one drone pilot has ever been busted for flying without a license.* Retrieved from Marketwatch.com: https://www.marketwatch.com/story/exclusive-only-one-drone-pilot-has-ever-been-busted-for-flying-without-a-licensehe-got-a-warning-2018-02-08

GAO. (2019, October 17). *Unmanned Aircraft Systems: FAA's Compliance and Enforcement Approach for Drones Could Benefit from Improved Communication and Data.* Retrieved from General Accounting Office: https://www.gao.gov/reports/GAO-20-29/#finding2

Maro, P. V. (2019, November 16). *P. Vergilius Maro, Aeneid, John Dryden, Ed.* . Retrieved from perseus.tufts.edu : http://www.perseus.tufts.edu/hopper/text?doc=Perseus%3Atext%3A1999.02.0052%3Abook%3D2

Marshall, M. (2009, July 7). *Timeline: Weapons technology.* Retrieved from New Scientist: Marshall, M. (2009, July 7). Timeline: Whttps://www.newscientist.com/article/dn17423-timeline-weapons-technology/

medievalwarfare.info. (2019, November 16). Retrieved from Siege of Constantinople: http://www.medievalwarfare.info/

Mintz, S. (2019, November 1). *FAA Weighs In On Tiny Drones.* Retrieved from Politico.com: https://www.politico.com/newsletters/morning-transportation/2019/11/01/senate-passes-transportation-spending-bill-781967

Mirza, S. (2019, May 16). *Mirza, S. (2019, May 16). Don’t let your cybersecurity become another Maginot Line. Retrieved from Asia PacifiDont-let-your-cybersecurity-become-another-maginot-line/.* Retrieved from Mirza, S. (2019, May 16). Don’t let your cybersecurity become another Maginot Line. Retrieved from Asia Pacific Network blog.apnic.net: Mirza, S. (2019, May 16). Don’t let your cybersecurity become another Maginot Line. Retrievhttps://blog.apnic.net/2019/05/16/dont-let-your-cybersecurity-become-another-maginot-line/

Office, U. K. (2018). *Police powers and procedures, England and Wales, year ending* 31 *March* 2018. London: U. K. Home Office. Retrieved from United Kingdom Home Office. (2018). Police powers and procedures, England and Wales, year ending 31 March 2018. London: U. K. Home Office.: 31 March 2018. London: U. K. Home Office.

PBS. (2014). *Gun Timeline.* Retrieved from Public Broadcasting System: https://www.pbs.org/opb/historydetectives/technique/gun-timeline/

Rischgitz. (2019, January 21). *Trojan Horse.* Retrieved from pixels.com: https://pixels.com/featured/trojan-horse-rischgitz.html

STRATFOR. (2012, March 4). *On Security -A Practical Guide to Situational Awareness.* Retrieved from Stratfor Enterprises, LLC: https://worldview.stratfor.com/article/practical-guide-situational-awareness

Sun-Tzu. (1964). *The Art of War.* Oxford: Clarendon Press.

Additional Readings

European Commission. (2019). Speed choice: why do drivers exceed the speed limit? Brussels: European Union.

Small Unmanned Aircraft Systems, 14 CFR Part 107 (Federal Aviation Administration June 28, 2016).

Weeks, L. (2011, September 6). 5 Other Surprise Attacks That Changed History. Retrieved from NPR: https://www.npr.org/2011/09/06/140156564/5-other-surprise-attacks-that-changed-history

PART IV

SECTION 4: LEGAL AND ADMINISTRATIVE ISSUES

Chapter 12: C-UAS Regulation, Legislation, & Litigation from a Global Perspective

W.D. LONSTEIN

Student Learning Objectives

Counter Unmanned Aircraft Systems ("C-UAS") have opened the latest example of the dynamic interface between technology and law. It is the strong suggestion of the author that students access Unmanned Aircraft Systems in the Cyber Domain, as a launch point for this chapter. Many of the fundamental principles and considerations discussed concerning law and UAS will serve as a primer to this chapter's discussion of Counter UAS regulation and jurisprudence. (Nichols, et al., 2019) With the rapid development and implementation of automation and artificial intelligence ("AI"), including Unmanned Aircraft Systems ("UAS"), legal systems globally will be forced to balance public safety with the many benefits to everyday life. Legal scholars and legislators have wrestled with the friction between technology and law centuries. Students will be exposed to historical, examples of the techno-legal balance and asked to consider how best to as apply general principles to the challenges posed by C-UAS technology and its implementation globally.

Once Completed Students Should:

Have a broad perspective on the global variances and gaps within C-UAS law globally.

- Consider the impact of the ability to operate UAS remotely and

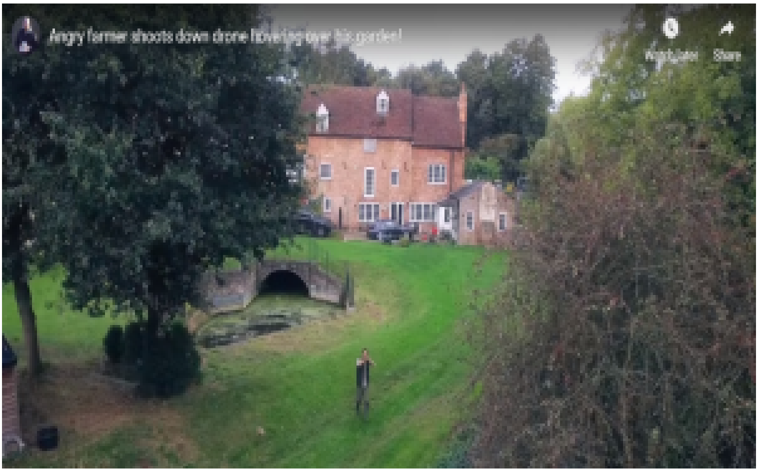
the possibility C-UAS activity may cause legal ramifications beyond the jurisdiction where it occurs.
- Examine whether a particular C-UAS technology such as Kinetic, non-kinetic, passive, active, laser, acoustic, jamming, and spoofing, might be subject to direct or indirect, regulation, and possible liability.
- Consider the sufficiency of the current statutory framework and jurisprudential precedent as it pertains to C-UAS design, deployment, or operation.
- Appreciate the likelihood of conflicting civilian and military C-UAS regulations impacting a particular deployment, technology, or location.

Current C-UAS Regulatory Landscape

The current state of C-UAS jurisprudence is in its infancy with widely divergent regulatory landscapes around the globe. From a general perspective, most nations prohibit an individual or private company's right to a "self-help" C-UAS policy (i.e., the prohibition of shooting down a drone at all with kinetic or non-kinetic measures). Much the same as is the case within the United States, internationally, private C-UAS activity is strictly prohibited unless conducted under the auspices of the military or police function. Students might ask why there is no right for a person (s) to protect their physical safety, property, pets, farm animals, and privacy from the threats posed by unwanted drones. The answer, though less than satisfactory to many, is that there may be many unintended consequences from self-help C-UAS activity. What if police were seeking a poacher of animals in the forest next to the farm? Now the facts implicate damage to police property, interferes with legal police activity, not to mention creates risks to others caused by the crash of the drone once disabled.

At first glance, it might seem that such a policy runs contrary to individual and property rights (Figure 12-1), especially if the drone is flown over private property or otherwise being flown dangerously or recklessly in public the prohibitions are grounded in logic.

Figure 12-1 Angry Farmer Spoof



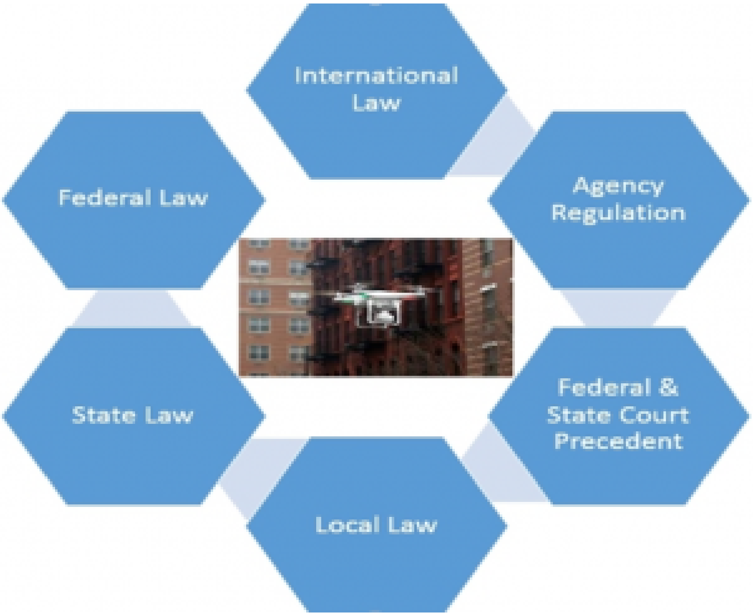
Source: (Junkin Media , 2016)

A global survey of current C-UAS regulations reveals near uniformity in most nations, prohibiting any C-UAS activity taken by any entity other than the National Security Apparatus, Civil Aviation Authorities, and military. Most notably and understandably, "self-help" C-UAS, such as that depicted in Figure 12-1, may seem a simple and understandable reaction to an apparent privacy invasion or aerial trespass. The challenge for C-UAS practitioners is when dealing with perceived threats from an aerial trespasser, shooting it out of the sky can have serious consequences.

Let's assume the farmer in Figure 12-1 is actually in Scranton, Pennsylvania, instead of the United Kingdom. What are the ramifications of a landowner, seeing a drone fly over his land at low altitude, deciding to use a shotgun to shoot it out of the sky? Applying current C-UAS law to this scenario reveals a confusing and uncertain landscape for confronting what is sure to become a more common occurrence Figure 12-3 traces the growing spectrum of Federal C-UAS regulation in the United States.[1] In addition to federal laws that prohibit "self-help" C-UAS activity, international laws, state laws, agency regulations, rules, and precedential court decisions can subject the farmer to significant criminal or civil consequences. Depending on the action

taken, and for our purposes, we will use the farmer with the shotgun that may result in criminal or civil liability under a complex interaction of various federal, state, and local laws.

Figure 12-2 Global C-UAS Legal Implication Matrix



Source: (West, 2019)

Back to our farmer, not only is he subject criminal liability under an array of federal laws and regulations, but he may have also run afoul of numerous state, local laws as well as subject himself to civil liability. A civil action is one brought by an injured or aggrieved party for monetary damages against the party who allegedly caused the loss. In the case of the farmer, a lawsuit might be filed by an injured party, including the drone owner, the drone operator, and even the person who may have hired the operator to perform a specific mission or task.

When the force of gravity added to the scenario, the situation gains complexity. According to Michael Hamann, there are many risks attendant to these kinetic countermeasures. The payload, if harmful, may well be dispersed throughout the crash area as well the impact of a plastic rotary falling from the sky has caused a crash test dummy to receive a powerful effect ranging from 9 foot-pounds and 233 foot-pounds, depending on the angle and speed of the falling drone. (Michael Hamann, 2018), citing (FAA UAS Center of Excellence, 2017)

To further complicate things, if the farmer successfully shot down the drone, and it landed on the head of his neighbor who succumbed to the injuries, he sustained an additional set of legal consequences will unfold. For example, the heirs of the deceased neighbors might seek to bring claims for civil damages, including but not limited to wrongful death and negligence. Criminal charges may result from the illegal shooting and the killing of the neighbor. Tables 12-3 – 12-5, below demonstrate the complexity of implications from the United States, as well as other nations, relating to C-UAS activity.

TABLE 12-1: UNITED STATES FEDERAL LAW

Federal Law or Regulation	Countermeasure	Prohibition or Rule	Penalty
FAA Reauthorization Act of 2018	N/A	Limits C-UAS authority to DHS, DOJ & U.S. Coast Guard and requires consultation with Department of Defense	N/A

Title 47 U.S.C. § 301 et., Seq.	Radio Interference Signal Disruption	47 U.S.C. § 301 Radio Transmitter License Required 47 U.S.C. § 302 Illegal to own sell, import, or operate radio signal “jamming” technology. 47 U.S.C. § 320 Allows FCC to require any radio station which in its opinion may interfere with distress signal of ships be required to have a licensed operator listening for distress signals. 47 U.S.C. § 325 Prohibits False, fraudulent or unauthorized distress or other re-broadcast of radio signals. 47 U.S.C. § 333 Prohibits willful or malicious interference with radio communications. 47 U.S.C. § 605 Unlawful interception of radio transmission	47 U.S. Code § 502 not more than $500 for each and every day during which such offense occurs

18 U.S.C. Chapter 119 **Interference with government & satellite communications**	Jamming, Spoofing & similar countermeasures	18 U.S.C. § 1362 Interface with Government Communications 18 U.S.C. § 1367 Interference with Satellite Communications	Fines and imprisonment of not more than 10 years
18 U.S.C. § 32 **Destruction of Aircraft or Facilities**	Destruction of aircraft –		Fines and/or imprisonment of not more than 20 years.
18 USC § 2510, 2511 **Wiretap Act**	“Spoofing” a GPS or other controlling signal or communication.	18 U.S.C. § 2511 Interception of Wire Communications	Fines up $ 250,000 and imprisonment of not more than 10 years

Source: (Federal Aviation Administration, 2018)

TABLE 12-2: STATE LAWS IN CALIFORNIA & NEW YORK

State Law or Regulation	Countermeasure	Prohibition or Rule	Penalty
New York Penal Law	Shooting Drone with Shotgun	NY Penal Law § 145.05: Criminal Mischief in the Second Degree: Intentionally damage someone else's property in an amount that exceeds $ 1,500.00	Class D Felony Fine & Imprisonment of up to 5 years imprisonment
		NY Penal Law § 145.05: Criminal Mischief in the Second Degree: Intentionally damage someone else's property in an amount between $ 250.00 and $ 1,500.00	Class E Felony Fine & Imprisonment of up to 4 years imprisonment
		NY Penal Law § 265.35 (2) Unlawfully discharging a firearm at an aircraft.	Class E Felony Fine & Imprisonment of up to 4 years imprisonment
		Civil Liability	Monetary Damages

			Misdemeanor or Felony depending on facts
California Penal Code	Shooting Drone with Shotgun	**Penal Code 246.3** PC 1. 2. Willfully discharge a firearm, in a grossly negligent manner, which could result in someone's injury or death Penal Code 246 PC Maliciously and willfully fire a firearm at: An occupied aircraft**[2] Penal Code 594 PC Vandalism: Maliciously commits any of the following acts with respect to any real or personal property not his or her own: (2) Damages; (3) Destroys Crime of Carrying a Loaded Firearm in Public Civil Liability	Misdemeanor – 1 Year in jail – Fine up to $ 1,000 Felony – 16 months – 4 years in jail. Fine up to $ 10,000 Misdemeanor 6 – 12 Months imprisonment Felony 3– 7 years imprisonment Fine up to $ 10,000 Damage over $ 400.00 Fine up to $ 10,000.00 1 Year County Jail Damage up to $ 10,000.00 Fine up to $ 50,000.00 Fine up to $ 10,000.00 1 Year County Jail Monetary Damages

TABLE 12-3: GLOBAL LEGAL EXAMPLES[3]

Country	Countermeasure	Prohibition or Rule	Penalty
United Kingdom	GPS Jamming or signal interference	Wireless Telegraphy Act 2006 UK Public General Acts, 2006 c. 36, Part 2 Chapter 4 Unauthorized use etc. of wireless telegraphy station or apparatus	Fine of up to £ 250,000; and 5% Gross Revenue Imprisonment up to 2 years
	Misleading messages (spoofing), Interception	Wireless Telegraphy Act 2006 UK Public General Acts, 2006 c. 36, Part 2 Chapter 4 A person commits an offence if, by means of wireless telegraphy, he sends or attempts to send a message to which this section applies. (a) is false or misleading; and (b) is likely to prejudice the efficiency of a safety of life service or to endanger the safety of a person or of a ship, aircraft or vehicle.	Fine of up to £ 250,000; and 5% Gross Revenue Imprisonment up to 2 years
	Computer Hacking	Computer Misuse Act of 1990	Up to 2 years Imprisonment and up to £ 5,000 Fine
	Shooting UAV with illegal weapon	Section 5(2A)(c) of the Firearms Act 1968	· For possession, purchase or acquisition – 10 years imprisonment. · For manufacture, sale of transfer – Life imprisonment.

		Chapter 27, Part 1 (16) Firearms Act of 1968 Possession of firearm with intent to endanger life or cause serious injury to property Chapter 27, Part 1 (18) Firearms Act of 1968 Carrying firearm with criminal intent Chapter 27, Part 1 (19) Firearms Act of 1968 Carrying a Firearm in a Public Place Chapter 27, Part 1 (20) Firearms Act of 1968 Trespassing with a Firearm	· 6 months – 4 years imprisonment
	Damaging or attempting to damage a UAV	Criminal Damage Act 1971 Chapter 48 Part 1 (1), (2) Destroying or damaging property Criminal Damage Act 1971 Chapter 48 Part 3 (a), (b) Possessing anything with intent to destroy or damage property	·
Russian Federation	Using a weapon to destroy a UAV	Chapter 27. Crimes Against Traffic Safety and the Operation of Transport Vehicles Article 263. Violation of the Rules for Traffic Safety and Operation of the Railway, Air, Sea and Inland Water Transportation Systems, as Well as of the Underground Railroad	· 100,000 – 300,000 Rubles Up to 4 Years in prison or 2 years in labor camp.

	Article 267. Putting out of Commission Transport Vehicles or Communications 1. Destruction, damage, or putting out of commission transport vehicles, warning devices, communications or communications facilities, or any other transport equipment, and likewise blocking transport communications, if these acts have involved, by negligence, the infliction of grave injury to human health, or the infliction of large damage	100,000 – 300,000 Rubles Up to 4 Years in prison or 2 years in labor camp.
	Article 271.1. Breaking the Rules for Using the Airspace of the Russian Federation	Up to 7 years imprisonment
Using GPS Jamming, Radio interference of other disabling of computer systems or hacking	Chapter 28. Crimes in the Sphere of Computer Information Article 272. Illegal Access to Computer Information 1. Illegal access to legally protected computer information, if this deed has involved the destruction, blocking, modification or copying of computer information	fine up to 200 thousand rubles, , or with restraint of liberty for a term of up to two years, or with compulsory labor for a term of up to two years, or with deprivation of liberty for the same term.

		Article 273. Creation, Use, and Dissemination of Harmful Computer Programs 1. Creation, dissemination or use of computer programs or another computer information, which are knowingly intended for unsanctioned destruction, blocking, modification or copying of computer information or for balancing-out of computer information security facilities –	fine up to 200 thousand rubles, , or with restraint of liberty for a term of up to two years, or with compulsory labor for a term of up to two years, or with deprivation of liberty for the same term.
		Article 281. Sabotage 1. Perpetration of an explosion, arson, or of any other action aimed at the destruction or damage of enterprises, structures, transport infrastructure facilities and transport vehicles, or vital supply facilities for the population, with the aim of subverting the economic security or the defense capacity of the Russian Federation	Punishable by deprivation of liberty for a term of ten to 15 years
Australia	Damaging or Shooting A Drone	**1 Crimes (Aviation) Act 1991 –No. 139, 1991** **Compilation No. 257 Destruction of aircraft** (1) A person must not intentionally destroy a Division 3 aircraft.	Penalty: Imprisonment for 14 years.
		Dangerous Use of Firearms Section 93 H (2) of the Crimes Act of 1900	10 Years Imprisonment

	Endangering safety of aircraft–general (1) A person who, while on board a Division 3 aircraft, does an act, reckless as to whether the act will endanger the safety of the aircraft, commits an offence. section 195 of the Crimes Act 1900 THE OFFENCE OF MALICIOUS DAMAGE The offence of Malicious Damage is contained in section 195 of the Crimes Act 1900	Penalty: Imprisonment for 10 years
GPS Jamming	**Prohibition relating to RNSS jamming devices** Under section 190 of the Act, the ACMA declares that:	Penalties for breaching the rules can be a fine of up to $1.05 million or up to 5 years in prison
Radio Signal Interference	**Use of Non-approved Radio** **Transmission devices**	Fines of up to $25,200 up to two years in prison

Sources: (Federal Aviation Administration Office of Airports Safety and Standards, 2016) (Secretary of State for the Home Department, 2019) (Russian Federation, 1996) (United Nations, 2019) (United Nations, 2019)

CAN C-UAS BE REGULATED? THE C-UAS FABLE

The current paucity of global C-UAS regulation is not only a product of the fact that UAS legislation is still in its formative stages, but it is also equally a result of the speed with which UAS, and consequently C-UAS technology is developing.

When considering whether and to what extent to regulate C-UAS technology, I turn to one of my favorite legal fables where the moral of the story is that when legislating, less can be more, particularly apropos when considering C-UAS regulation, more specifically micro-drones, and swarms.

In an attempt to eliminate a problem with pesky flies, the local town decides to deploy a solution to make life more pleasant for its residents. Although there are many more possible solutions, the village elders provide the three which they feel to be representative of different levels of risk vs. reward.

Choice 1:

Provide each household a fly swatter to give them a tool to stop flies coming into their homes.

Result:

Somewhat useful, but in the long run, not a solution that will eliminate the nuisance.

Unintended Consequence:

Sore elbow, broken items in the home, the species survives intact.

Figure 12-3 Cockroaches and Nuclear Bombs

I can survive a nuclear explosion, and I can live for 10 days without my head!
Can you survive being hit by a slipper?
But... a nuclear bomb...
10 days...

Source: (Daftardar, Depressed Man Meme, 2019) & (Daftardar, Can Cockroaches Really Survive A Nuclear Explosion?, 2015)

Choice 2:
Use aerial or water sprayed dispersion of pesticides.

Result:

Most flies eliminated, no method to contain ingestion by unintended targets or limit environmental pollution in a safe & effective manner.

Unintended Consequence:

May cause side effects to the population of humans, pets, farm animals, plant life, crops, air purity, and water. Causing a cascading series of complications ranging from remediating the environmental damage to treating generations of diseased humans, animals, and plants.

Choice 3:

Deploy a unique acoustic wing-speed signature detection technology for the species of fly native to the region where the village is situated. Once confirmed, a radio frequency countermeasure would cause the fly to die from brain injury within one minute.

Result:

Current species of native flies mostly eliminated.

Unintended Consequence:

Flies evolve where their wing-speed changes, and their acoustic sensitivity and brains become immune to the technology. Additionally, aircraft, radios, GPS, and other technologies adversely affected, causing mass disruptions to daily life.

Primum Non Nocere – First Do No Harm

The Latin phrase "Primum non Nocere" – First Do No Harm, borrowed from the field of medicine seems to be a worthy objective for C-UAS legislation. C-UAS covers a broad spectrum of kinetic and non-kinetic measures taken to destroy, disable, confuse, hijack, or otherwise interfere with the intended operation of an Unmanned Aerial System. A C-UAS tactic might be as simple as throwing a stone at a drone or as complex as introducing malware into its operating systems and everything in between. My talented co-authors more than amply discuss these technologies and tactics in other chapters of this text. For our purposes, it is necessary to determine (1) whether C-UAS regulation on a globally functional basis is possible? (2) If it was possible, how would such law impact the rights of individuals, technology companies, the respective national security interests of each nation, individual security rights and cultural differences between countries around the globe; and (3) how are inevitable conflicts in law resolved given the inherently international nature of UAS and C-UAS technology?

While the United States and other nations are currently studying the issue, as of late November 2019, it is safe to summarize the current global C-UAS specific legislation landscape as non-existent. (Jason Snead, 2018) Since UAS technology is currently being used in both military and civilian applications worldwide, NGO's such as the United Nations ("UN") and individual nations are to create effective C-UAS regulation, some degree of commonality must exist.

What is meant by commonality? For our examination, commonality means uniform foundational principles that must be recognized globally. Much like a Geneva Conventions for warfare, this policy is best run by an NGO, the most logical being the UN. Unfortunately, history teaches than UN enforcement is inherently challenging due to having 193 member states, each with separate values, cultures, religions, political and economic systems. (United Nations, 2019) Add the all too common realities of formal and informal military conflict, and it becomes a certainty that nations will interpret the regulations in a manner that supports its objectives. Accordingly, a uniform global C-UAS law does not appear to present a viable option. However, the Geneva Conventions, Hague Conventions, War Crimes, Genocide, Ethnic Cleansing, International Humanitarian laws and adjudication thereof by the UN War Crimes Tribunal should be amended to include UAS and C-UAS activity warfare specifically. (International Committee of the Red Cross, 2016) (United Nations, 2019)

When technology becomes widely available and less expensive, not to mention remotely operable, it becomes attractive to those with nefarious intent. Add the capability to deliver biologic, chemical, and nuclear payloads, and the potential to be used as a Weapon of Mass Destruction by non-state actors becomes a frightening reality. (Office of the President of the United States, 2018)

Most nations eschew C-UAS specific legislation instead of choosing to provide-UAS authority to military, civil aviation, and homeland security functions and relying upon existing criminal statutes and aviation rules and regulations to control widespread C-UAS activity. The Federal Aviation Administration issued one of the most recent pronouncements on the subject on August 14, 2018. In short, the Law Enforcement Guidance letter discussed the primacy of the Federal Governments' role in *any* C-UAS activity in the United States with state and local Law Enforcement being invaluable partners in ensuring safe drone operation. According to the guidance letter, Law Enforcement's role in C-UAS activity should be in accord with the process described by the acronym D-R-O-N-E:

- **Direct** attention outward and upward, attempt to locate and identify individuals operating the UAS. Look at windows/ balconies/rooftops. Law enforcement is in the best position to locate the suspected operator of the aircraft, and any participants or personnel supporting the operation.

- **Report** the incident to the FAA Regional Operations Center (ROC). Follow-up assistance can be obtained through FAA Law Enforcement Assistance Program (LEAP) special agents. Immediate notification of an incident, accident, or other suspected violation to one of the FAA ROCs, located around the country, is valuable to the timely initiation of the FAA's investigation. These centers are manned 24-hours a day, seven days a week, with personnel trained to contact appropriate duty personnel during non-business hours when there has been an incident, accident, or other matter that requires timely response by FAA employees.

- **Observe** the UAS and maintain visibility of the device. Note that the battery life of a UAS is typically 20 to 30 minutes. Look for damaged property or injured individuals. Local law enforcement is in the best position to identify potential witnesses and conduct initial interviews, documenting what they observed while the event is still fresh in their minds. Administrative proceedings often involve very technical issues; therefore, we expect our own aviation safety inspectors will need to interview most witnesses. During any witness interviews, use of fixed landmarks depicted on maps, diagrams, or photographs, immeasurably help in fixing the position of the aircraft, and such landmarks should be used to describe lateral distances and altitude above the ground, structures or people (e.g., below the third floor of Building X; below the top of the oak tree located at Y; or any similar details that give reference points for lay witnesses). We are mindful that in many jurisdictions, state law may prohibit the transmission of witness statements to third parties, including the FAA. However, capturing the names and contact information of witnesses to provide to the FAA will also be extremely helpful.

- **Notice** features. Identify the type of device, whether it is fixed wing or multi-rotor, its size, shape, color, and payload, such as video equipment, and the activity of the device. Pictures taken in close proximity to the event are often helpful in describing light and weather conditions, any damage or injuries, and the number and density of people, particularly at public events or in densely populated areas.

- **Execute** appropriate action. Follow your policies and procedures for handling an investigation and securing a safe environment for the public and first responders.

- It must be noted, any investigations conducted by LEAs should be in accordance with local or state authorities, as the FAA's statutes and regulations do not permit their use as a basis for LEAs to conduct investigations. (Federal Aviation Administration, 2018)

In order to reinforce current C-UAS restrictions, a recent FAA Law Enforcement Guidance letter cites specific Federal laws and regulations which are implicated when an unauthorized person engages in C-UAS activity in the United States. (Figure 12-4)

By way of comparison, the United Kingdom allows Law Enforcement a broader use of C-UAS technology and tactics including DTI (Detect Track and Identify) technology, and effector technology which can disable hostile drones. In a recent Counter Unmanned Aircraft presentation given to Parliament in October 2019, the British Home Department established a multifold strategy for C-UAS preparation and capability.

The stated objective of the plan is:

1. **1**. Developing a comprehensive understanding of the evolving risks posed by the malicious and illegal use of drones;

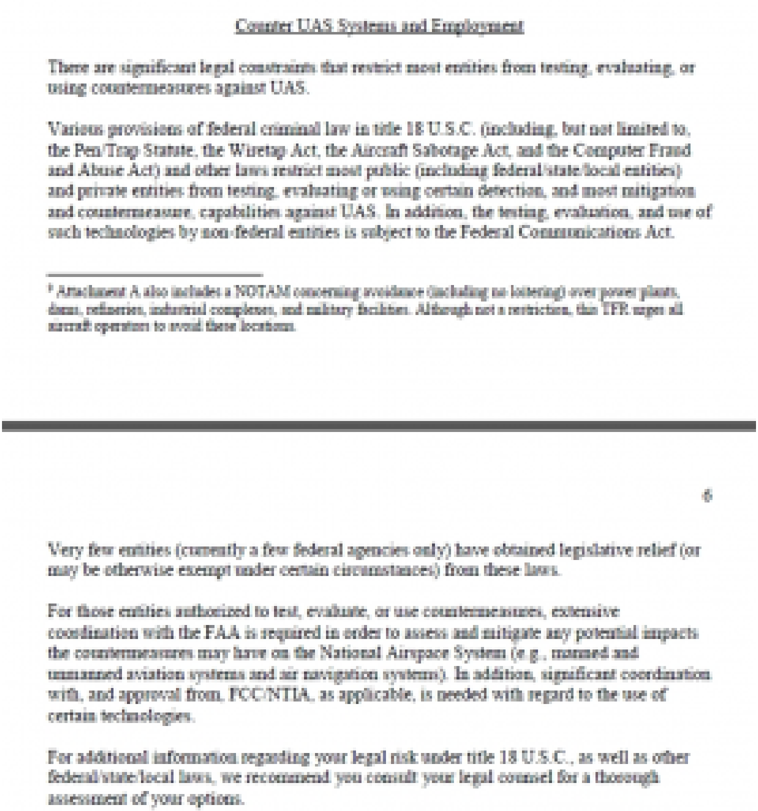
2. Taking a 'full spectrum' approach to deter, detect and disrupt

the misuse of drones;

3. Building strong relationships with industry to ensure their products meet the highest security standards and,

4. Empowering the police and other operational responders through access to counter-drone capabilities and effective legislation, training and guidance.(Secretary of State for the Home Department, 2019)

Figure 12-4: FAA Law Enforcement Guidance



Counter UAS Systems and Employment

There are significant legal constraints that restrict most entities from testing, evaluating, or using countermeasures against UAS.

Various provisions of federal criminal law in title 18 U.S.C. (including, but not limited to, the Pen/Trap Statute, the Wiretap Act, the Aircraft Sabotage Act, and the Computer Fraud and Abuse Act) and other laws restrict most public (including federal/state/local entities) and private entities from testing, evaluating or using certain detection, and most mitigation and countermeasure, capabilities against UAS. In addition, the testing, evaluation, and use of such technologies by non-federal entities is subject to the Federal Communications Act.

[5] Attachment A also includes a NOTAM concerning avoidance (including no loitering) over power plants, dams, refineries, industrial complexes, and military facilities. Although not a restriction, this TFR urges all aircraft operators to avoid these locations.

6

Very few entities (currently a few federal agencies only) have obtained legislative relief (or may be otherwise exempt under certain circumstances) from these laws.

For those entities authorized to test, evaluate, or use countermeasures, extensive coordination with the FAA is required in order to assess and mitigate any potential impacts the countermeasures may have on the National Airspace System (e.g., manned and unmanned aviation systems and air navigation systems). In addition, significant coordination with, and approval from, FCC/NTIA, as applicable, is needed with regard to the use of certain technologies.

For additional information regarding your legal risk under title 18 U.S.C., as well as other federal/state/local laws, we recommend you consult your legal counsel for a thorough assessment of your options.

Source: (Federal Aviation Administration, 2018)

The current UK C-UAS policy differs from that of the United States in that it provides for a more active C-UAS role given to Law Enforcement agencies:

"The police are able to legally deploy a range of DTI and counter-drone effector systems. We will develop options for the creation of a UK national counter-drone capability that will reduce our domestic reliance on defence capability to respond to the most challenging drone security incidents and will allow the police to protect national iconic events, or support crisis response. We will identify the most appropriate equipment and resource to procure and deliver this capability." (Secretary of State for the Home Department, 2019)

While current C-UAS regulations and enforcement regimes vary significantly, given time and study, it is likely that more certainly will come to C-UAS practice. The challenge facing C-UAS practitioners will be multi-fold. Off the shelf obsolescence, Counter- Counter-UAS technology will inevitably be incorporated into many UAS just as chaff, flares, jamming, DIRCM (Directed Infrared Counter Measures), and other technologies rapidly developed to counteract anti-aircraft technology from the dawn of military aviation up to today.

Students must account for the reality that a measure-countermeasure dynamic will present challenges to any scheme of C-UAS legislation or regulation. Therefore, it is incumbent upon those who enact C-UAS laws to avoid the temptation of focusing upon specific technologies or tactics instead of focusing upon the establishment of general principal legislation.

For example, a regulation that proscribes C-UAS technology or tactics which are likely to endanger the public nationwide is far more flexible than a statute that prohibits the use of C-UAS technology in or near cities with a population over 100,000.

The principle of legislative generality was affirmed by the Government of Victoria, Australia when it issued the following guidance:

"Regulation of specific activities, industries or professional groups is a last-resort option. Preference will be given to promoting industry self-regulation and best practice, including codes of conduct, assessing whether existing broader legislation (State or Commonwealth) applies to particular cases, using other non-legislative methods (e.g. government provision of information) to address concerns. (DTF 2005, p. 1–7) (Consumer Affairs Victoria, 2006)

Regulating technology can have many unintended consequences, which were articulated by Christopher Fonzone and Kate Heinzelman in a 2018 opinion piece regarding legislating Artificial Intelligence.

"Decisions made today may have substantial ripple effects that legislators could easily miss on the development of AI technology down the road. Who could have possibly imagined the full implications of Section 230 of the Communications Decency Act when it was enacted in 1996? Or the effect of the Electronic Communication Privacy Act's warrant requirement for emails less than 180 days old in 1986? Early legislative enactments about new technologies tend to persist." (Christopher Fonzone, 2018)

There are no clear answers when it comes to ethics, technology, warfare, terrorism, and crime. C-UAS Students, Practitioners, and Regulators would be wise to remember that job 1 in public safety and national defense is first not to harm those you seek to protect.

OTHER CONSIDERATIONS – Self Defense

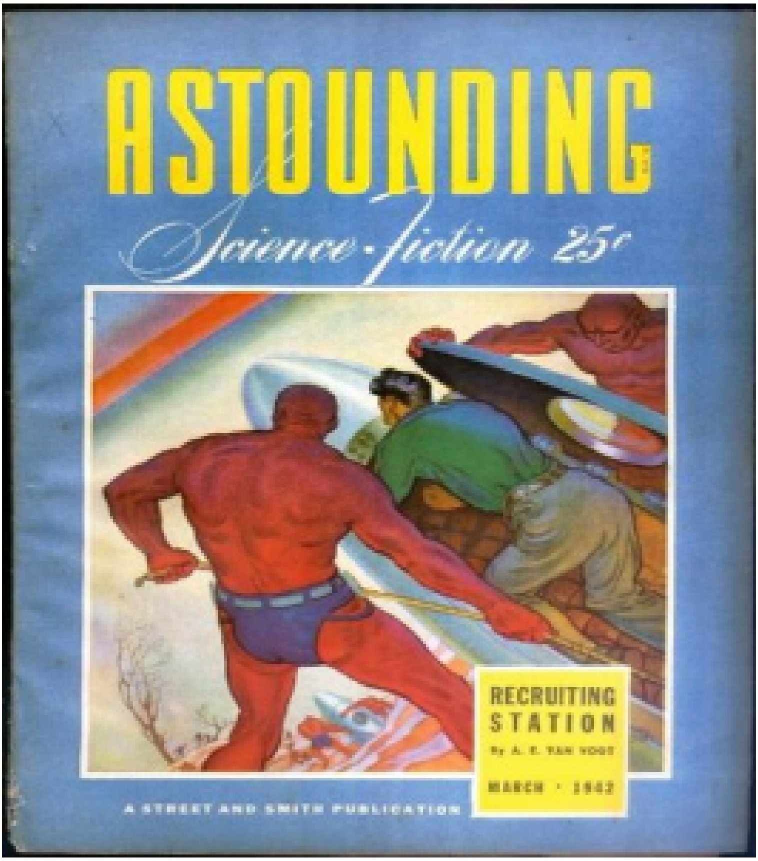
Recently Hollywood has been capturing the imagination of audiences globally with thrillers involving UAS attacks by traditional and non-traditional combatants, terrorists, and other bad actors. The 2019 film, "Angel Has Fallen" takes quite a bit of license, however, is undoubtedly demonstrative of how UAS technology, in the hands of a bad actor, could wreak havoc on society. (Waugh, 2019) The use of mobile launched mini-drone swarm technology presents a growing threat to all society. Let's hope it's a case of art imitating imagination instead of creativity imitating life.

Figure 12-5: Angel Has Fallen

Source: (Waugh, 2019)

Films including Star Trek, War Games, Star Wars, Runaway, and Terminator are a few examples of films that examine AI, Automation, Unmanned technology, and the attendant risks they pose when falling into the wrong hands or become out of control due to a fault or defect. In a world where weapons of war have been finding their way off the battlefield and onto the streets, we must be prepared and assume the reality that UAS technology will also be a prime target for the black-market profiteers. Even worse, UAS technology designed for the hobbyist, farming or other non-military functions is currently flooding the market at low prices. This new affordability begs the question, if technology falls into the hands of those who present asymmetric threats, and can appear to be part of everyday life, is it ethical for the government to prohibit individuals from engaging in self-defense? Isaac Asimov, the noted writer, and scientist first introduced and right of self-defense against automated technology ("robots") in the short story *Runaround* published in 1942.

Figure 12-6: Asimov's 3 Laws for Robots



Source: (Asimov, 1942)

To allow for an orderly introduction of robotics into our lives, Asimov, a visionary futurist, created the "The Laws for Robots."

1. **A robot may not injure a human being or, through inaction,**

allow a human being to come to harm.

2. A robot must obey the orders given to it by human beings, except where such orders would conflict with the First Law.

3. A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.

He later introduced a zeroth law which stated:

1. **A robot may not harm humanity, or, by inaction, allow humanity to come to harm.** (MIT Technology Review, 2014)

Subsequently, other scholars examined Asimov's three laws in the context of the drone age, where remotely piloted or autonomous aircraft are now capable of inflicting harm to humans on a massive scale. Ulrike Barthelmess, Koblenz Ulrich Furbach expanded upon this concept when they wrote in a paper discussing whether Asimov's laws of robotics in 2014:

"But we also should mention that there do exist autonomous vehicles and robots designed *per se* to harm humans. Military robots or autonomous drones are aiming explicitly at violating Asimov's laws. What we desperately need are legal and ethical rules for the commitment of robots. We can see this from the debate around drone strikes in Pakistan, Yemeni Somali. According to the Bureau of Investigative Journalism there is a kind of covert drone war in those countries. Drones are used to strike against targets in countries, without being officially in war according to the international law of armed conflict. More or less autonomously operating drones are destroying targets i.e. humans, which are associated with terrorism. And as can easily be imagined there is a significant number of civilians killed or injured as collateral damage. We want to argue that a similar procedure would not so readily be accepted by the world public, if instead of drones manned aircrafts would be used. It seems as if there is much lower acceptance threshold to use robots instead of regular military forces for illegal or covert warfare.

Besides of moral and ethical considerations, this raises a lot of legal questions. Is it legal to strike targets with unmanned drones in a country which is not in a formal state of war with the owner of drones? Is it legal for a third-party country to support such an action, e.g. by delivering data for military reconnaissance or by hosting the pilots of the drones? In the context of this discussion it would be more likely to answer the question from the title as follows: It is not allowed to build and to use robots which violate Asimov's first law." (Barthelmess, 2014)

Currently, it is hard to establish whether a drone flying overhead is benign or a threat to the safety of those below. The stealthy nature and ability to deliver payloads, surveil or interrupt activities of normal daily life drones that pose a threat can often appear as harmless as a hobbyist learning to fly the gift they received for their birthday. With literally millions of drones flying daily, the reality is that no law enforcement strategy, much less C-UAS military deployment, can reasonably be relied upon to 100% protect military, domestic, and individuals from the risks posed by UAS technology. Students are strongly urged to read the 2015 article in the Connecticut Law Review entitled "Self-Defense against Robots and Drones." Although it is now four years later and the UAS industry continues to grow exponentially in the military, commercial and civilian applications alike, the subject of self-defense against drones lies at the heart of C-UAS regulation. The authors correctly observe that absent a reliable system that the everyday citizen can use to determine whether a UAV is a friend or foe, individuals must have, at least to a certain degree, the right of self-defense. (Colangelo, 2015)

Conclusions

While there will be no shortage of pain points in the creation of a robust yet flexible C-UAS legislative and jurisprudential scheme, students should consider the reality that no matter how broad the policy may be, a motivated attacker will always find a way to exploit it. One need look no further than to constant friction between those who want to make certain classes of firearms illegal, and those who feel the right is a natural inheritance in countries such as the United States. Both make valid arguments yet were either side to prevail; those who are intent on harming will find a way to legally or illegally acquire a weapon. As we head further into the age of ubiquitous automation, there will be no shortage of debates about how best to regulate the legal and prevent the illegal use of the technology. Dr. Martin Luther King, Jr., delivered a speech in 1963 when he discussed the challenge of legislating morality, as opposed to regulating behavior:

"Religion and education must play a great role in changing the heart. But we must go on to say that while it may be true that morality cannot be legislated, behavior can be regulated. It may be true that the law cannot change the heart, but it can restrain the heartless. It may be true that the law cannot make a man love me, but it can keep him from lynching me and I think that is pretty important, also." (Dr. Martin Luther King, 1963)

Those who seek to engage in a career in the UAS / C-UAS field will undoubtedly have to confront this challenge regularly. Whether you are creating CUAS technology, deploying that technology, or designing strategies, the result of what you do will inevitably have a long-lasting consequence to humanity. Risk, reward, cost, and morality are but a few of the factors you will have to balance while the speed of new technology will make the ground beneath your feet feel like a treadmill moving 100 miles per hour.

No matter how good the technology, strategy, or defense, a motivated actor will find a way to exploit vulnerabilities inherent within it. So too is the case when legislating and regulating C-UAS activity. Every exigency, contingency, circumstance, and location will challenge the applicability of the law, not to mention possible provide a means for malevolent actors to exploit it to inflict great harm legally. Laws can inhibit the development of technologies that may offer more safety, certainty, and clarity to the field of UAS / C-UAS jurisprudence, and so knee-jerk, reactionary rules can do more harm than good. The best course of action? Think for today but be flexible enough to understand the consequence tomorrow. No law can be perfect, particularly when it comes to technology in its infancy.

QUESTIONS TO CONSIDER:

1. If the farmer in Figure 12-1 shot down the drone flying near his farm, only to find the payload was a vial of liquid with a timer attached. Thankfully the buckshot from the shotgun and the fall to earth did not damage the vial ort timer. The farmer immediately calls authorities who respond and disarm the timer. They rush the drone away to a secure facility where they discover that vial contained an aerosolized form of the Ebola virus. But for the farmer's action, thousands may have died. Should he be charged with violating the various statutes listed in Figures 12-3 – 12-5 above?

2. Would your opinion change if the buckshot damaged the vial and let the virus escape into the atmosphere? What if the target location was 20 miles away with a dense population while the population within 5 miles of his farm was under 100?

3. Imagine the drone launcher from "Angel has fallen," as depicted in Figure 12-7, was pulling up to a remote area within proximity

of Camp David, Maryland. Further, assume that a C-UAS hobbyist, uncertain of the law, was nearby and coincidentally testing a new C-UAS technology using magnetized plasma energy. Despite excellent efficacy, its components are military-grade and, therefore, illegal for a citizen to possess. Understanding the fact that Camp David is near and not seeing any indicia of Secret Service or other lawful entities on the launcher vehicle, he deploys the plasma energy weapon, disables the swarm, and saves the president, his family, and those in protection party. Should the hobbyist be treated as a criminal or a Good Samaritan?

4. What if the scenario in number 3 above was the same, and the president was safe; however, the plasma energy cause three helicopters overhead to lose computer-assisted guidance, power and control surface function resulting in all three crashing and the lives of 16 agents were lost. Should the hobbyist be held criminally responsible?

References

Asimov, I. (1942, March). runaround. *Astounding Science Fiction*, pp. 94-103.

Barthelmess, U. &. (2014). Do we need Asimov's Laws?. *arXiv – Cornell University*, 9-11.

Christopher Fonzone, K. H. (2018, February 26). *Should the government regulate artificial intelligence? It already is.* Retrieved from The Hill: https://thehill.com/opinion/technology/375606-should-the-government-regulate-artificial-intelligence-it-already-is

Colangelo, A. M. (2015). Self-Defense Against Robots and Drones. *Connecticut Law Review*, 10-30.

Consumer Affairs Victoria. (2006). *Choosing between general and industry specific legislation.* Melbourne: Consumer Affairs Victoria.

Daftardar, I. (2015, June 26). *Can Cockroaches Really Survive* A *Nuclear Explosion?* Retrieved from Science ABC: https://www.scienceabc.com/eyeopeners/revealed-can-cockroaches-really-survive-nuclear-explosions.html

Daftardar, I. (2019, November 11). *Depressed Man Meme*. Retrieved from images-wixmp-ed30a86b8c4ca887773594c2.wixmp.com: https://images-wixmp-ed30a86b8c4ca887773594c2.wixmp.com/f/db28749d-3a5e-4956-9e70-ef417f1f8b21/d5hdmki-379818b5-1b65-4420-8639-9697faa9dcb1.jpg?token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJ1cm46YXBwOjdlMGQxODg5ODIyNjQzNzNhNWYwZDQxNWVhMGQyNmUwIiwi

Dr. Martin Luther King, J. (1963, December 18). Speech at Western Michigan University. Kalamazoo, Michigan, USA.

FAA UAS Center of Excellence. (2017). FAA UAS *Center of Excellence Task* A4: UAS *Ground Collision Severity EvaluationRevision* 2. Washington, DC: Federal Aviation Administration.

Federal Aviation Administration. (2018). *Law Enforcement Guidance For Suspected Unauthorized* UAS *Operations – Version* 5. Washington, DC: United States Department off Transportation.

Federal Aviation Administration Office of Airports Safety and Standards. (2016, July 2018). *Airport Safety Media.* Retrieved from FAA.Gov: https://www.faa.gov/airports/airport_safety/media/attachment-1-counter-uas-airport-sponsor-letter-july-2018.pdf

International Committee of the Red Cross. (2016, October 19). *What are the rules of war and why do they matter*? Retrieved from International Committee of the Red Cross: https://www.icrc.org/en/document/what-are-rules-of-war-Geneva-Conventions

Jason Snead, J.-M. S. (2018, April 16). *Establishing a Legal Framework for Counter-Drone Technologies.* Retrieved from The Heritage Foundation: https://www.heritage.org/technology/report/establishing-legal-framework-counter-drone-technologies

Junkin Media . (2016, October 23). Angry farmer shoots down drone hovering over his garde. Los Angeles, CA, USA.

Michael Hamann. (2018, November 18). *Can You Legally Counter a Drone.* Retrieved from Police MAgazine: https://www.policemag.com/486684/can-you-legally-counter-a-drone

MIT Technology Review. (2014, May 16). *Do We Need Asimov's Laws?* Retrieved from MIT Technology Review: https://www.technologyreview.com/s/527336/do-we-need-asimovs-laws/

Nichols, R. K., Mumm, H. C., Lonstein, W. D., Ryan, J. J., Carter, C., & and Hood, J.-P. (2019). *Unmanned Aircraft Systems in the Cyber Domain.* Manhattan, KS: New Prairie Press.

Office of the President of the United States. (2018). *National Strategy for Countering Weapons of Mass Destruction Terrorism.* Washington, DC: United States of America.

Russian Federation. (1996, June 13). Criminal Code of the Russian Federation No. 63-FZ of June 13, 1996 (as amended up to Federal Law No. 18-FZ of March 1, 2012). *Criminal Code of the Russian Federation.* Moscow, Russian Federation: Russian Federation.

Secretary of State for the Home Department. (2019). *UK Counter-Unmanned Aircraft Strategy.* London: HM Government.

United Nations. (2019, November 15). *Member States.* Retrieved from United Nations: https://www.un.org/en/member-states/index.html

United Nations. (2019, October 29). UN *Documentation: International Law.* Retrieved from Dag Hammarskjold Library: https://research.un.org/en/docs/law/courts

Waugh, R. R. (Director). (2019). *Angel Has Fallen* [Motion Picture].

West, H. S. (2019, March 16). *Six Ways to Disable a Drone.* Retrieved from Brookings: https://www.brookings.edu/blog/techtank/2016/03/16/six-ways-to-disable-a-drone/

[1] It is notable that beginning on 2016 Title 49 of the U.S. Code was amended to establish a pilot program for C-UAS mitigation at and around airports and critical infrastructure.

[2] The issue of whether a UAV qualifies as an “occupied aircraft” is currently unclear

[3] The survey of laws listed in tables 12-1, 12-2 and 12-3 are by no means complete in terms of applicable laws within the respective jurisdictions listed or the overall global C-UAS regulatory framework.