UNMANNED VEHICLE SYSTEMS & OPERATIONS ON AIR, SEA, LAND

UNMANNED VEHICLE SYSTEMS & OPERATIONS ON AIR, SEA, LAND

PROFESSOR RANDALL K. NICHOLS, JULIE RYAN, HANS MUMM, WAYNE LONSTEIN, CANDICE CARTER, JEREMY SHAY, RANDALL MAI, JOHN P HOOD, AND MARK JACKSON

NEW PRAIRIE PRESS
MANHATTAN, KS

Contents

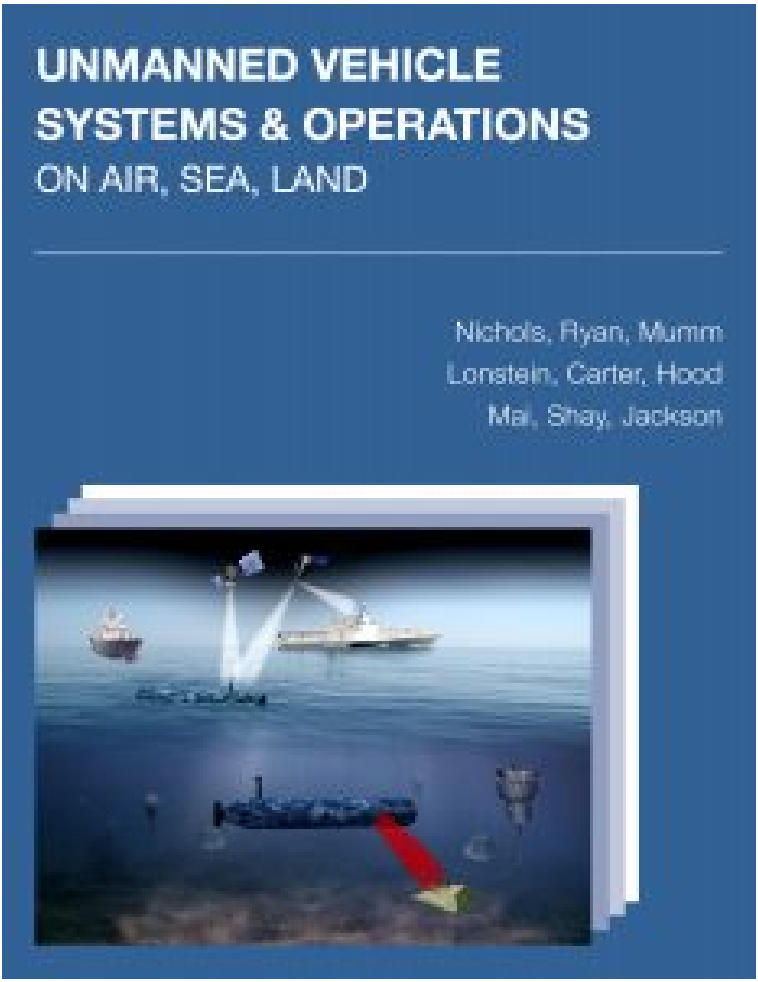
Part I. Main Body

Part II. Section 2: Unmanned Underwater Systems

Part III. Section 3 Unmanned Vehicles for Ground & Land Operations & Penetration of ADS

Title Page

PROFESSOR RANDALL K. NICHOLS, HANS MUMM, JULIE RYAN, WAYNE LONSTEIN, CANDICE CARTER, JOHN P HOOD, MARK JACKSON, RANDALL MAI, AND JEREMY SHAY



UNMANNED VEHICLE SYSTEMS & OPERATIONS ON AIR, SEA, LAND

Copyright / Publication Page

PROFESSOR RANDALL K. NICHOLS

UNMANNED VEHICLE SYSTEMS & OPERATIONS ON AIR, SEA, LAND

By

Nichols, R. K., Ryan, J., J.C.H., Mumm, H.C., Lonstein, W.D., Carter, C., Hood, J.P, Mai, R., Shay, J., & Jackson, M.

Cover design /modifications by R.K. Nichols and Kira Miller
Cover image: Courtesy of *Unmanned Systems News*, General Dynamics Completes Successful Critical Design Review for Knifefish UUV, Retrieved on 09142020 from https://www.unmannedsystemstechnology.com/2013/04/general-dynamics-completes-successful-critical-design-review-for-knifefish-uuv/ (Rees, 2013)

This print edition published by
Professor Randall K Nichols
Salina, KS
ISBN: 9798690020255

References

Dynamics, G. (2013, April). *General Dynamics Completes Successful Critical Design Review for Knifefish UUV*. Retrieved from Unmanned Systems News : https://www.unmannedsystemstechnology.com/2013/04/general-dynamics-completes-successful-critical-design-review-for-knifefish-uuv/

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, (2020) ***Counter Unmanned Aircraft Systems Technologies and Operations.*** 01 February 2020, Copyright 2019-2025, All Rights Reserved, Manhattan: New Prairie Press (NPP). ISBN: 979-8-613302-29-1. https://newprairiepress.org/ebooks/31

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, state, and local law enforcement for keeping our blessed 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.

From: Jeremy Shay

I would like to dedicate this work first to my wife, children, and grandchildren. Their never-ending support inspires me to strive to better myself for them every day. I would also like to dedicate this work to the many mentors, professional peers, and servant leaders I have worked for and with through the years. Without whom I would not have the examples of what a better me could look like. Finally, I dedicate this work to all who use it to equip themselves with the information provided by this team of authors, I have been blessed to work with, and possibly be better for those that look to them as an example.

From Mark J. Jackson:

I dedicate my chapter to my wife, Deborah, and to the memory of my great-uncle, Captain George Richards, a founding officer of the Corps of Royal Electrical and Mechanical Engineers of the British Army. After initially serving in the British Expeditionary Force (Royal Engineers) in France from 1940 – 1941, he quickly rose through the ranks, promoted to captain in 1942 initially serving as an officer in the Royal Engineers, then transferred to the newly-formed Corps of Royal Electrical and Mechanical Engineers specializing in the construction of Bailey bridges in North Africa. Captured in Libya by the German Afrika Corps, he became a prisoner-of-war at Oflag IV located in Colditz, Germany. After demobilization, he became a chartered mechanical engineer working for Imperial Chemical Industries but continued to build model Bailey bridges with his children and nephews.

From Randall W. Mai:

I dedicate my work to my late mother Dorothy M. Thrasher and my two daughters, Courtney J. Mai and Katherine M. Mai. My mother's never ending support and care kept me going. She was my biggest cheerleader. Without her encouragement my life would have taken a much different trajectory. My daughters impacted my life and now my heart will forever go walking around outside me. They are my true mark on this world. I hope they will always believe in themselves and know they can accomplish whatever they set their minds on. And lastly, Professor Nichols has become a valued mentor and true friend. He has helped me to establish balance and pulled from me accomplishments I never thought possible. Thank you Professor Nichols.

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, UUVs, Maritime Cybersecurity 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 Kurt Carraway,UAS Department Head & Executive Director, Applied Aviation Research Center

I am honored to introduce this fourth book, once again led by Professor Randall Nichols and his esteemed colleagues and subject-matter experts on unmanned vehicles and cybersecurity. This compilation of work is thoughtfully broken down into sections including air and underwater domains in which unmanned vehicles operate as well as a section dedicated to unmanned vehicles as weapons and a section focused on geopolitical and legal advances.

The first section, "Unmanned Aircraft Systems," walks students through a series dedicated to the constantly evolving information advances on the topic, including a review on the state-of-the-art, serving as an exploration of current and emerging technologies and some fascinating implications it may have on the UAS industry. The entire section introduces some fascinating applications for UAS—both by the commercial sector as well as the federal government.

Section 2 provides a fascinating glimpse into the maritime domain, with an emphasis on Unmanned Underwater Systems, or UUVs. The introduction focusses on navigational solutions for submarines and UUVs, including a discussion on the use of exteroceptive sensors to supplement map references, and when they do not exist, they may use these sensors for simultaneous

localization and mapping, or SLAM. All of these methodologies are able to operate underwater without the use of global navigation systems—an area where one could argue that their unmanned air counterparts are overly reliant. The UUV section also goes into some depth (pun intentional) on the subject of underwater basing and military applications. Chapter 6 provides a reflection on the history of underwater vehicles, the advancement of sensors and UUV technology and commercial implications for the UUV market. This section is rounded off by chapter 7, a bit of a "deep dive" into UUV design considerations for naval architecture.

Section 3 kicks off by adding historical context on regulatory development pertaining to technologies and an exploration on the subject of multi-domain traffic management systems. It goes on to introduce the counter UAS problem set and uses Iranian attacks on Saudi Arabian oil fields as a case study to illustrate challenges with cyber defense and vulnerabilities posed to Air Defense Systems, followed by an examination of path planning tactics.

In section 4, one chapter stems from a graduate research project in which the author explored how FAA regulations pertaining to UAS operations are influenced by the Fourth Amendment, as well as privacy laws at multiple levels of government. This section also introduces how UVs may be vulnerable to misinformation and disinformation, and the consequences if unaddressed.

Section 5 is fascinating. Carter's chapter on Chinese Unmanned Proliferation Along New Silk Road Sea/Land routes offers some important strategic context on the People's Republic of China. The chapter on crossing the machine-human barrier reviews the risks posed by social media and links its use to acceptance and trust—and then explores how it may be utilized in a nefarious manner. This offers a thought-provoking examination on the broader topic of artificial intelligence and autonomous technology. The final chapter explores the relationship between increased dependencies on the

Internet of Things and how its incorporation into maritime systems may be bringing the industry into the future, but not without broadscale risks from a cybersecurity perspective.

Common threads across all of the sections includes an illustration of how technological advances promote the technical readiness level and implications of unmanned vehicles across all three domains, including military and commercial applications. This is underscored by a theme of considering various levels of autonomy and artificial intelligence across the range of systems—including the topics of dependability, trust, vulnerabilities, and human interaction associated with them.

This body of work is derived from open source references and written by esteemed subject matter experts in their field is a compilation of thought provoking and up-to-date materials for consumption by students of all types. Professor Nichols and his colleagues have done it again!

Kurt J. Carraway
UAS Department Head and Executive Director, Applied Aviation Research Center
Kansas State University Polytechnic
Salina, Kansas

Preface

This is our fourth textbook in a series previously covering the world of *Unmanned Aircraft Systems (UAS) and Counter Unmanned Aircraft Systems (CUAS). Unmanned Aircraft Systems in the Cyber Domain: Protecting USA's Advanced Air Assets, 2nd edition* and *Counter Unmanned Aircraft Systems Technologies and Operations* have seen considerable global recognition in the field. (Nichols R. , et al., 2019) (Nichols R. , et al., 2020)

The authors have expanded our purview beyond UAS / CUAS systems. Our title shows our concern for growth and unique operations **for all unmanned vehicles in all theaters: Air, Sea and Land.** Three different factors have spurred the authors into expanding our textbook offerings. First, unmanned technology has seen an economic explosion in production, sales, testing, specialized designs, and friendly / hostile usages of deployed UAS / UAVs / Drones / UUVs / UDV / UGTs (hereafter referred to as a group as UVs). There is a huge global growing market and entrepreneurs know it. Small UV companies have been reproducing like rabbits. Many companies are exploring / creating new, unique, and profitable unmanned technologies for all military branches, LEO, commercial, high-mountain and deep-sea rescue, and recreational purposes. Covid-19 has brought a new dimension to UV planning and designs for medical and rescue missions.

Second, hostile use of UVs is on the forefront of DoD defense and offensive planners. They are especially concerned with SWARM behaviors in the air, over land and a new threat of underwater. The influence of *IoT, AI and Cyber technologies* has complicated the defense planning mission.

Third, UV technology has outpacing our first and second editions plus our textbook on CUAS. Everyday our writers group read / discussed new UAS / UV developments in navigation, weapons, surveillance, data transfer, fuel cells, stealth, weight distribution,

tactics, GPS / GNSS (and replacement technologies) elements, SCADA protections, privacy invasions, legislation, big-data usage, terrorist uses, cryptographic protections, pressure protection for deep water exploration, maintenance, rescue or intelligence gathering; ASW, and defense; specialized software and security protocols and more. As authors we felt compelled to address at least the edge of some of these new UV developments. It was clear that we would be lucky if we could cover some of the more interesting and priority technology updates for the various UV AOs.

Expanded purview means more experience was needed to write our newest work. We are privileged to add to original writing team of Nichols, Ryan, Mumm, Lonstein, Carter, and Hood new SMEs in the various UV technologies: Mai, Jackson, and Shay. Their extensive backgrounds are found in our tribute to the authors in a latter section.

Here is an outline of topics in our latest work:

SECTION 1: UNMANNED AIRCRAFT SYSTEMS

Chapter 1 Information Advances, Remote ID, & Extreme Persistence ISR **[Ryan]**

Chapter 2 : Unmanned Aerial Vehicles & How They Can Augment Mesonet Weather Tower Data Collection **[Mai]**

Chapter 3 Tour de Drones for the Discerning Palate **[Nichols]**

SECTION 2: UNMANNED UNDERWATER SYSTEMS

Chapter 4 Underwater Autonomous Navigation & other UUV Advances **[Mumm]**

Chapter 5 Autonomous Maritime Asymmetric Systems **[Hood]**

Chapter 6 UUV Integrated Autonomous Missions & Drone Management **[Mumm]**

Chapter 7 Principles of Naval Architecture Applied to UUV's **[Jackson]**

SECTION 3: UNMANNED VEHICLES FOR GROUND / LAND OPERATIONS & Penetration of ADS

Chapter 8 : Unmanned Logistics Operating Safely & Efficiently Across Multiple Domains **[Lonstein]**

Chapter 9 Chinese Advances in Stealth UAV Penetration Path Planning in Combat Environment **[Nichols]**

SECTION 4: UNMANNED VEHICLES WEAPONS FOR C4ISR & POPULATION TRACKING & CONTROL

Chapter 10 UAS, the Fourth Amendment and Privacy **[Shay]**

Chapter 11 UV & Disinformation / Misinformation Channels **[Ryan]**

SECTION 5: UV GEOPOLITICAL & LEGAL ADVANCES

Chapter 12 Chinese UAS Proliferation along New Silk Road Sea / Land Routes **[Carter]**

Chapter 13 Automaton, AI, Law, Ethics, Crossing the Machine – Human Barrier **[Lonstein]**

Chapter 14 Maritime Cybersecurity **[Nichols]**

We trust our newest look at Unmanned Vehicles in Air , Sea and Land will enrich our students and readers understanding of the purview of this wonderful technology we call UV.

Best

Randall K Nichols

Professor of Practice

Director, Unmanned Aircraft Systems (UAS) –

Cybersecurity Certificate Program

Managing Editor / Co-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

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., Carter, C., Lonstein, W., & Hood, J. (2020). *Counter Unmanned Aircreaft Systems Technologies and Operations*. Manhattan, KS: New Prairie Press, #31.

Nichols, R., Ryan, J., Mumm, H., Lonstein, W., Carter, C., & Hood, J. (2019). *Unmanned Aircraft Systems in Cyber Domain: Protecting USA's Advanced Air Assets, 2nd edition*. Manhattan, KS: https://newprairiepress.org/ebooks/27/.

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

Acknowledgements

Books such as this are the products of contributions by many people, not just the musings of the authors. ***Unmanned Vehicle Systems and Operations on Air, Sea, Land*** 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 / OVRP 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, Associate Dean; Professor Troy Harding, 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, Kurt Carraway,UAS Department Head & Executive Director, Applied Aviation Research Center, 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. M.J. Pritchard, Sr. Davis Scientist; Dr. Siny Joseph, ARG, and Associate Professor of Economics; 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, prior Professor and Coordinator of Electronic Publishing at New Prairie Press and Pressbooks,[my mentor in the publishing gig]; Emily Finch and Ryan Otto at NPP; Chad Bailey, Instructor SIS KSUP, Aris Theocharis, our terrific editor; and especially Joel Anderson, KSU OVPR and Research Director.

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, UAS Pilot and Dr Amit K Maitra, Chairman and Founder of Borders and Beyond, Inc., Dr. Bartosz Wojszczyk, President and CEO Decision Point Global and Bart Shields, Inventor and CTO of Olympus Sky, Inc.

Next comes our expanded 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. Randall Mai, Research Technologist for KSU, a Dragon convert, with years of experience in UAS filed operations; Dr Mark Jackson, SME in UUV, naval architecture, and nanotechnologies, Sgt Jeremy Shay, Dragon student, COVID-19 expert, RET USAF, Fabrication Production Manager, Spirit AeroSystems; and Joel Coulter, President, Mobile Sciences Consortium, LLC.

Last, Professor Randall K. Nichols is managing editor / author

/ co-author of nine prior books and developer of six Masters and Certificate programs in Cybersecurity at Utica College and Kansas State University. He has five decades of Cybersecurity experience.

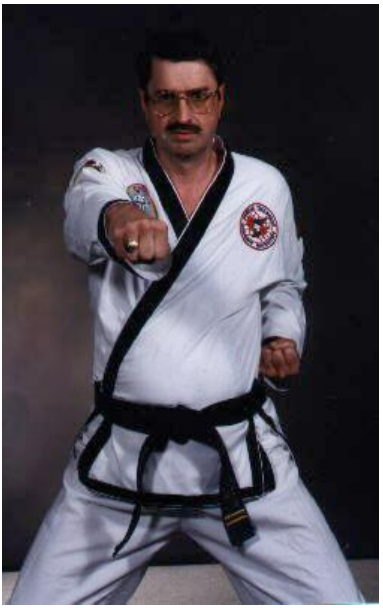
Finally, Montine Nichols deserves a commendation for her help on the final drafts and copy edit work for our book (and living with a real Dragon). Several KSUP UAS pilot – students (now employed) helped with the "student view," and made valid suggestions for improvement, Vincent Salerno, Senior Airman 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 Kira C. Miller who professionally developed (more like "nailed") our cover art four times in a row.

The team especially thanks Assistant Professors Ryan W. Otto, and Emily Finch Scholarly Communication Librarians, for their expert assistance with the NPP final efforts.

Randall K Nichols
Professor of Practice
Director, Unmanned Aircraft Systems (UAS) – Cybersecurity Graduate Certificate Program
Managing Editor / Co-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).

Nichols holds a 3rd Dan Black Belt (R) in Chung Do Kwan Tae Kwon Do and permanent rank of 2nd Dan Black Belt (D). He refereed the National Tae Kwon Do Championships in 1994 in San Antonio , TX.

UNMANNED VEHICLE SYSTEMS & OPERATIONS ON AIR, SEA,

LAND is the 4th textbook in the unmanned vehicle series and his 10th book published. The most recent textbooks in the UAS field ***Counter Unmanned Aircraft Systems Technologies and Operations,*** New Prairie Press (published on February 1, 2020) are available as *free ebooks* at: https://www.newprairiepress.org/ebooks/31/
and
Unmanned Aircraft Systems (UAS) in Cyber Domain: Protecting USA's Advanced Air Assets, New Prairie Press (*NPP 2nd Edition* published on July 26, 2019)
at: https://www.newprairiepress.org/ebooks/27

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 $140M. 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.

Dr. 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).

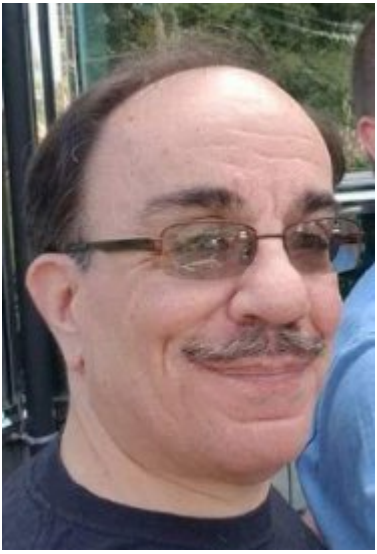
Dr. Ryan came to academia from a career in industry that began when she completed military service. Upon graduating from the U.S. Air Force Academy, Dr. Ryan served as a Signals Intelligence Officer in the Air Force, and then as a Military Intelligence Officer with the Defense Intelligence Agency. Upon 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.

Professor Candice Carter (Co-Author)

Ms. Candice Carter is a cybersecurity expert with over 15 years of hands-on experience in the areas of counterterrorism, counterintelligence and criminal cyber investigations. She conducts Classified/Unclassified briefings in the areas of Terroristic Cyber Capabilities using Social Media and Counterterrorism 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 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. (Associate Dean & 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.

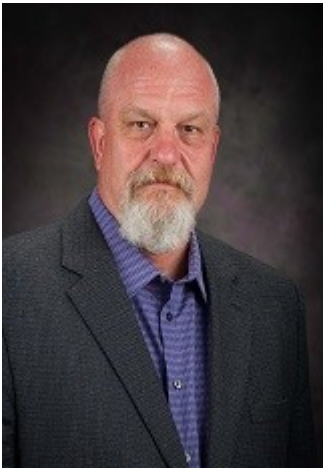
CPT John-Paul Hood USA (Co-Author)

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 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, 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 Geospatial 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 interagency 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).

Jeremy S. Shay, PMP (Co-Author) USAF SMSGT (Ret)

Jeremy is an expert in aerospace maintenance, manufacturing, modification, and maintainability. He specializes in advanced composite structural maintenance and advanced coatings. He recently completed the requirements to earn his PMT Cybersecurity UAS from Kansas State University. His other academic holdings are a Graduate Certificate in Unmanned Aircraft Systems Information Assurance and a Bachelor of Science Degree in Technology Management with a focus on Engineering Technology which is ABET accredited from Kansas State University, an Associate of Science in Aviation Maintenance and Professional Managers' Certification from the Community College of the Air Force, and Project Manager Professional certification from Project Management Institute.

Jeremy currently serves as a Senior Principal Manufacturing Engineer at Northrop Grumman. He recently retired from the United States Air Force as a Senior Master Sergeant with 26 years of service. During this time, he served as a Structural Maintenance and Low Observables mechanic on F-111, F-15, F-16, and B-2 aircraft.

Dr. Mark J. Jackson (Co-Author)

Doctor Mark James Jackson is the McCune and Middlekauff Endowed Professor and University Faculty Fellow at Kansas State University. Born in Widnes, Lancashire, England, in 1967, Doctor Jackson began his engineering career in 1983 when he studied O.N.C. part I examinations and first-year apprenticeship-training course in mechanical engineering. After gaining an Ordinary National Diploma in Engineering with distinctions and I.C.I. prize for achievement, he studied a degree in mechanical and manufacturing engineering at Liverpool Polytechnic and spent periods in industry working for I.C.I. Pharmaceuticals, Unilever Industries, Anglo Blackwells, Unicorn International and Saint-Gobain Corporation. After graduating with the Master of Engineering (M. Eng.) degree with Distinction under the supervision of Professor Jack Schofield, M.B.E., Doctor Jackson subsequently conducted research for the Doctor of Philosophy (Ph. D.) degree at Liverpool in the field of

materials engineering focusing primarily on microstructure-property relationships in vitreous-bonded abrasive materials under the supervision of Professors Benjamin Mills and H. Peter Jost, C.B.E., Hon. F.R.Eng.. He was subsequently employed by Unicorn Abrasives' Central Research & Development Laboratory (Saint-Gobain Abrasives' Group) as materials technologist, then technical manager, responsible for product and new business development in Europe, and university liaison projects concerned with abrasive process development. Doctor Jackson then became research fellow at the Cavendish Laboratory, University of Cambridge, working with Professor John Field, O.B.E., F.R.S., and Professor David Tabor, F.R.S., on condensed matter physics and tribology before becoming a lecturer in engineering at the University of Liverpool in 1998. At Liverpool, he attracted a number of research grants concerned with developing innovative manufacturing processes for which he was jointly awarded an Innovative Manufacturing Technology Centre from the Engineering and Physical Sciences Research Council in November 2001. In 2002, he became associate professor of mechanical engineering and faculty associate in the Centre for Manufacturing Research, Centre for Electric Power, and Centre for Water Resources and Utilization at Tennessee Technological University (an associated university of Oak Ridge National Laboratory), and a faculty associate at Oak Ridge National Laboratory. Dr. Jackson was the academic adviser to the Formula SAE Team at Tennessee Technological University. At Tennessee Technological University, Dr. Jackson established the NSF Geometric Design and Manufacturing Integration Laboratory. Dr. Jackson collaborated with Nobel Laureate Professor Sir Harold Kroto, F.R.S., editing a book on 'Surface Engineering of Surgical Tools and Medical Devices' and a special issue of the International Journal of Nanomanufacturing on 'Nanofabrication of Novel Carbon Nanostructures and Nanocomposite Films'. Dr. Jackson was appointed member of the United Nations Education, Scientific and Cultural Organization's (UNESCO) International Commission for the Development of the 'Encyclopedia of Life Support Systems' Theme

on 'Nanoscience and Nanotechnologies', (http://m-press.ru/English/nano/index.html), and still serves in this capacity. The first edition of the encyclopedia was published 2009 and second edition published 2018. In March 2017, the degree of Doctor of Science (D. Sc.) in mechanical engineering was conferred upon Dr. Jackson in absentia by congregation for sustained contributions made in the area of mechanical engineering and advanced manufacturing over a period of twenty years.

Research Technologist – Randall W. Mai (Co-Author):

Randall grew-up on the family farm in rural Kansas near Tribune. He spent a large sum of his summers helping on the family farm that was established by his great-grandfather in 1929. Before graduating high school Randall was nominated to the United States Naval, Military, and Merchant Marine Academies by Congressman Keith G. Sibelius and Senator Bob Dole. Randall earned an A.S. degree in Mechanical Engineering Technology and a B.S. in Biology / Chemistry minor. Graduating Magna cum Laud. Randall has worked as an engineer in agriculture equipment mfg., an Analytical Chemist / Validation Analysis of computer / software validation for Abbott Labs and currently works as a Research Technologist

for Kansas State University. He is now establishing himself in the Cybersecurity field as he stands on his knowledge of Computer / Software Validation experience gained within the Pharmaceutical field. He was responsible for leading the 21CFRpart11 program at the Abbott Labs facility in McPherson, Ks. and was also responsible for the validation of the Laboratory LIMS and Millenium32 software. The validation encompassed network security and disaster recovery.

Randall will complete a Master program at Kansas State University in May 2020 in Professional Masters of Technology with concentration in UAS and Cybersecurity.

KURT J. CARRAWAY, Col, USAF (Ret) [Foreword to Book 4]

After serving 25 years with the United States Air Force, retired Colonel Kurt J. Carraway is the Unmanned Aircraft Systems (UAS) Department Head and Executive Director of the Applied Aviation Research Center (AARC) at Kansas State University's Polytechnic Campus. As Department Head, Carraway leads UAS faculty in the university's UAS program, which includes a Bachelor of Science in Aviation Technology program, a UAS Minor and a UAS Certificate program. He also serves as a member of the graduate faculty on the campus. As Executive Director, Carraway provides strategic leadership in advancing Kansas State University's UAS program goals. He directs the execution of research activities involving UAS through the AARC. Carraway also directs flight operations development and maturation of the UAS training program through direct supervision

of the Flight Operations staff. He manages highly skilled UAS professionals that perform hundreds of UAS flights per year in civil airspace. He sets policies and procedures for unmanned flight operations. He serves as Principal Investigator (PI) on UAS activities through the AARC and is the University PI representative to ASSURE, the FAA's UAS Center of Excellence.

Before arriving at Kansas State Polytechnic, Carraway was stationed at Camp Smith in Oahu, Hawaii where he served first as Joint Operations Director and then Division Chief of Current Operations, both for the U.S. Pacific Command. Carraway worked with the Global Hawk UAS, as an evaluator and instructor pilot, and later became commander of the Global Hawk squadron. Carraway established standard operating procedures and composed technical manuals for the military's use of the Global Hawk.

A native of St. Louis, Missouri, Carraway received a Bachelor of Science in Mechanical Engineering at the University of Missouri Science and Technology in Rolla, prior to entering the Air Force. During his service, Carraway also completed a Master of Science in Systems Engineering at the Air Force Institute of Technology on the Wright-Patterson Air Force Base in Dayton, Ohio, and a Master of Arts in Management from Webster University in St. Louis, Missouri.

Abbreviations and Acronyms

Abbreviations: Acronyms [Rev 80A] 09212020

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

A-STAR Heuristic search algorithm discussed in chapter 9

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

ABMS Advanced battle management system

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

ADAPs Adaptive compute acceleration platforms

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.

AGV Autonomous Guard Vehicle

AHA Autopilot Hardware Attack

AHD Analog high definition

AHRS Attitude and heading reference system

AI Artificial intelligence: "1. a branch of computer science dealing with the simulation of intelligent behavior in computers and 2: the capability of a machine to imitate intelligent human behavior." (Merriam-Webster, 2020)

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-Qaeda 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

ART Autonomous Rail Transport

ARW Anti-radiation weapons

AS Airborne Sensing Systems

ASB Advisory Service Bulletin / Air Sea Battle

ASBM Anti-ship ballistic missile

ASCM Anti-ship cruise missile

ASEA Active electronically scanned arrays

ASEAN Association of Southeastern Asian Nations

ASICs Application specific integrated Circuits & circuit boards

ASL Airborne Systems Laboratory

ASMS Automated Separation Management System

ASR Chinese Air Silk Road

ASOS Automated surface weather observation 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

ATN Aids to Navigation (aka ATON)

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

AWOS Automated weather observation system

AWSAS All Weather Sense and Avoid System

B IF equivalent bandwidth, Hz

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

BAMS Broad Area maritime surveillance

BATS Bermuda Atlantic Time-series Study

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

BPAUV Battlespace preparation autonomous underwater vehicle

BRI Chinese 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 CyA)*

C/A Civilian acquisition code for GPS

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 /Connectivity & automation in transport

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*

CCMCPS Cooperative Cognitive Maritime Cyber Physical System

CCS Cyber Counter Sabotage

CCT Cyber Counter Terrorism

CC-UAS Counter-Counter Unmanned Aircraft Systems

CD Conflict Detection

CDL Common datalink

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

C/NA Communication / Navigation Aid

CM / CyM *Countermeasure* / 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

COOP Cooperative Observer Program

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

CPS Cyber-physical systems

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-STAR Variation of A-STAR algorithm suitable for solving path planning problems in unknown environments

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

DCL Drone Champions League

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

DEM Digital elevation model

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 Datalink interface

DNA Deoxyribonucleic acid

DoD Department of Defense

DOF Degrees of Freedom

DVL Doppler velocity log

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

DROV Remote operating vehicle

DSA Detect, sense and avoid / Dynamic Sense-and-Act

DSR Chinese Digital Silk Road

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

EFF Electronic Frontier Foundation

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
EPIRB Emergency Positioning -Indicating Radio Beacon
EQUAS Explainable question answering 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 *Fundamental 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

FIIP Floating Integrated Information Platforms

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

Floats Floating sensors (USN)

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

FY Fiscal year

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

GDP Gross Domestic Product (USA)

GDPR European Union's (EU) General Data Protection Regulation

GDT Ground data terminal

GEO Geostationary Earth orbit satellite

GEOINT Geospatial-Intelligence

GeoFence A geo-fence is a virtual perimeter for a real-world geographic area

GIGO Garbage in, garbage out

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)

HCE Highly contested environment

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

Human "a bipedal primate mammal (Homo sapiens), a person" (Merriam-Webster, 2020); Humanity "the quality or state of being human." (Merriam-Webster, 2020)

Humanoids "a humanoid being: a nonhuman creature or being

with characteristics (such as the ability to walk upright) resembling those of a human."

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 / Industrial control systems

ID Information Dominance / Inspection and Identification /Identification

IEDs Improvised Explosive Devices

IEEE Institute of Electrical and Electronics Engineers

IETM Interactive Electronic Maintenance Manuals

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
IOB Internet of bodies
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
ISCS Integrated shipboard control systems
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
JADC2 Joint all-domain command & control
JADO Joint all-domain operations (Thatcher, 2020)
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

JST Japan Time zone

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

KSU Kansas State University

L $\lambda / 2$ 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 / Law Enforcement Officer

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)

LORAN-C Long Range Navigation, Revision C

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
LUSV Large Unmanned Surface Vehicles
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
MARIN Maritime Research Institute Netherlands
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
Mesonet network of automated weather and environmental monitoring stations designed to observe mesoscale meteorological phenomena

MCE Mission control element

MCM Mine countermeasures

MCU Master Control Unit

MCVs Mesoscale convective vortices

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 take-off 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

ML Machine learning techniques

MLRS Multi launch rocket systems

MLU Mid-life upgrade

MMI Man-machine interface

MORS Military Operations Research Society

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

MPA Maritime patrol aircraft

MPI Message-passing interface

MPC Model-based predictive control

MPO Mission payload operator

MR Medium range / Maritime Reconnaissance

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)

MSSM Multi-step optimization method to achieve re-planning for stealth UAV penetration of ADS

MTCR missile Technology Control Regime

MTI Moving target indication

MTOM Maximum take-off mass

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 /Maritime Transportation Systems / Sector

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

MUSV Medium Unmanned Surface Vehicles

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[i]

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

NEMESIS Netted Emulation of Multi-Element Signature against integrated Sensors (USN)

NGA National Geospatial Intelligence Agency

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

NOAA National Oceanographic and Atmospheric Administration

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

NTM/NTOM Notice to mariners

NTSB National Transportation Safety Board

NTT Non-Threat Traffic

NULLO Not using live operator (USAF)

O Other methods of CR

OEM Original Equipment Manufacturer

OIO Offensive Information Operations

OLOS Out-of-the-line-of-sight

OODA Decision Loop: Observe, Orient, Decide, Act

OoT Ocean of Things (USN) (DARPA)

ONR Office of Naval Research

OPA Optionally piloted aircraft

OPAV Optionally piloted air vehicle

OPSEC Operations Security

OSI Open systems interconnection

OT Operational technology

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 sub-atomic particles moving at relativistic velocities.

PBL Planetary boundary layer

PCAS Persistent close air support

PCS Personal Communication Services

PEIRP Transmitter 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 People's Liberation Army Navy (China)

PLC Programmable Logic Controllers

PLOCAN Research facility Oceanic Platform of the Canary Islands

PMIAA Permissions Management: Identification, Authentication and Authorization

PNF Plug and Fly with custom transmitter, receiver, battery, and charger

PNT Reliable communications; positioning, navigation, and timing

PO Psychological Operations

POS Position and Orientation System

POV Point of View

PPP Precise Point Positioning

PPS Precise positioning service (GPS)

PRC People's 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

PS Pressure sensor

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)for military positioning

QOS Quality of Service in HAPs

QR QR code is a type of matrix barcode which is machine or phone readable

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

Remote ID Remote ID has two meanings in this textbook. It is used as an information / technology device to identify people from a UAV. This term is used in the UAS industry and the FAA as a mechanism for identifying an aircraft type and the registrant from the ground, essentially a digital license plate and registration.

RES Radio electronic systems

RF Radio Frequency

RGB Red Green Blue for VIS camera
RGT Remote ground terminal
RIAS Research Institute for Autonomous Systems -University of North Dakota
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)
ROV/ROUV Remote operating vehicle / Remotely operated underwater vehicle
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

SAHRV Semi-autonomous Hydrographic Reconnaissance vehicle

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

SINS Ships inertial navigation systems

SJM Salafi-Jihad Movement

SKASaC Seeking airborne surveillance and control

SKYNET Fictional artificial intelligence system that becomes self-aware

SLAM Simultaneous localization and mapping

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

SOLAS Safety of Life at Sea (International Maritime Convention)

SONAR Sound Navigation and Ranging

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

SPURV Special purpose underwater research vehicle

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

ST&T Submarine Track and Trail

STANAG 4856 Standard interfaces of UAV Control System for NATO UAV

STK Satellite tool kit

STOL Short take-off and landing

sUAS Small Unmanned Aircraft System

SubT Subterranean Challenge Urban Circuit

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: Technology readiness levels are a rating method developed by NASA to describe where a technology is in terms of its development. The lowest levels (1 – 3) are technologies that are being researched, the middle levels (4 – 6) are technologies that are being prototyped and tested, and the highest levels (7 – 9) are technologies that are being demonstrated and used. (NASA, 2017)

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
UG Underwater glider (USN)
UGCS Unmanned Ground Control Station
UGS Unmanned ground-based station
UGT Unmanned ground transportation
UGV Unmanned ground vehicle
UHF Ultra High Frequency, 300 MHz – 3 GHz
UIT Unintentional Insider Threats
UK United Kingdom
UL Upload link
ULC Uniform Law Commission
ULPCG University of Las Palmas de Gran Canaria
UMTS Universal Mobile Telecommunications System
U.N. United Nations
UND University of North Dakota
UNESCO United Nations Educational, Scientific and Cultural Organization
UNICEF United Nations Children's Fund
US United States
USCG United States Coast Guard
USCGA United States Coast Guard Auxiliary
USD Unmanned surveillance drone
USS Undersea Search and Survey
USV Unmanned surface vehicle

UTM Unmanned Traffic Management / Safe Uniform Traffic Management

UTV Unmanned target vehicle

UUV Unmanned underwater / undersea vehicle

UV Unmanned Vehicle

UUNs / DUNSs Urgent / deliberate universal needs statements

V Visible

VFR Visual flight rules

VHS Very High Frequency Radio

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

VTC Vessel traffic control

VTM Vessel traffic management

VTOL Vertical take-off and landing

VTUAV Vertical take-off UAV

WABN wide available broadband networks

WARM identify war reserve mode emissions

WEF World Economic Forum

WEZ Weapon Engagement Zone

WMD Weapons of Mass Destruction

WRC World Radio Conference Standards Organization

XLUUV Extra-large unmanned undersea vehicle

XO Executive Officer of Naval vessel

ZIGBEE or KILLERBEE Sniffing / penetration tools specific to UAS

Greek / Mathematical 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

υ UAV velocity vector and UAV speed (ms -1)

θ Horizontal angle in inertial axes (rad)

Ψ Vertical angle in inertial axes (rad)

x,y,z Inertial position coordinates (m)

κ Curvature (m-1)

τ Torsion, (m-1)

r(q) Path, with path variable (q)

h Path length (m)

e Basis axes vector set

P(x, y, z, θ, Ψ) UAV pose where: where x, y, z, is the UAV location or waypoint and (θ, Ψ) are the horizontal and vertical angles , respectively

Ps Starting pose for UAV moving to

Pf Finish pose

Ị Path constraint in (9.4)

a lateral acceleration proportional to curvature k

∞ vector operator in (9.6)

f(n) Path cost function in (9.9)

g(n) cost of path from start node n to the goal

h(n) Heuristic function which estimates the distance from the next node n on the path to goal in (9.9)

h(X) represents actual journey cost from goal X

g(X,E) represents the estimate journey cost from state X to the current position of the stealth UAV in (9.10)

N Length of the prediction domain in (9.11) & N steps in (9.12)

W length of the control domain in (9.11)

qi Output prediction error

qj Is the weighting coefficient of the control variable in (9.11)

k Kth node for prediction of cost of predicted flight path in MPC (9.12)

3-D	three dimensional

Special Definitions

Asymmetric warfare can describe a conflict in which the resources of two belligerents differ in essence and, in the struggle, interact and attempt to exploit each other's characteristic weaknesses. Such struggles often involve strategies and tactics of unconventional warfare, the weaker combatants attempting to use strategy to offset deficiencies in quantity or quality of their forces and equipment. (Thomas, 2010) Such strategies may not necessarily be militarized. (Steponova, 2016)

This is in contrast to *symmetric warfare*, where two powers have comparable military power and resources and rely on tactics that are similar overall, differing only in details and execution. (Thomas, 2010)

Sources plus Bibliography below: (Nichols R. K., Unmanned Aircraft Systems In the Cyber Domain: Protecting USA's Advanced Air Assets. 2nd Ed. Manhattan, KS: New Prairie Press., 2019) and (Nichols, et al., Counter Unmanned Aircraft Systems Technologies and Operations, 2020)

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 R. K., et al., Unmanned Aircraft Systems in the Cyber Domain, 2019) and (Nichols, et al., Counter Unmanned Aircraft Systems Technologies and Operations, 2020) Other definitions from the following references:

References

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

Adamy, D. (2015). *EW Against a New Generation of Threats.* Boston: 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

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*.

Angelov, P. (2012). *Sense and avoid in UAS research and applications.* Hoboken: NJ.

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

Army, U. (1992, November 23). US Army Field Manual FM 34-40-7. *Communications Jamming Handbook*.

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.

Barnhart, R. K. (2012). *Introduction to Unmanned Aircraft Systems.* New York: CRC Press.

Beaudoin, L. e. (2011). Potential Threats of UAS Swarms and the Countermeasures Need. *ECIW*.

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.

Dalamagkidis, K. V. (2012). *On Integrating Unmanned Aircraft into the National Airspace System, 2nd edition.* Denver, CO: Springer.

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 Missle Threats.* Washington, DC: DoD.

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/

Durham, W. (2013). *Aircraft Flight Dynamics and Control.* The Atrtium, Chesterton, UK: Wiley.

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

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/

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

Eshel, T. (2019, September 14). *AFRL to Test a Drone-Swarm Killer HPM.* Retrieved from Defense Update: https://defense-update.com/20190923_hpm.html

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

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/

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

Filbert, F. &. (2014, (July – August). *Joint Counter Low, Slow, Small Unmanned Aircraft Systems Test. Fires PB644-14, no 4.* Washington: DoD.

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

Fitts, R. (1980). *The Strategy of Electromagnetic Conflict.* Los Altos, CA: Peninsula Publishing.

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/

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/

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/

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.

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

Horowitz, E. (1978). *Fundamentals of Computer Algorithms*. Potomac, MD: Computer Science Press.

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.

Ibrahim, A. (2019). *Optimization Methods for User Admissions and Radio Resource Allocation for Multicasting over High Altitude Platforms* . Memorial Univeresity 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-Satellities. *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.

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*.

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

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

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/

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

Lipschutz, M. (1969). *Schaums Outline for Differential Geometry.* NYC: McGraw-Hill .

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

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) – thePhilosophy 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).

Marshall, D. M. (2016). *Introduction to Unmanned Aircraft Systems, 2nd Edition.* New York: CRC Press.

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. (2020, August 5). *Definition of human (Entry 2 of 2).* Retrieved from Merriam-Webster.com: https://www.merriam-webster.com/dictionary/human#h2

Merriam-Webster. (2020, August 11). *humanity noun.* Retrieved from Merriam-Webster.com: https://www.merriam-webster.com/dictionary/humanity

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.

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.

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

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

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.

N/A. (2020, July 25). *Cambridge Dictionary on line.* Retrieved from dictionary.cambridge.org/us/: https://dictionary.cambridge.org/us/

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 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. (2008, September 05). Counterintelligence & Sensitive Compartmented Information Facility . *(SCIF) Needs – Talking Points.*

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.* Alaxandria, 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. M., & & Hood, J. P. (2020). *Counter Unmanned Aircraft Systems Technologies & Operations.* Manhattan, KS: New Prairie Press #31.

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.

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., Ryan, J., Mumm, H., Carter, C., Lonstein, W., & Hood, &. J. (2020). *Counter Unmanned Aircraft Systems Technologies and Operations.* Manhattan, KS: New Prarie Press #31.

Nichols, R., Ryan, J., Mumm, H., Lonstein, W., Carter, C., & & Hood, J. (2019). *Unmanned Aircraft Systems (UAS) in Cyber Domain: Protecting USA's Advanced Air Assets, 2nd Edition.* Manhattan, KS: New Prairie Press #27 .

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.

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

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

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.* Manhatten, 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, D. J. (2000). *Defending Your Digital Assets against Hackers, Crackers, Spies and Thieves.* New York: RSA Press.

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.

Rani, C. M. (2015). Security of unmanned aerial vehicle systems against cyber-physical attacks. *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*.

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

Reklaitis, G. R. (1983). *Engineering Optimization: Methods and Practices*. Boston: Wiley.

Reklaitis, G. R. (1983). *Engineering Optimization: Methods and Practices*. Boston: Wiley.

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). ACompact 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

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

Singer, P. W. (2010, February 25). Will Foreign Drones One Day attack the US? . *Newsweek*.

Skolnik, M. (2008). *Radar Handbook, 3rd Edition*. Boston: McGraw Hill.

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

Steponova, E. (2016). 2008 Terrorism in Asymmetrical Conflict. *SIPRI Report 23.*

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

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.

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 ChannelCharacterization 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*.

Tewari, A. (2011). *Advanced Control of Aircraft, Spacecraft and Rockets*. Chichester, UK: Wiley.

Thatcher, M. K. (2020, August 9). *Integrated Joint All-Domain Operations Full Spectrum Operations.* Retrieved from www.lockheedmartin.com: https://www.lockheedmartin.com/content/dam/lockheed-martin/aero/documents/mdo/Integrated_JADO_Solution_Whitepaper.pdf

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

Thomas, R. (2010). Relearning Counterinsurgency Warfare. *Parameters*, PDF.

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

Tsourdos, A. &. (2011). *Cooperative Path Planning of Unmanned Aerial Vehicles* . Reston, VA: American Institute of Aeronotics and Astronautics, Vol #235.

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. (2019b)*. 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

Wikipedia. (2020, July 26). A* *Algorithm*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/A*_search_algorithm

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*.

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

2016. 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.

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

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).

Zhang, Z. W. (2020). Rapid Penetration Path Planning Method for Stealth UAV in Complex Environment with POP-UP Threats. *International Journal of Aerospace Engineering*, TBA.

[i] FM 34-40-7

Detailed Table of Contents

Table of Figures

Table of Tables

Table of Equations

Chapter 9: Chinese Advances in Stealth UAV Penetration Path Planning in Combat Environment [Nichols]

SECTION 4: UNMANNED VEHICLES WEAPONS FOR C4ISR & POPULATION TRACKING & CONTROL

SECTION 5: UV GEOPOLITICAL, MARITIME & LEGAL ADVANCES

Table of Appendices

Section 1: Unmanned Aircraft Systems

PART I

MAIN BODY

1. Chapter 1 Information Technology Advances, Remote ID,[1] & Extreme Persistence ISR [Ryan]

Student learning objectives. After reading this chapter, students should be able to do the following:

- – Identify, describe, and explain the advances in technologies that affect unmanned system design and use
- – Discuss the impacts of technology advances on the ability to remotely identify individuals
- – Discuss how energy availability affects the range and duration of unmanned system operations

The Emerging World of Unmanned Vehicle Uses

As noted in the preface to this book, unmanned technology has undergone a growth explosion. Innovations in production, sales, testing, specialized designs, and uses continue to push the adoption of unmanned systems into new markets while expanding its use in existing markets. The improvement in the underlying technologies, such as cameras, have enabled many new uses. Further, use in one area can inspire use in another area as knowledge about capabilities spreads. The first types of jobs that are being tasked to unmanned vehicles are typically the ones that are dangerous or relatively expensive to use humans to execute. The next types of jobs being assigned to unmanned vehicles are the repetitive but simple tasks that are less expensive to execute without humans. Examples of some of the emerging uses of unmanned systems include the following:

- Governmental uses, such as for military purposes and population control. The use of unmanned systems by military forces includes bomb disposal robots, surveillance drones, and battle damage assessment (Page, 2020). Police forces use them for "mass surveillance, crime investigation, search and rescue operations, locating stolen goods, and surveying land and infrastructure." (Electronic Frontier Foundation, 2017)
- Emergency services, including first responder support and humanitarian relief. These types of applications assist emergency personnel in finding victims, surveying disaster areas, and getting relief supplies to people who would otherwise be unreachable. (CB Insights, 2020)
- Construction and infrastructure. Drones are being used to not only monitor the progress of construction (Burger, 2019) but also to move supplies around construction zones. An emerging use of drones is to actually construct buildings: a proof of concept experiment in Switzerland used drones to "lift and stack thousands of polymer bricks… to create a geometric structure nearly 10 meters high" (CB Insights, 2020).
- Crime. From transporting drugs and contraband into prisons and across borders to delivering bombs and spying on people, unmanned systems provide a cost effective and risk reducing capability to determined criminals. (Swales, 2019)

Predictably, some of the uses are hostile to one or more parties. Of course, hostility is in the eyes of the beholder: a criminal views law enforcement use of unmanned surveillance technology as hostile to their interests; a pro-democracy protestor views population surveillance as hostile and adversarial. The point is, of course, that the technology itself is agnostic as to usage and that it is growing in leaps and bounds, with innovations in both the underlying technology base and in the use of the technology coming seemingly every day.

In order to understand how the uses of unmanned systems can evolve and adapt, it is necessary to keep tabs on how the component

technologies – sensors, communications, controls, etc. – are evolving. This chapter provides an overview of these advances from the perspective of unmanned systems. Many advances in technologies and uses have occurred, with some of the most interesting being in the marrying of information technologies – imagers, signal sensors, etc. – with advances in aeronautics, energy sources, and engine technologies. In this chapter, we will look some of the more interesting technology changes and explore some implications.

Information Technologies

When talking with people about unmanned systems, it is sometimes surprising to realize that they do not fully appreciate the fact that few systems are fully autonomous. When something is unmanned, it just means that the "manning" is outsourced. But what is "manning" and what is "outsourcing"?

"Manning" implies a lot of things, most specifically that a human is in the operational loop in the same location as the equipment being operated. When a piece of equipment is "unmanned", then one or more of those elements is different. It may be that a human is still in the operational loop, but at a different location. It may be that some aspect of human intelligence has been automated and integrated into the equipment. Or it may be a combination of those. Outsourcing is when one or more tasks that one person would do is given to another entity to perform. Aspects of human labor are most easily outsourced to machines but could also be outsourced, when possible, to distant people. Aspects of human intelligence can be outsourced to smart machines, to distributed groups of people, or to companies. Therefore, when we say that "unmanned means that manning has been outsourced", we are really saying that some aspects of human labor and cognition have been separated out and assigned to some mix of distant humans, distant machines, and on-premise technologies.

The operations of any unmanned system is complex. As noted in Nichols et al (2020):

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. 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.

The separation of human labor, cognition, and equipment into disparate pieces means that a concomitant need for collaborative technologies becomes important. The most obvious collaborative technologies are communications – exchanging data, commands, and responses. Other types of collaborative technologies that need to be considered are those that prevent adverse interactions between system components, environmental sensing and reaction technologies, and control guidance technologies. All of these enable the remote operation of an unmanned system.

When considering the operation of anything that is unmanned, be it an earth-bound robot or a high-flying weather balloon, it is very useful to think about two things: where the intelligence associated with the operations is located, and how the intelligence is divided between elements. The process of automation is fundamentally the process of taking elements of human intelligence and replicating those elements in machines. Advances in automation follow the development of technologies that allow increasing distance

between humans and their tools, but also follow a fairly predictable cycle of development, use, integration, and innovation. Successful innovation can both restart the cycle and spawn separate cycles.

In order to explore advances in information technology as applied to unmanned systems, we will look at the several general categories of technologies and how they are poised to affect the future of unmanned systems. When appropriate, examples of real-world implementations will be provided. (The use of these examples does not constitute endorsement: they are simply examples of what is going on in the world.) The general categories of technologies covered are:

- Internet of Things (IoT)
- Artificial Intelligence
- Advanced Manufacturing

In addition, a short look at energy advances is included, because without portable and sufficient energy, unmanned system operations are limited.

Internet of Things (IoT)

The term "Internet of Things" was coined to describe the network of everyday items (such as thermostats, toasters, and pet collars) that have been enhanced with information technology and enabled with communicative capabilities. The simplicity of the term belies the extraordinary complexity of the reality. Billions of devices sharing data over the internet means that tons of very granular data can be combined to create new knowledge. Moreover, the direct connection to each device enables a level of control that transcends the individual component. Within the last decade, major advancements in two fundamental technologies, sensors, and wireless communications, have led to an explosion of the IoT. According to SAS, there are "127 new IoT devices connected to the internet every second" and there will be "more than 150 billion devices connected across the globe by 2025". Further, "the global

datasphere will grow from 33 zettabytes in 2018 to 175 zettabytes by 2025." (SAS, 2019)

The phenomenon of linking many small devices over very large networks is one aspect of the IoT. There are also geographically smaller implementations of interconnected devices that create what can be effectively considered a swarm of minimally intelligent elements collaborating for a larger purpose. One such implementation has been called an **"internet of bodies" (IoB),** where human bodies wearables and embeddables are connected to a network. The initial purpose of IoB has been to augment health treatments, diagnoses, and monitoring, but once human health and behavioral data is being shared and accessed via the greater Internet, many possibilities emerge, including the merging of human and machine capabilities over great distances.

Near Term IoT Technologies

According to Strativerse, a collaborative research effort that "analyzed the capabilities of current technologies and their likely trajectory" (L'atelier BNP, 2020), there are several technologies that are at *technology readiness levels* [2] (TRL) 7 or higher that are worthy of consideration. These include data marketplace, simultaneous localization, and mapping (SLAM), and digital twinning. Those near-term technologies are already being used in some areas but could be more widely adopted in the coming years as the infrastructure support for them expands.

Data marketplace is the term given to a service that allows people to buy and sell data. Buying and selling data is nothing new but the adoption of marketplaces to connect buyers and sellers has made the practice more convenient and efficient. As noted by Jeremiah Smith, data marketplaces provide the following advantages:

- ***Crowdsourcing:****by making self-serve data selling a reality, they provide the solution to move away from inaccurate/expensive single-source data.*
- ***Aligned incentives:*** *data owners/collectors directly benefit from keeping data in structured form and making it available to others.*
- ***Standardization****: by design, a marketplace defines a common data model and interface for buyers and sellers to exchange data.*
- ***Fairness:*** *instead of a having a central authority pricing data, providers can set their own prices while consumers can choose who they buy from.* (Smith, 2018)

How might this affect unmanned systems? A big effect might be increased use of unmanned systems by individuals: smaller operations are incentivized because it makes collecting and selling data, even as a single person operation, possible. This incentive makes it attractive to collect more data and to compete for buyers on both price and accuracy. Over time, this could translate to aggregation of data providers, making the business case for operating large fleets of unmanned systems for the purpose of purely commercial data collection.

Simultaneous localization and mapping (SLAM) is already in use by some unmanned systems and should be expected to expand to many more. Imagine being taken into an unfamiliar building and being asked to draw a detailed and accurate map. You don't know where you are, you don't know the dimensions of any of the rooms or even how many there are, and you don't know if there are stairs or elevators. When you start drawing the map, by measuring first what is around you and then moving outward, you are doing simultaneous localization and mapping. Asking a human to do this is tricky but ultimately doable, because of the experiences that the human has accumulated over a lifespan with navigating and mapping. Teaching a robot to do this more difficult because the problem is inherently paradoxical: in order to know where it is, the robot needs a map, but in order to make a map, the robot needs to

know where it is. Furthermore, as it moves, it does not know where it is going. (Martin, 2019) (Burgard, Stachniss, Arras, & Bennewitz, 2020)

The benefits of getting SLAM right are pretty obvious: drop an unmanned system into a danger zone and let it figure out how to navigate. Send a robot to another planet and let it find its way around. Launch an unmanned underwater vehicle to explore a deep canyon. Send a drone into a cave system to explore. As the technology matures, it will increasingly be used to assist unmanned systems in navigation, as well as provide important real time improvements in the quality of data about our physical environment.

Digital twins are highly detailed computer models of actual systems, which are different from other models in that they are continually updated with data from the actual system so the model reflects the current operational status accurately. The key to successful implementations of digital twins is the data feed between the system and the twin: the digital thread. The distinction between the twin and the thread is time: "the digital twin is the current representation of a product or system, mimicking a company's machines, controls, workflows, and systems. The digital thread meanwhile is a record of a product or systems lifetime, from its creation to its removal." (Miskinis, 2018)

The benefits to unmanned systems lie in the ability to exploit the real time aspects of the twin in order to detect and react to challenges faster. The thread provides a way of analyzing the longitudinal aspects of the system. For example, if "a vehicle has an accident due to the fault of the system such as unplanned acceleration, the digital thread through having traceability across the lifecycle of a vehicle, will be able to identify the issue." (Miskinis, 2018)

Longer Term IoT Technologies

Atomic scale storage is an experimental approach to encoding information in atoms. It is currently at TLR 4 and can only be done in a laboratory. The promise of this technology is intriguing: "the storage density of this memory is 500 times larger than that of state-of-the-art hard disk drives. If perfected, this technology could enable the manufacturing of memory cards with capacity of 62 terabytes." (L'atelier BNP, 2020)

A synthetic doppelganger is a "realistic robot powered by advanced artificial intelligence with the ability to emulate one's personality and subsequently substitute for them." (L'atelier BNP, 2020) The idea here is that a "human brain would be scanned and digitized, with the resulting content being fed into an artificial neural network." (L'atelier BNP, 2020) The application to unmanned systems would be in using the synthetic copy to operate in places where human bodies are not well suited, such as space or underwater, with the full learning, deciding, and personality cues of the original human. This technology is at TLR 3 and faces many challenges before being realized. (L'atelier BNP, 2020)

Artificial Intelligence (AI)

The growth and promulgation of both weak and strong AI is already evident in many aspects of our lives. The integration of AI into unmanned systems holds a lot of promise. As noted in Nichols (2020):

… 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, trade offs 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. (Nichols, et al., 2020)

There is an enormous amount of progress being made in realizing applications of AI. Three of the emerging technologies are already being incorporated into unmanned systems: facial recognition, gait recognition, and gesture tracking.

Facial recognition has gained a bit of notoriety because of some governmental applications. The use of facial recognition capabilities in unmanned systems is useful for threat recognition as well as for commercial purposes, such as urban planning. Understanding who goes where in a city and when can be extremely important information for city management purposes.

Abuses of human rights, however, have made it a controversial capability. By 2019, 64 countries were using facial recognition for surveillance purposes. (Feldstein, 2019) China in particular has made extensive use of facial recognition in many sectors, including "from catching criminals in huge crowds to detecting and shaming jaywalkers to deciding whether someone can get an extra square of

toilet paper in a public bathroom." (Samuel, 2018) This technology has been used in unmanned systems, with a new level of secrecy and disguise has been reached through the development of robotic birds for population surveillance. (Chen, 2018) "The drones have wings that flap so realistically they're difficult to distinguish from actual birds. In fact, animals on the ground often can't make the distinction, and even real birds in the sky sometimes fly alongside the drones." (Samuel, 2018)

Gait recognition is less widely proliferated but of great interest to augment facial recognition and other identification methods. Gait recognition is based on analyzing how people walk. Even those who have very similar faces move differently. "One promising extension of gait recognition is to use inputs from multiple or moving cameras … (e.g., cameras installed on drones) [to] actively detect people behaving suspiciously by capturing pedestrians from different viewpoints." (Shigeki, Okura, Mitsugami, Hayashi, & Yagi, 2018)

Gesture tracking, which is a technology that captures how people move, enables a new type of interface for computer system control. While the early implementations of gesture-based controls relied on instrumented gloves and other wearables, the use of computer vision and other sensing systems has freed the human from having to don equipment. "Gesture-based technology is already in place and commonly used (e.g., public buildings, public restrooms) without special instruction required for effective use. A common example of a well-designed gestural command is the use of hands to "wave" to activate (e.g., public bathroom faucet)." (Elliott, Hill, & Barnes, 2016) The use of gestures to control unmanned systems can enable a more intuitive and rich interface with the systems. "Navigating and controlling a mobile robot in an indoor or outdoor environment by using … hand gestures offer some unique capabilities for human–robot interaction inherent to nonverbal communication with features and application scenarios not possible with the currently predominant vision-based systems." (Stancic, Music, & Grujic, 2017)

Advanced Manufacturing

From creating new materials to creating new ways to use materials, manufacturing is being affected in ways that change many aspects of system use. Two technologies in particular are having impacts on the use of unmanned systems: 3-D printing and auxetic material.

3-D printing can be done in many different ways, such as adding material incrementally to create something or incrementally removing material to create something. Swarm 3-D printing occurs when many small printers are connected together in a swarm. Each part of the swarm is assigned a small task. The collaboration makes 3-D printing of very large projects possible. (L'atelier BNP, 2020) The combination of the swarm approach to 3-D printing with unmanned systems opens up a wide variety of potential applications, including creating structures in remote or inhospitable areas.

Auxetic materials are those that can "react to changes in their physical environment" and which can act as sensors by virtue of harnessing that change. (L'atelier BNP, 2020) Auxetic materials act differently than normal materials: they get "wider when stretched and narrower when squashed." (Mir, Ali, Sami, & Ansari, 2014) They also "possess attractive acoustic properties, and it is found that at frequencies up to 1600 Hz auxetic forms of polymeric and metallic foams possess enhanced acoustic absorption." (Mir, Ali, Sami, & Ansari, 2014) Current applications include smart bandages, which act both as sensor for detecting when medicine is needed and as protection for wounds. The integration of auxetic materials into unmanned systems for enhanced resiliency and acoustic absorption is intriguing. There is also an application of these types of materials to create a new type of prosthetic, such as a gripper, that is "smaller, more energy efficient and more puncture resistant." (Chin, 2019)

Energy Sources

One never-ending challenge for automated systems of all types is energy access and availability. Approaches to managing this

challenge include reducing energy usage, improving energy efficiency, and creating power sources that have a higher energy density. Lighter weight materials in unmanned systems contribute to energy management, as do the incorporation of renewable energy sources in systems (such as solar panels). Advances in energy storage technologies, such as batteries, are being made as well.

Nuclear energy is contributing to small and portable energy applications. A research team looking to "develop an energy source that is both small and light, and produces more power for a longer time" (MaterialsToday, 2009) created a battery that uses radioactive material. The use of advanced materials for sealing and shielding the battery enables it to be used in a variety of applications. (MaterialsToday, 2009) This work has continued in many different labs, with an expectation that commercial use of nuclear batteries could be achieved by the mid-2020s. "The space industry would also greatly benefit from compact nuclear batteries. In particular, there is a demand for autonomous wireless external sensors and memory chips with integrated power supply systems for spacecraft. Diamond is one of the most radiation-proof semiconductors. Since it also has a large bandgap, it can operate in a wide range of temperatures, making it the ideal material for nuclear batteries powering spacecraft." (Moscow Institute of Physics and Technology, 2018)

Concluding Thoughts

The advances made in science and engineering are important for the future of unmanned systems. The advances in information technologies enable more complicated operations but require more energy. The advances in energy technology, both in energy density and in portability, open the door for more integration of advanced information technologies in unmanned systems. The advances in manufacturing technologies and approaches create a rich future for unmanned systems.

While reading the rest of this textbook, keep these advances in

mind and imagine how what you are reading will be changed, enhanced, or revolutionized in the coming decades.

References

Burgard, W., Stachniss, C., Arras, K., & Bennewitz, M. (2020). *Introduction to Mobile Robotics Teaching Material.* Retrieved September 12, 2020, from University of Freiburg: http://ais.informatik.uni-freiburg.de/teaching/ss12/robotics/slides/12-slam.pdf

Burger, R. (2019, August 15). *6 Ways Drones Are affecting the Construction Industry.* Retrieved September 11, 2020, from The Balance Small Business: https://www.thebalancesmb.com/drones-affecting-construction-industry-845293

CB Insights. (2020, January 9). *38 Ways Drones Will Impact Society: From Fighting War To Forecasting Weather, UAVs Change Everything.* Retrieved September 11, 2020, from CB Insights Research: https://www.cbinsights.com/research/drone-impact-society-uav/

Chen, S. (2018, June 24). *China takes surveillance to new heights with flock of robotic Doves, but do they come in peace?* Retrieved September 14, 2020, from South China Morning Post: https://www.scmp.com/news/china/society/article/2152027/china-takes-surveillance-new-heights-flock-robotic-doves-do-they

Chin, L. T. (2019). *A High-Deformation Electric Soft Robotic Gripper via Handed Shearing Auxetics.* Boston: Massachusetts Institute of Technology.

Electronic Frontier Foundation. (2017, August 28). *Drones/Unmanned Aerial Vehicles.* Retrieved September 11, 2020, from EFF Street-Level Surveillance: https://www.eff.org/pages/dronesunmanned-aerial-vehicles

Elliott, L. R., Hill, S. G., & Barnes, M. (2016, July). *Gesture-Based Controls for Robots: Overview and Implications for Use by Soldiers.*

Retrieved September 14, 2020, from Defense Technical Information Center: https://apps.dtic.mil/sti/pdfs/AD1011904.pdf

Feldstein, S. (2019, September 17). *The Global Expansion of AI Surveillance.* Retrieved September 14, 2020, from Carnegie Endowment for International Peace: https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847

L'atelier BNP. (2020). *Strativerse*. Retrieved August 20, 2020, from Envisioning Radar: https://atelier.net/strativerse/?pg=about

Martin, S. (2019, July 25). *What Is Simultaneous Localization and Mapping?* Retrieved September 12, 2020, from NVIDIA Blog: https://blogs.nvidia.com/blog/2019/07/25/what-is-simultaneous-localization-and-mapping-nvidia-jetson-isaac-sdk/

MaterialsToday. (2009, December 22). *Small and powerful nuclear battery developed*. Retrieved September 14, 2020, from Materials Today Energy News: https://www.materialstoday.com/energy/news/small-and-powerful-nuclear-battery-developed/

Mir, M., Ali, M. N., Sami, J., & Ansari, U. (2014, November 13). *Review of Mechanics and Applications of Auxetic Structures.* Retrieved September 14, 2020, from Advances in Materials Science and Engineering: https://www.hindawi.com/journals/amse/2014/753496/

Miskinis, C. (2018, November). *What does a digital thread mean and how it differs from digital twin.* Retrieved September 12, 2020, from Challenge Advisory: https://www.challenge.org/insights/digital-twin-and-digital-thread/

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/

Moscow Institute of Physics and Technology. (2018, June 1). *Prototype nuclear battery packs 10 times more power*. Retrieved September 14, 2020, from Phys.org: https://phys.org/news/2018-06-prototype-nuclear-battery-power.html

NASA. (2017, August 7). *Technology Readiness Levels*. Retrieved August 20, 2020, from NASA Engineering Technologies: https://www.nasa.gov/directorates/heo/scan/engineering/technology/txt_accordion1.html

Nichols, R. K., Mumm, H. C., Lonstein, W. D., Ryan, J. J., Carter, C., & Hood, J.-P. (2020). *Counter Unmanned Aircraft Systems Technologies and Operations*. Manhattan, Kansas: New Prairie Press.

Page, S. (2020, February 5). *5 U.S. MILITARY DRONE USES THAT MAY SURPRISE YOU*. Retrieved September 11, 2020, from Sandboxx: https://www.sandboxx.us/blog/5-u-s-military-drone-uses-that-may-surprise-you/

Samuel, S. (2018, August 16). *China Is Going to Outrageous Lengths to Surveil Its Own Citizens*. Retrieved September 14, 2020, from The Atlantic: https://www.theatlantic.com/international/archive/2018/08/china-surveillance-technology-muslims/567443/

SAS. (2019, January 1). *The Internet of Things*. Retrieved August 20, 2020, from What is IOT?: https://www.sas.com/content/dam/SAS/documents/infographics/2019/internet-of-things-109082.pdf

Shigeki, Y., Okura, F., Mitsugami, I., Hayashi, K., & Yagi, Y. (2018). *Directional Characteristics Evaluation of Silhouette-Based Gait Recognition*. Retrieved September 14, 2020, from IPSJ Transactions on Computer Vision and Applications: https://link.springer.com/article/10.1186/s41074-018-0046-7

Smith, J. (2018, July 24). *Data Marketplaces: The Holy Grail of our Information Age*. Retrieved August 20, 2020, from Hackernoon: https://hackernoon.com/data-marketplaces-the-holy-grail-of-our-information-age-1211a6fec390

Stancic, I., Music, J., & Grujic, T. (2017, November). *Gesture Recognition System for Real-time Mobile Robot Control Based on Inertial Sensors and Motion Strings*. Retrieved September 14, 2020, from Engineering Applications of Artificial Intelligence: https://www.sciencedirect.com/science/article/abs/pii/S0952197617301975

Swales, V. (2019, November 3). *Drones Used in Crime Fly Under*

the Law's Radar. Retrieved September 11, 2020, from The New York Times: https://www.nytimes.com/2019/11/03/us/drones-crime.html

[1] Remote ID has two meanings in this textbook. It is used as an information / technology device to identify people from a UAV. This term is used in the UAS industry and the FAA as a mechanism for identifying an aircraft type and the registrant from the ground, essentially a digital license plate and registration.

[2] Technology readiness levels are a rating method developed by NASA to describe where a technology is in terms of its development. The lowest levels (1 – 3) are technologies that are being researched, the middle levels (4 – 6) are technologies that are being prototyped and tested, and the highest levels (7 – 9) are technologies that are being demonstrated and used. (NASA, 2017)

2. Chapter 2: Unmanned Aerial Vehicles & How They Can Augment Mesonet Weather Tower Data Collection [Mai]

Student Learning Objectives

The student will gain conceptual knowledge of a Mesonet, how a Mesonet can aid in weather prediction, and how a sUAV (small Unmanned Aerial Vehicle – usually tethered up to 400 feet) can fill in holes and create a 3D Mesonet.

The student will be able to:

1. Understand the Highlights of Mesonet Data collection selected weather instrument(s)

2. Gain an overview of sUAV's currently interaction with Mesonet(s)

3. Explore future uses of sUAV's for assisting Weather prediction.

What is a Mesonet? (Wikipedia, 2020)

Mesonet, is a network of automated weather and environmental monitoring stations designed to observe mesoscale

meteorological phenomena. (Service, 2020) (Glickman, 2000) Dry lines, squall lines, and sea breezes are examples of phenomena that can be observed by mesonets. Due to the space and time scales associated with mesoscale phenomena, weather stations comprising a mesonet will be spaced closer together and report more frequently than synoptic scale observing networks, such as ASOS. The term mesonet refers to the collective group of these weather stations and are typically owned and operated by a common entity. Mesonets usually record in situ surface weather observations but some involve other observation platforms, particularly vertical profiles of the planetary boundary layer (PBL). (Marshall, (11 Jan 2016))

The distinguishing features that classify a network of weather stations as a mesonet are station density and temporal resolution. Depending upon the phenomena meant to be observed, mesonet stations use a spatial spacing of 1 to 40 kilometers (0.62 to 24.85 mi) (Fujita T. , 1962) and report conditions every 1 to 15 minutes. **Micronet**s (see microscale and storm scale), such as in metropolitan areas such as Oklahoma City, (Basara, et al., 2011) may be even denser in spatial resolution. (Muller, Chapman, Grimmond, Young, & Cai, 2013)

Thunderstorms, squall lines, drylines, (Pietrycha & Rasmussen, 2004) sea and land breezes, mountain breeze and valley breezes, mountain waves, mesolows and mesohighs, wake lows, mesoscale convective vortices (MCVs), tropical cyclone and extratropical cyclone rainbands, macrobursts, gust fronts and outflow boundaries, heat bursts, urban heat islands, and other mesoscale phenomena can cause weather conditions in a localized area to be significantly different from that dictated by the ambient large-scale conditions. (Fujita T. , 1981) (Ray, 1986) As such, meteorologists need to understand these phenomena in order to improve forecast skill. Observations are critical to understanding the processes by which these phenomena form, evolve, and

dissipate.[This is where the sUAV comes into play – enhancing the data collection and reduction of chaos.]

The long-term observing networks (ASOS, AWOS, Coop),[1, 2] however, are too sparse and report too infrequently for mesoscale research. ASOS and AWOS stations are typically spaced 50 to 100 kilometers (31 to 62 mi) apart and report only hourly at many sites. The Cooperative Observer Program (COOP) database consists of only daily reports. "Mesoscale" weather phenomena occur on spatial scales of tens to hundreds of kilometers and temporal (time) scales of minutes to hours. Thus, an observing network with finer temporal and spatial scales is needed for mesoscale research. This need led to the development of the mesonet.

Mesonet data is directly used by humans for decision making, but also boosts the skill of numerical weather prediction and is especially beneficial for short-range mesoscale models. Mesonets, along with remote sensing solutions (data assimilation of weather radar, weather satellites, wind profilers), allow for much greater temporal and spatial resolution in a forecast model. As the atmosphere is a *chaotic nonlinear dynamical system* (i.e. Butterfly effect), this increase in data increases understanding of initial conditions and boosts model performance. In addition to meteorology and climatology users, transportation departments, energy producers and distributors, other utility interests, and agricultural entities also have a need for fine scale weather information. These organizations operate dozens of mesonets within the US and globally. Environmental, emergency management and public safety, and insurance interests also are heavy users of mesonet information.

In many cases, mesonet stations may (by necessity) be located in positions where accurate measurements may be compromised; for instance, this is especially true of the stations built for WeatherBug's network, many of which were located on school buildings. The

potential bias that these locations may cause must be accounted for when entering the data into a model, lest the phenomenon of "GIGO"[3] may occur.

Mesonets were born out of the need to conduct mesoscale research. The nature of this research is such that mesonets, like the phenomena they are meant to observe, are short-lived. Long term research projects and non-research groups, however, have been able to maintain a mesonet for many years. For example, the U.S. Army Dugway Proving Ground in Utah has maintained a mesonet for many decades. The research-based origin of mesonets has led to the characteristic that mesonet stations tend to be modular and portable, able to be moved from one field program to another.

Whether the mesonet is temporary or semi-permanent, each weather station is typically independent, drawing power from a battery and solar panels. An on-board computer takes readings from several instruments measuring temperature, humidity, wind speed & direction, and atmospheric pressure, as well as soil temperature and moisture, and other environmental variable deemed important to the mission of the mesonet, solar irradiance being a common non-meteorological parameter. The computer periodically saves these data to memory and transmits the observations to a base station via radio, telephone (wireless or landline), or satellite transmission. Advancements in computer technology and wireless communications in recent decades made possible the collection of mesonet data in real-time. The availability of mesonet data in real-time can be extremely valuable to operational forecasters as they can monitor weather conditions from many points in their forecast area.

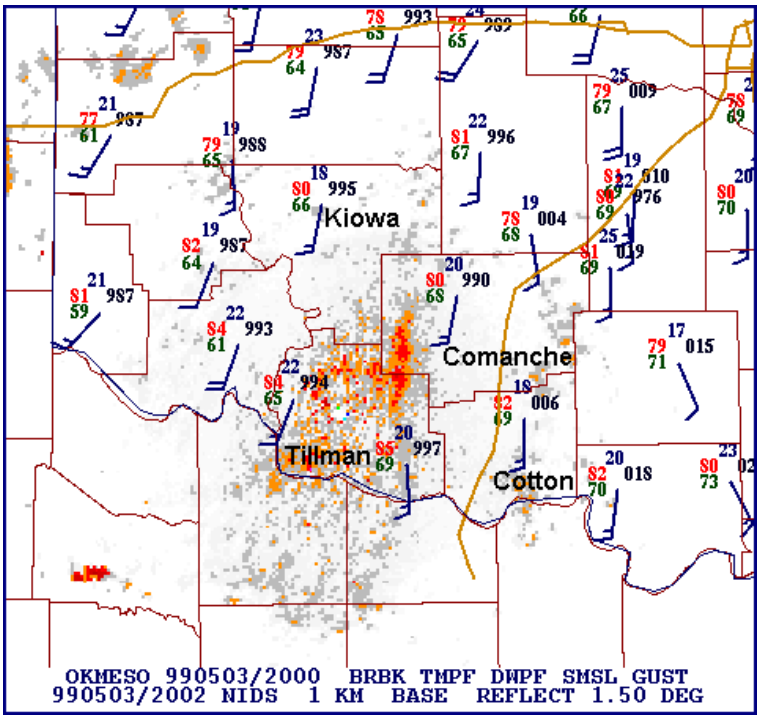


Figure 2.1 A weather map consisting of a station model plot of Oklahoma Mesonet data overlaid with WSR-88D weather radar data depicting possible horizontal convective rolls as a potential contributing factor in the incipient 3 May 1999 tornado outbreak Source: (Wikipedia, 2020)

Introduction

How does weather prediction work? Weather is extremely difficult to predict. Atmospheric conditions must be compiled around the world for a number of days monitoring such things as changes in pressure, temperature, wind speed, and rainfall. Weather balloons are sent up to take weather readings. Ships and aircraft also monitor weather data. Cloud patterns are monitored

by satellite imagery. Historical data is also used to assist prediction by using variables of heat, air, and moisture in numerical modeling to see how they flow over the earth's surface.

An examination a Mesonet Data Collection weather instrument(s).

A Mesonet is a network of environmental monitoring stations designed to measure the environment at the size and duration of mesoscale weather events. The phrase "Mesonet" is a portmanteau of the word's mesoscale and network. One can think of Mesonet as the average occurring weather, not large scale, or microclimate without being used in combination of the before mentioned inputs to weather prediction. In this case we will concentrate on a network made up of 10-meter towers with a set of research grade weather and ground sensing instruments.

In Figure 2.2 a 30ft. weather tower is depicted. The instruments spaced at 10m are: 1 – RM Young anemometer, 1 – HMP60 temperature/relative Humidity sensor w/ radiation shield. Instruments at 2m are: 1 – RM Young anemometer, 1 – HMP60 temperature/relative Humidity sensor w/ radiation shield, 1 – CS301 Pyranometer. Midway up the tower is a 7dbi antenna. Inside the NEMA enclosure: 1 CR1000X data logger, 1 – RV50 Modem, 1 – CS106 Barometer, 1 – Charge controller.

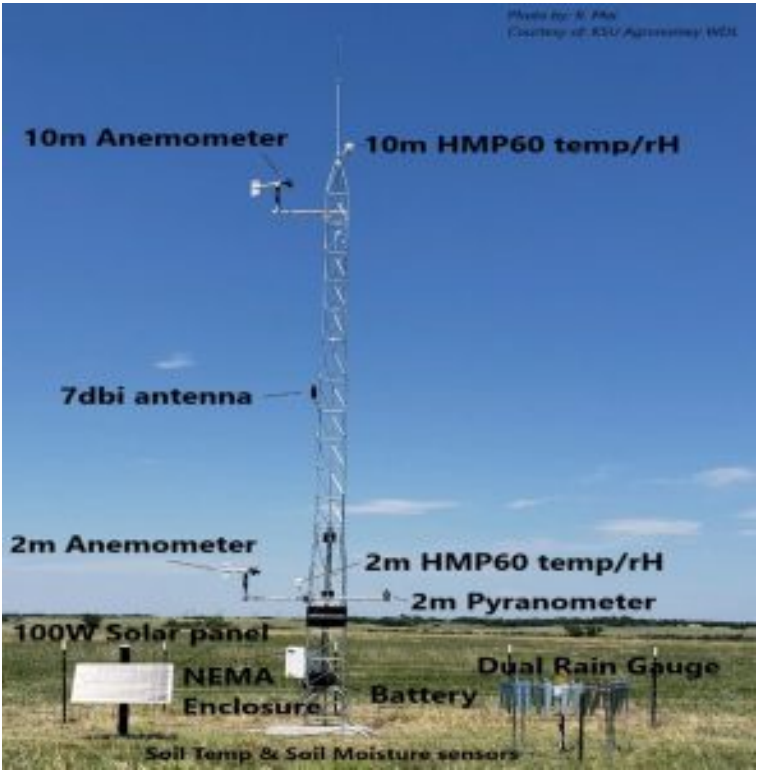


Figure 2.2: 30' Weather Tower

Source: (Campbell Sci, 2020)

Businesses such as airlines and farming rely heavily upon accurate weather forecasting. Forecasting accurately is extremely important in keeping track of deadly weather events. That demand for accuracy places an emphasis on making proper predictions and also using high quality instrumentation that is proven to be reliable and repeatable with known calibration intervals that can be traced to know standards. We will now make an examination of the standard instrumentation used in Figure 2.2 top to bottom.

Figure 2.3: 05103 Wind Monitor

Source: (Campbell Sci, 2020)

Wind monitors, also known as Anemometers, are kinetic and require a robustness that can tolerate all weather conditions. The wind monitor show in Figure 2.3 is a lightweight, sturdy instrument for measuring wind speed and direction in your harsh environments. Its simplicity and corrosion-resistant construction make it ideal for a wide range of wind measuring applications. Manufactured by R. M. Young. The 05103 Wind Monitor is made out of rigid UV-stabilized thermoplastic with stainless steel and anodized aluminum fittings. The thermoplastic material resists corrosion from sea air environments and atmospheric pollutants. It uses stainless-steel precision-grade ball bearings for the propeller shaft and vertical shaft bearings. The 05103 measures wind speed with a helicoid-shaped, four-blade propeller. Rotation of the propeller produces an AC sine wave that has a frequency directly proportional to wind speed. The AC signal is induced in a transducer coil by a six-pole magnet mounted on the propeller shaft. The coil

resides on the non-rotating central portion of the main mounting assembly, eliminating the need for slip rings and brushes. Wind direction is sensed by the orientation of the fuselage-shaped sensor body, which is connected to an internal potentiometer. The data logger applies a known precision excitation voltage to the potentiometer element. The output is an analog voltage signal directly proportional to the azimuth angle. (Campbell Sci, 2020)

Figure 2.4: HMP60 temp/relative Humidity

Source: (Campbell Sci, 2020)

Figure 2.5: HMP60 temp/relative Humidity w/ radiation shield
Source:(Campbell Sci, 2020)

The HMP60, manufactured by Vaisala, probe measures air temperature for the range of -40° to +60°C, and relative humidity for the range of 0 to 100% RH. It uses the INTERCAP® capacitive RH chip. This field-replaceable chip eliminates the downtime typically required for the recalibration process.[4] (Campbell Sci, 2020)

Figure 2.6: CS301 Pyranometer
Source: (Campbell Sci, 2020)

The CS301 uses a silicon photovoltaic detector mounted in a cosine-corrected head to provide solar radiation measurements. Its dome-shaped head prevents water from accumulating on the sensor head. To eliminate internal condensation, the sensor head is potted solid and the cable is shielded with a rugged Santoprene casing. The CS301 is calibrated against a Kipp & Zonen CM21 thermopile Pyranometer to accurately measure sun plus sky radiation. (Campbell Sci, 2020)

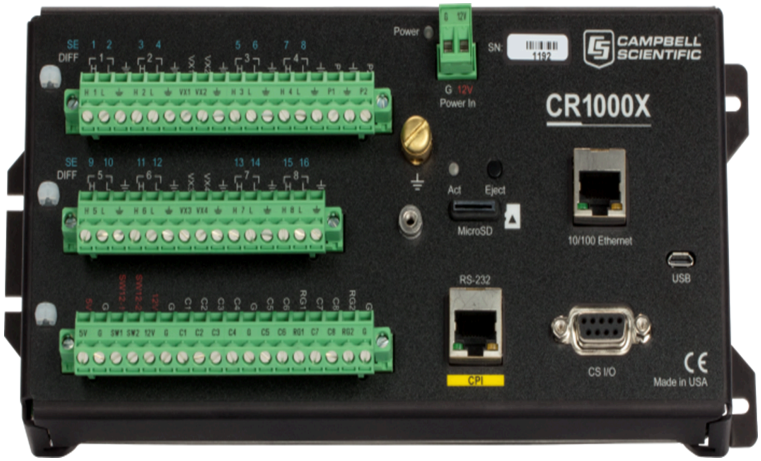


Figure 2.7: CR1000X Datalogger

Source: (Campbell Sci, 2020)

The CR1000X is a low-powered device designed to measure sensors, drive direct communication and telecommunications, analyze data, control external devices, and store data and programs in on-board, non-volatile storage. The electronics are RF-shielded and glitch-protected by a unique sealed, stainless-steel canister. A battery-backed clock assures accurate timekeeping. The on-board, BASIC-like programming language—common to all Campbell Scientific data loggers—supports data processing and analysis routines. The CR1000X wiring panel includes two switchable 12 V terminals, analog grounds dispersed among 16 analog terminals, and non pluggable terminal blocks for quick deployment. (Campbell Sci, 2020)

Figure 2.8: CS106 Barometer

Source: (Campbell Sci, 2020)

The CS106 uses Vaisala BAROCAP silicon capacitive sensor to measure barometric pressure. It is encased in a plastic shell (ABS/PC blend) fitted with an intake valve for pressure equilibration.

The CS106 outputs a linear signal of 0 to 2.5 Vdc, which allows the barometer to be directly connected to a Campbell Scientific data logger. An internal switching circuit allows the data logger to power the CS106 only during measurement, which reduces power consumption. (Campbell Sci, 2020)

Figure 2.9: NEMA Enclosure

Source: (Campbell Sci, 2020)

Note: The Datalogger, Barometer, Charge Controller, and Modem are housed within the NEMA.

The ENC16/18 is a weather-resistant enclosure that is 16 inches wide and 18 inches tall. It can house a data logger, a power supply, and at least one peripheral. This enclosure is recommended for applications that need to have multiple communication or

measurement and control peripherals housed in the same enclosure. (Campbell Sci, 2020)

Figure 2.10 TE525 Rain Gauge

Source: (Campbell Sci, 2020)

The TE525 funnels precipitation into a bucket mechanism that tips when filled to its calibrated level. A magnet attached to the tipping mechanism actuates a switch as the bucket tips. The momentary switch closure is counted by the pulse-counting circuitry of our data loggers. (Campbell Sci, 2020)

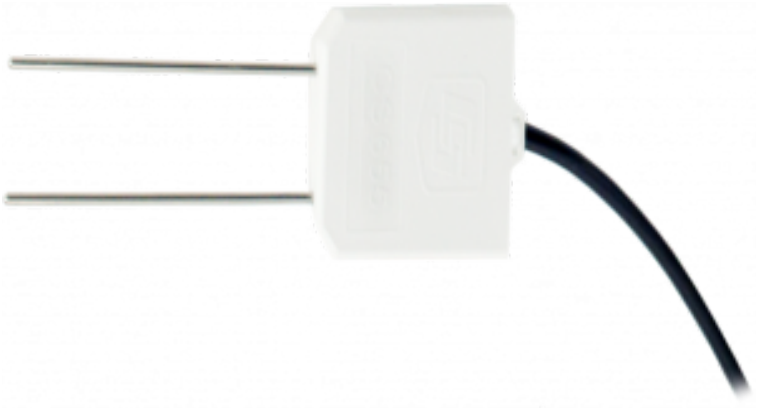


Figure 2.11: CS655 TDR Soil Moisture and Temperature

Source: (Campbell Sci, 2020)

The CS655 consists of two 12-cm-long stainless-steel rods connected to a printed circuit board. The circuit board is encapsulated in epoxy and a shielded cable is attached to the circuit board for data logger connection.

The CS655 measures propagation time, signal attenuation, and temperature. Dielectric permittivity, volumetric water content, and bulk electrical conductivity are then derived from these raw values.

Measured signal attenuation is used to correct for the loss effect on reflection detection and thus propagation time measurement.

This loss-effect correction allows accurate water content measurements in soils with bulk EC ≤8 dS m-1 without performing a soil-specific calibration.

Soil bulk electrical conductivity is also calculated from the attenuation measurement. A thermistor in thermal contact with a probe rod near the epoxy surface measures temperature. Horizontal installation of the sensor provides accurate soil temperature measurement at the same depth as the water content. Temperature measurement in other orientations will be that of the region near the rod entrance into the epoxy body. (Campbell Sci, 2020)

Figure 2.12: 107 Temperature probe

Source: (Campbell Sci. , 2020)

The 107 is a rugged, accurate probe that measures temperature of air, soil, or water from -35° to +50°C. It easily interfaces with most Campbell Scientific data loggers and can be used in a variety of applications. The 107 consists of a thermistor encapsulated in an epoxy-filled aluminum housing. The housing protects the

thermistor, allowing you to bury the probe in soil or submerge it in water. (Campbell Sci, 2020)

Additional Components in the Weather Ground Station part of the sUAV ecosystem

Additional components needed are: A rugged modem such as a Raven RV50 w/ 4g antenna, Solar panel(s) based on power demand, deep cycle 12Vdc battery for power storage, and a charge controller for power management.

The above components are by no means the limit to the type and style of sensors and hardware that can be added to a Mesonet tower. However, they will acquire the basic data, moisture, wind speed and direction, temperature, relative humidity, barometric pressure, solar radiation, used in recording data.

A tower by itself would not be good enough to do any type of weather prediction. Even combined with multiple towers they are only good enough to record the weather at each point at any given time. As a Mesonet increases its number of towers they become more valuable. As stated before, the data collected on its own is only a record. If used in conjunction with the other forms and types of weather data collection, only then can weather prediction become possible. Even then, many holes could be filled by more towers creating more data collection points. The only way to be 100% accurate in weather prediction is to be omniscient or collect data on every square inch of the earth. Which we all understand that is economically unfeasible and a temporal impossibility.

Billions of dollars are spent each year in the recording and prediction of the weather to save lives, assist businesses and help the public with their individual daily activities. The collection of more data can only assist in that goal. But just more data is not the only requirement. Understanding that data and making inferences to establish a prediction is most important. So how do we interrupt the weather?

If a butterfly flaps its wings in Brazil, could it really cause a hurricane in Texas?

That's more or less a spoof on the mathematics of Chaos Theory.[5] (Roulstone, 2013) *To be more specific that is how we determine weather patterns.* The mathematics of the known laws of motion are not good enough to predict weather. The movement of weather is so complicated it requires the use of a computer to develop models of probability. Even if you change the initial conditions only slightly the end conditions are wildly different resulting in Chaos. This is where Chaos theory becomes involved. By using contributing factors of weather, we do have models on how these variables behave. If a perfect weather prediction is impossible, then better computer computations and as many possible data points sampled would be the best we as humans can expect to strive towards. **This is the point sUAV's could help in increasing sampling points and predictive of severe weather events.**

Figure 2.13 120m Tethered UAV on windy weather, cable feeder, 400VDC

Source: (Campbell Sci. , 2020)

To work with a Mesonet, a Tethered sUAV could be added and create a 3D Mesonet. Power and data could flow thru the wiring acting as a tether. This would also provide stability and retrieval.

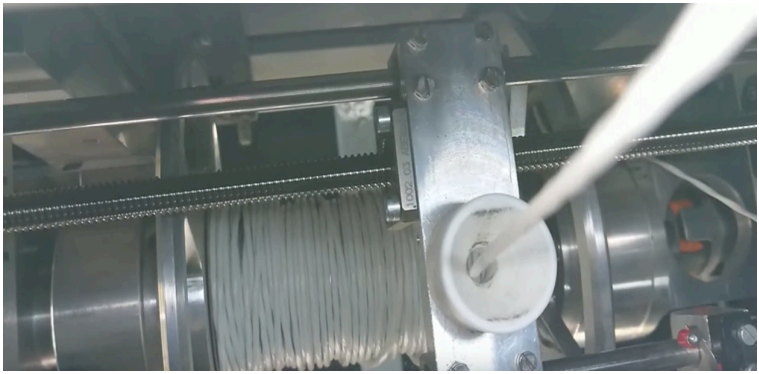


Figure 2.14: Automatic Winch to Control Tether Retrieval

Source: (Campbell Sci. , 2020)

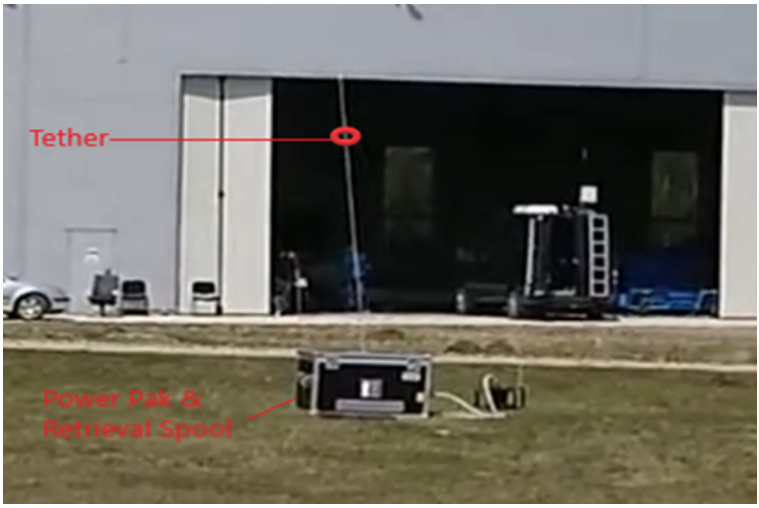


Figure 2.15: Tether Power Pak

Source: (Campbell Sci. , 2020)

Oklahoma Mesonet

The following abstract focuses on the efforts of the Oklahoma Mesonet and their efforts to design and build a 3D Mesonet with the aid of UAV's. At the time of this writing the author is aware of only the Oklahoma Mesonet making significant funded efforts to use sUAV's in their operations.

Fixed monitoring sites, such as those in the US National Weather Service Automated Surface Observing System (ASOS) and the Oklahoma Mesonet provide valuable, high temporal resolution information about the atmosphere to forecasters and the general public. The Oklahoma Mesonet is comprised of a network of 120 surface sites providing a wide array of atmospheric measurements up to a height of 10 m with an update time of five minutes.

The deployment of small, unmanned aircraft to collect in-situ vertical measurements of the atmospheric state in conjunction with surface conditions has potential to significantly expand weather observation capabilities. This concept can enhance the safety of individuals and support commerce through improved observations and short-term forecasts of the weather and other environmental variables in the lower atmosphere.

We report on a concept of adding the capability of collecting vertical atmospheric measurements (profiles) through the use of unmanned aerial systems (UAS) at remote Oklahoma sites deemed suitable for this application. While there are a number of other technologies currently available that can provide measurements of one or a few variables, the proposed UAS concept will be expandable and modular to accommodate several different sensor packages and provide accurate in-situ measurements in virtually all-weather conditions. Such a system would facilitate off-site maintenance and calibration and would provide the ability to add new sensors as they are developed, or as new requirements are identified. The small UAS must be capable of accommodating the weight of all sensor packages and have lighting, communication, and aircraft avoidance

systems necessary to meet existing or future FAA regulations. The system must be able to operate unattended, which necessitates the inclusion of risk mitigation measures such as detect and avoid radar and the ability to transmit and receive transponder signals. Moreover, the system should be able to assess local weather conditions (visibility, surface winds, and cloud height) and the integrity of the vehicle (system diagnostics, fuel level) before takeoff. We provide a notional concept of operations for a 3D Mesonet being considered, describe the technical configuration for one station in the network, and discuss plans for future development.

Future uses of sUAV and Weather stations

As the use of UAV's in a 3D Mesonet configuration are perfected, these same applications can be moved into situations were atmospheric gases can be sampled and quantified. For example, controlled burns in the central US could be monitored by mobile and tethered UAV's carrying smoke canisters. The particulates from the smoke canisters can be quantified then statistically equated to the imagery of the satellites. This would allow for a close approximation to the amount of biomass consumed and the amount of CO and CO2 released into the atmosphere. This technology could be used on forest fires, oil field fires, and volcanic eruptions to quantify the number of particulates and greenhouse gases released. It would allow operators to stay at a safe distance while gathering data. A sonic anemometer could be used during the study to verify background CO2 flux and other trace gases. Done correctly, this could lead into xo-atmospheric research.

Figure 2.16: Smoke study
Source: (Randall, Mai, author courtesy of KSU/WDL)

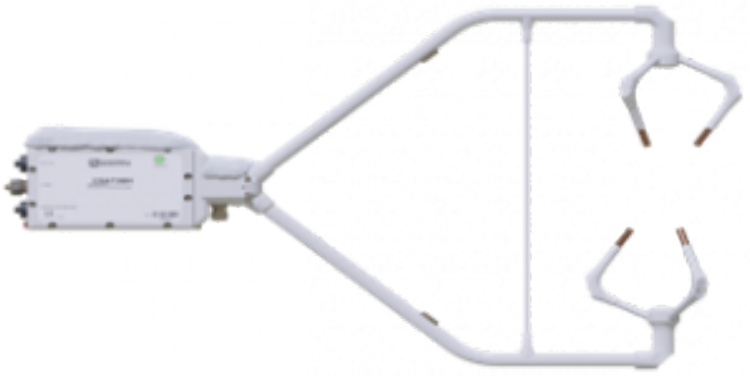


Figure 2.17: Sonic Anemometer
Source: (Tethered Pictures, 2020)

Conclusions

Civilization has come a long way since first trying to predict the weather. For example: Red sky at night sailors take delight and red sky in the morning sailors take warning. This revels clouds position of clouds at sunrise and sunset. We now have very sophisticated instruments that can take very exact readings. But those readings cannot act alone in a vacuum. And they are forever changing and changing immediately. So, the only way humans can improve weather prediction is to increase the number of readings and the profile of those readings. And then the never-ending task of making inference as to what all that data means. As we push into AI and things such as Quantum Computers we can solve more quickly the interruption of massive amounts of data. However, physically we will have to push the envelope on how to sample the never-ending pool of data the weather presents. Tethered and even mobile UAV can assist by carrying atmospheric sensors to improve the profile that we call weather and eventually climate.

Student Think Questions

1. Where might we find a valuable place to deploy Tethered UAV's?
2. How can we assure powering a UAV in its role as a Tethered UAV package?
3. How would you design a request for funding for a Tethered UAV?

Campbell Sci. (2020, July 02). *Campbell Scientific*. Retrieved from Wind Monitor – Campbell Scientific: https://www.campbellsci.com/05103-l

Campbell Sci. (2020, July 02). *Campbell Scientific*. Retrieved from Wind Monitor – Campbell Scientific: https://www.campbellsci.com/05103-l

References

Basara, J., Illston, B. G., Fiebrich, C. A., Browder, P. D., Morgan, C. R., McCombs, A., . . . McPherson, R. A. (2011). The Oklahoma City Micronet. *Meteorological Applications*, pp. 18 (3): 252–61. doi:10.1002/met.189.

Campbell Sci. (2020, July 02). *Campbell Scientific*. Retrieved from Wind Monitor – Campbell Scientific: https://www.campbellsci.com/05103-l

Campbell Sci. . (2020, July 2). *Campbell Scientific. Wind Monitor.* Retrieved from www.campbellsci.com/05103-l: https://www.campbellsci.com/05103-l

Fujita, T. (1962). A Review of Researches on Analytical Meso Meteorology. *SMRP Research Paper.* #8, p. Chicago: University of Chicago. OCLC 7669634.

Fujita, T. (1981). Tornadoes and Downbursts in the Context of Generalized Planetary Scales. *Journal of the Atmospheric Sciences*, pp. 38 (8): 1511–34. Bibcode:1981JAtS...38.1511F. doi:10.1175/1520-0469(1981)038<1511:TADITC>2.0.

Glickman, T. S. (2000). *Glossary of Meteorology (2nd ed.).* Boston: American Meteorological Society. ISBN 978-1-878220-34-9.

Marshall, C. ((11 Jan 2016)). The National Mesonet Program. *22nd Conference on Applied Climatology*. New Orleans: American Meteorological Society.

Muller, C., Chapman, L., Grimmond, C. S., Young, D. T., & Cai, X. (2013). Sensors and the City: A Review of Urban Meteorological Networks. *Int. J. Climatol*, pp. 33 (7): 1585–600. Bibcode:2013IJCli..33.1585M. doi:10.1002/joc.3678.

Pietrycha, A., & Rasmussen, E. N. (2004). Finescale Surface Observations of the Dryline: A Mobile Mesonet Perspective. *Weather and Forecasting*, pp. 19(12): 1075–88. Bibcode:2004WtFor..19.1075P. doi:10.1175/819.1.

Ray, P. e. (1986). *Mesoscale Meteorology and Forecasting*. Boston: American Meteorological Society. ISBN 978-0933876668.

Roulstone, I. &. (2013). *Invisible in the Storm: The Role of Mathematics in Understanding Weather*. Princeton: Princeton University Press.

Service, N. W. (2020, September 8). "Mesonet". National Weather Service Glossary. Washington, DC.

Tethered Pictures. (2020, September 8). Retrieved from www.youtube.com: https://www.youtube.com/watch?v=AY3kHXRGPIQ

Wikipedia. (2020, September 8). *Mesonet*. Retrieved from en.wikipedia.org/wiki/Mesonet: en.wikipedia.org/wiki/Mesonet

[1] ASOS = Automated Surface Weather System

[2] AWOS= Automated Weather Observing System

[3] GIGO = refers to computer data garbage in, garbage out

[4] *https://s.campbellsci.com/documents/us/product-brochures/b_hmp60.pdf*

[5] A useful source is Roulstone, I. & Norury, J. (2013) *Invisible in the Storm: The Role of Mathematics in Understanding Weather.* Princeton University Press

3. Chapter 3 Tour de Drones for the Discerning Palate [Nichols]

Student Objectives

To enjoy the range of UAS and UUV technologies by shared stories. At Olive Garden© they call it a "Tour de Italy" This chapter is a "Tour de Drone for the Discerning Palate." Through stories and vignettes, UAS and UUV world are further discovered.

Introduction

In our three previous textbooks, the authors covered the whole spectrum of UAS / CUAS technologies. (Nichols R. K., et al., 2020)(Nichols, et al., Unmanned Aircraft Systems (UAS) in Cyber Domain: Protecting USA's Advanced Air Assets, 2nd Edition, 2019)(Nichols R. K., et al., 2019) Every day since our publication have come to market, news about UAS and CUAS technologies have emerged in as many publications and media. In this textbook (4th textbook in the series) the authors have added the unmanned underwater vehicles (UUVs) as technologies based on many of the same autonomous principles working in a different medium. This chapter highlights some of the interesting finds since February 2020 publication of ground-breaking textbook on CUAS. (Nichols, et al., Counter Unmanned Aircraft Systems Technologies and Operations, 2020)

Suspicious Drones?

On 3 August 2020, an interesting poster was received from the Chief of Security at KSU regarding identification of suspicious unmanned aircraft systems (UAS). It was CISA's Office of Bombing Protection. (Bombing, 2020)

Figure 3.1 is aimed at the protection of national critical infrastructure but has elements common to civilian facilities and personnel protections from a wide variety of threats.

Figure 3.1 Recognize Suspicious UAS

Source: (Bombing, 2020)

The poster shows several interesting items:

Indicators of Suspicious UAS Activity

- Repeated unauthorize flights

- Suspected reconnaissance, such as repeated flyovers or prolonged hovering at low altitudes,
- Testing facility security protocols by flying in sensitive areas to observe the reaction of security personnel (Bombing, 2020)

Easy Acronym – DRONE

Detect all available elements of the situation; attempt to locate and identify the individuals operating the drone (look at windows, balconies, roof tops)

Report the incident to local LEO and FAA Regional Operations Center.

Observe the UAS and maintain visibility of the device, look for damage or injured individuals.

Notice Features: Identify the type of device (fixed wing/ multi-rotor), size, shape, color, payload, and activity

Execute appropriate security actions. (Bombing, 2020)

Grounded UAS

Treat a suspicious grounded UAS as a potential explosive threat! (Treat as an IED) (Bombing, 2020)

Figure 3.1 is aimed at / designed for personnel protecting our national critical infrastructure. However, it is just as useful for determining UAS privacy invasions, drug flow and delivery, fraudulent delivery from retailers, residential property casing, stalking, child exploitation, and robberies to name a few possibilities. Treating every downed UAS as an IED is a bit over the top (perhaps) however, better to be cautious because one mistake could cost lives. One the key features of the poster is the "navigation lights taped over or removed" observation. This disabled safety feature can be seen – especially at night – for quite a distance or approximately 500 feet elevation. This is a serious indicator that the UAS is suspicious. (Bombing, 2020)

Cops, Drones and Nudes

From Minnesota comes a strange story. On 31 July 2020 cops in Minnesota flew a drone over a public beach to see if they could spot some exposed females – and then sent seven officers down to ticket topless sunbathers. (Cole, 2020). In response to dozens of complaints regarding nudism, alcohol and drug use, the Golden Valley Police Department used a drone to find people in the nude at Twin Lake, a public beach that's secluded but popular with locals who want to let it "hang out a little." The city defended the police citing Covid-19 concerns. The drone was used to "avoid unnecessary face-to-face interactions and the data was used for documentation, evidence collection, and prosecution if need and deleted as soon as possible." (Cole, 2020)

An ordinance from the Minnesota Park and Recreation Board states that "no person 10 years of age or older shall intentionally expose his or her own genitals, pubic area, buttocks or female breast below the top of the areola, with less than a fully opaque covering in or upon any park or parkway." (Cole, 2020) (PRBC, 2020) [1] The ordinance has been attacked by a coalition LGBT civil rights activists as discriminating. The author of the article chided the Golden Valley Police Department in her conclusions: " The fact that the police department—especially around Minnesota, one of the cities at the center of protests against police brutality this year—would break out the most over-the-top means of surveillance and enforcement they could, shouldn't be surprising." (Cole, 2020)

All this over a drone!

28,300 feet

Inspired by the 1924 expedition of George Leigh Mallory and Andrew 'Sandy' Irvine, National Geographic is working on a documentary titled 'Lost on Everest.' Mallory's remains were found in 1999, but Irvine's body is still missing. It remains a mystery as to whether the team actually reached the summit before their unfortunate deaths. If they did, it would have been long before Edmund Hillary and Tenzing Norgay reach the top of Mount Everest in 1953. A team from National Geographic surveyed Mount Everest

with a drone at 28,300 feet putting the unmanned aircraft in uncharted territory. They flew the drone as high as 28,300 feet or 8,625 meters, just shy of the summit of Mount Everest, which is at 29,000 feet or 8,840 meters, flying the Mavic 2 into 'uncharted territory.' Mark Sinnott and Renan Ozturk from National Geographic renewed the search for Irvine's body and brought with them a DJI Mavic 2 to survey the terrain. With the drone, the team was able to capture sweeping landscape views and close-up photos of key areas of Mount Everest (Figures 3.2, 3.3) (Kesteloo, 2020) [2]

Figure 3.2 National Geographic Climbing Team with Mavic 2 Drone

Source: (Kesteloo, 2020)

Figure 3.3 Key Search area of Mt Everest

Source: (Kesteloo, 2020)

Turtles

From Mt Everest , we fly 8,313 km (5,165.5 miles) to the Great Barrier Reef. Researchers at Raine Island, the world's largest green turtle rookery, have used a drone to conduct accurate population surveys, with stunning results. Drone vision captured in December 2019 as part of the Raine Island Recovery Project showed up to 64,000 green turtles around the island waiting to come ashore and lay clutches of eggs. (See Figure 3.4.) Dr Andrew Dunstan from the Department of Environment and Science (DES) and lead author of the paper said researchers had been investigating different ways of conducting turtle population surveys. "New scientific research published on Monday 8 June in PLOS ONE found that drones, or Unmanned Aerial Vehicles (UAVs), were found to be the most efficient survey method," Dr Dunstan said. "Previous population survey methods involved painting a white stripe down the green turtles' shell when they were nesting on the beach. The paint is non-toxic and washes off in a couple of days. "From a small boat, we then counted painted and non-painted turtles, but eyes are attracted much more to a turtle with a bright white stripe than an unpainted turtle, resulting in biased counts and reduced accuracy. "Trying to accurately count thousands of painted and unpainted turtles from a small boat in rough weather was difficult. Using a drone is easier, safer, much more accurate, and the data can be immediately and permanently stored." The drone vision was analyzed, frame by frame in the laboratory, reducing observer error and allowing accurate counts on painted and unpainted turtles. "The ratio of unpainted and painted turtles allowed us to estimate the total population for last December to be 64,000 green turtles waiting to nest on the island," Dr Dunstan said.

Figure 3.4 Raine-Island-turtle-aggregation

Source: Raine-Island-turtle-aggregation2.-credit-Great-Barrier-Reef-Foundation-and-Queensland-Government-min (1).jpg

"By using drones, we have adjusted historical data. What previously took a number of researchers a long time can now be by one drone operator in under an hour." "This research is of prime importance to the understanding and management of the vulnerable green turtle population, according to Dr. Dunstan." (USA weekly, 2020) [3]

Aerobatic Drone

From counting sea turtles' eggs, we turn our heads to getting air sick as a passenger (not the pilot) in the first manned aerobatic drone flown by the Drone Champions League (DCL). The Drone Champions League (DCL) has been captivating audiences since 2016 with the world's best pilots of quadcopter racing in head-to-head battles flying drones that can reach speeds of over 160 km/h. It is recognized as the World Championship of professional drone racing. Pilots are chosen by being the best players of the "DCL -The

Game" video game. The game can be played by anybody at home, giving everyone the chance to qualify for real-life drone racing events by playing in the DCL Draft Selection.

Now, Drone Champions AG, the creators of the Drone Champions League and DCL – The Game, have revealed their latest innovation: the world's first manned drone capable of aerobatic maneuvers such as loops and rolls. It was invented by Herbert Weirather, the Drone Champions founder and CEO of DCL. (Steffen, 2020) See Figures 3.5 -3.7.

Dubbed the "Big Drone," the aircraft is a full-sized, carbon fiber airframe that has six arms protruding from an aerodynamically faired chassis. Each arm has a pair of coaxial rotors mounted at the end. There is a middle seat to carry a passenger, not a pilot. The Big Drone was designed to be flown from the ground by professional drone racing pilots over a remote control. (Steffen, 2020)

Figure 3.5 “Big Drone” by DCL

Source: (Steffen, 2020)

Figure 3.6 “Big Drone” by DCL (2)

Source: (Steffen, 2020)

Figure 3.7 "Big Drone" by DCL (3)

Source: (Steffen, 2020)

A very cool flying machine!

Swarm Farming

In our textbook on CUAS we consider drone SWARMS a dangerous threat. (Nichols, et al., Counter Unmanned Aircraft Systems Technologies and Operations, 2020) However, what if we could use it for improving our agricultural outputs. Swarm farming is the concept of using multiple smaller robotic platforms to autonomously conduct farming operations as a substitute to large manned agricultural equipment. (See Figures 3.8 & 3.9) Now, rural agricultural communities have large sections of farmlands and large equipment, which can rapidly cover acres for planting, nutrition, pesticide, and harvesting operations (sometimes involving multiple operations for nutrition and pest control). During a growing season, limited days suitable to work are available to timely complete the specific operation without penalty on yield and profitability. (Precision AG , 2020)

Key drivers for the motivation in swarm farming include decreasing number of people engaged in agriculture, sustainable crop production methods for environmental sustainability, potential negative effects from soil compaction when using larger ag equipment, increasing size of farming operations, and rising average age of U.S. farmers. (Precision AG , 2020)

When it comes to substituting current large equipment with swarm farming, one of the key qualifiers is going to be comparative system productivity and accuracy. There are probably dozens of different types of robotic platforms which have been designed in Europe and the U.S. Some examples include Robotti by Agrointelli, Tertil by Franklin robotics, OZ, and DINO by Naio technologies, TerraSentia by Earthsense, AVO and ARA robots by Ecorobotix, DOT by Raven Autonomy, SwarmFarm Robotics, and BoniRob by

Deepfield Robotics. Platform sizes vary from small robots to do scout activities, medium sized for operations like weeding, and some large enough to conduct multi-row operations like spraying and seeding. (Precision AG , 2020)

Most of the robotics platforms currently in sight are standalone with a future vision to operate as swarms. The majority of these robotic platforms are light enough to just conduct non-soil engaging activities, whereas only a few can do soil engaging activities. These platforms are currently shown to operate on crops with low canopy heights (vegetable and fruits), with few exceptions like vineyards. (Precision AG , 2020)

However, there are very few options for row crop operations requiring operation on substantially large acreage, greater draft, and weight transfer. Another interesting facet is that not all of these robotic platforms have been designed with full considerations on implementations or application systems to be utilized in the real-world. Today's producers use a lot of technology, automation, automatic machine data, and not to mention, the human intelligence sitting inside the machine. One question we need to ask ourselves as stakeholders in the industry is, are farmers ready to provide a practical switch? (Precision AG , 2020)

Currently, there are a handful of swarm farming concepts which are being explored. Robotic platforms, like ones from Swarmfarms, DOT, Naio, Guss and others, are examples of how swarm robots could become reality. Personally, I feel the biggest hurdle we need to cross is the ability of such robotic platforms to operate as a fleet or implement swarm farming on large acres in a representative manner. (Precision AG , 2020)

Swarm farming definitely has some foreseeable advantage, if this swarm fleet becomes fully autonomous in operation over larger fields. Personally, I see two biggest advantages. One, a fully integrated system can reduce operational time spent by farm owners on and off the machines and continuous optimization using

machine learning, Two, the automatic decision-based applications using artificial intelligence, data assimilation, and aggregated data availability for analytics are strong assets. Swarm has the ability to operate on its own, detect and communicate faults, automatic reloading of operational boundaries if one platform is down, and many more. (Precision AG , 2020)

The big dream is that platforms within swarm farming will have capability to operate nearly 24/7, but the question is, how far are we from that reality? (Precision AG , 2020)

Figure 3.8 Swarm Farming -Spray Operations

Source: https://www.silicon-saxony-day.de/

Figure 3.9 Swarm Farming – Land Survey Operations

Source: https://pt.wikipedia.org/wiki/Ficheiro:Aerial_View_-_Landschaft_Markgr%C3%A4flerland1.jpg

COVID-19

It is an understatement that Covid-19 pandemic has affected millions of lives globally. However, a company called SkySkopes is doing something positive in the midst of chaos.

Unmanned aerial systems (UAS) are being studied as tools to fight the novel coronavirus. (See Figure 3.10 sprayer for disinfectant) The UAS will be used to disinfect large public areas and to deliver supplies. In Grand Forks, N. Dakota, SkySkopes, a UAS flight operator that serves a wide variety of industries; the Center for Innovation at the University of North Dakota (UND); and a number of other companies are engaged in a study to determine how drones can be used to accomplish these tasks. (Zimmer, 2020)

SkySkopes is also testing the use of thermal sensors that are positioned in stationary locations above research participants. The sensors detect elevated temperatures and help ensure that an individual is healthy enough to return to work. Like Syracuse-based drone startup EagleHawk, SkySkopes is determining what methods can be used to disperse disinfectant effectively and on a large scale.

Since mid-March, the company has been making test runs, spraying public playgrounds using nozzles and tanks. The only substance SkySkopes has sprayed outdoors is water. When its UAS have been used indoors, they have sprayed a solution of 3 percent hydrogen peroxide and 97 percent water. (Zimmer, 2020) [4]

SkySkopes is also developing procedures for drone pilots and visual observers to travel to and from a site, and to clean instruments before, during and after use, and take measures to inform and protect the public. SkySkopes CEO Matt Dunlevy said that reconsidering the use of drones during the pandemic requires identifying new precautions and protocols. (Zimmer, 2020)

Figure 3.10 SkySkopes Covid-19 Disinfectant sprayer drone
Source: (Zimmer, 2020)

"One of our biggest questions is what we will need to do to discourage crowds who want to observe our work from forming. We

do not want to exacerbate community spread as we disinfect public spaces," said Dunlevy. (Zimmer, 2020)

Dunlevy added that while playgrounds are not the only target site being considered, they are good locations to conduct research. "We're using them to learn how to disinfect many other objects and areas, including vehicles, the outsides of different types of buildings, park equipment, and indoor spaces such as movie theaters and gymnasiums," said Dunlevy. (Zimmer, 2020)

Fortunately, playgrounds are ideal for study because they contain a number of complex elements that can indicate how to tackle similar areas in other outdoor workplaces. For instance, SkySkopes has a number of clients in the energy industry, where ladders and platforms are present, and crowds are unavoidable for project executions. (Zimmer, 2020) (See Figure 3.11 SkySkopes Playground Test Area)

Figure 3.11 SkySkopes Playground Test Area

Source: (Zimmer, 2020)

Dunlevy explained that smaller areas could be disinfected with a single payload of liquid carried on the drone and released by "one fell swoop" of a drone pilot. Larger areas could be disinfected with liquid drawn from a tank on the ground by an assistant, carried to the drone by a tube, and sprayed out of a nozzle attached to the tube. A tank-and-hose combination could also be effective at disinfecting the underside of elements like monkey bars. The drone could fly under the play structure and turn the nozzle to spray disinfect upwards.

Currently, SkySkopes is running thermal sensor tests with Infrared Cameras Inc.'s Optical Gas Imaging camera, which is made with components by FLIR Systems, Inc., on DJI's Zenmuse XT. SkySkopes expects real-life use of the sensors could involve mounting the device on the wall of a hospital or care facility, with an employee standing under the device to take a reading. (Zimmer, 2020)

"Right now, we're just testing out use of that on the ground. We are only testing it on SkySkopes employees and research participants. As for nozzles for drone spraying, we are testing out a combination of different spray nozzles and tanks. We're borrowing heavily from already-proven techniques in agriculture," said Dunlevy. (Zimmer, 2020)

Mark Askelson, a professor of atmospheric sciences and executive director of the Research Institute for Autonomous Systems (RIAS) at the University of North Dakota, is assisting with the study. Askelson said the studies indicate that a spray of very small drops of disinfecting liquid would likely limit the fluid's ability to kill the virus. "The smaller the droplet, the faster it evaporates. That is the reason SkySkopes is out there under different conditions to determine how drop size, wind speed, and direction affect coverage," said Askelson. Askelson noted that determining the "residence time" of droplets of cleaning fluid is important to determine whether the drops stay on the surface of an object long enough to kill the virus. (Zimmer, 2020)

HAPS UAV – Stratospheric Test Flights

In our CUAS textbook, we covered the failed promises of HAPS technology using UAVS. (Nichols, et al., Counter Unmanned Aircraft Systems Technologies and Operations, 2020) However, there is progress.

HAPSMobile has successfully completed the fourth test flight of its Sunglider solar-powered high-altitude pseudo-satellite (HAPS) unmanned aerial vehicle (UAV). The test flight took place at Spaceport America in New Mexico, and its completion marks the conclusion of all basic aircraft tests for the aircraft. HAPSMobile will now begin preparations for stratospheric test flights. (UST Weekly eBrief, 2020) (See Figure 3.12)

During this round of testing, Sunglider reached altitudes higher than those of previous flights and maintained high altitudes for a long duration. Other test milestones included flight speed changes, steep turns, automated flight control in the event of interrupted communications with the Ground Control System, and in-flight balance control. (UST Weekly eBrief, 2020)

HAPSMobile has constructed a new specialized test site at Spaceport America, providing an additional facility to the existing test site on the Hawaiian island of Lanai. Spaceport America offers flexibility in coordinating test flight schedules, providing opportunities to conduct test flights with greater frequency and more freedom to conduct various types of tests. HAPSMobile also plans to conduct stratospheric test flights at Spaceport America. (UST Weekly eBrief, 2020)

Figure 3.12 HAPS Sunglider

Source: (UST Weekly eBrief, 2020)

Drones to Deliver Organ Transplants

Drones are slated to be the ideal technology to deliver organs to transplant patients—and a test program could soon make this premise a reality. Dr. Joseph Scalea, transplant surgeon at the University of Maryland Medical Center, is working with a group of researchers to explore if drones are a suitable method for transporting organs . The team recently concluded a series of 14 test flights that demonstrate the potential for drones to work as organ couriers. (Greenwood, 2019)

The team used a DJI M600 Pro drone for the experiment. See Figure 3.13. Its six motors lie directly below their respective rotors—and further away from its cargo, a smart cooler that contains an organ, reducing the organ's exposure to heat from the robot's motors. The team also designed a wireless biosensor that measures the organ's temperature, barometric pressure, altitude, vibration,

and GPS location while it is being transported. Finally, the team used a kidney that was not a viable transplant to test its drone. (Greenwood, 2019)

Figure 3.13 DJI M600 Pro for Organ Transplant
Source: (Greenwood, 2019)

The results, published by the IEEE, show the test was a success. [5] Biopsies of the kidney before and after the flight showed it remained undamaged. The temperature of the kidney remained at a stable 2.5°C, the air pressure matched the altitude, and the drone flew up to 67.6 kph. The kidney was even subjected to marginally fewer vibrations than it would have been exposed to on a fixed wing plane. (Greenwood, 2019)

Organs do not last very long outside the body, which means they must get to their intended recipients as soon as possible—often on short notice, making every second critical. But the current organ transport system relies on couriers, commercial airline schedules and expensive charter flights. Any delay or mistake during this process could mean the organ loses its effectiveness—or

deteriorates so much that it cannot be used at all. (Greenwood, 2019)

These costs and mistakes could be reduced by using drones. “It will be faster and cheaper and more predictable,” said Scalea. There are regulatory obstacles to overcome. The FAA strictly enforces limits on drone use, but the agency is planning to make changes based on data from 10 pilot programs–two of which plan to transport medical supplies. Those changes would make it possible for drones to make the organ transportation system–which supplies organs for more than 30,000 transplants a year–faster and more efficient. “Drones really work for this purpose,” said Scalea. (Greenwood, 2019) See Figure 3.14.

Figure 3.14 Organ Transplant coming in for landing at Hospital
Source: (Greenwood, 2019) https://spectrum.ieee.org/image/MzE3NTIwOA.gif

Robot Trucks?

The author is all for expanding the uses of drones in the transportation theater. But Robot trucks? Respectfully, this is a horrible idea. Living near a major trucking thoroughfare in Pennsylvania with 50+ huge trans-shipment / storage complexes off I-81 /, where real semi-trucks going North and South at a rate 100,000 + per hour along with triple that number in regular cars moving about 70 mph pile up the accidents (many fatal) every single day. This is with drivers that understand human nature, road rage, tailgating and impaired drivers have an advantage. Add to this mess robotic, autonomous, computer algorithm-based vehicles with lots of momentum and weight, portends a huge risk to public transportation. [6]

However, TuSimple, a self-driving startup with operations in the U.S. and China,[7] is opening what it calls the world's first "Autonomous Freight Network," a highway corridor stretching over 1,100 miles from Phoenix to Houston for its robot trucks to haul loads in a technology partnership with UPS, U.S. Xpress, Penske Truck Leasing and Berkshire Hathaway. The project involves the San Diego-based company's fleet of 40 self-driving semis (with human safety drivers in the cab), new proprietary software for TuSimple and its customers to monitor their on-road performance and location data, high-definition digital route maps and freight terminals at strategic locations.

TuSimple will haul revenue-generating loads for UPS and foodservice McLane as well as new customer U.S. Xpress on routes throughout the network–with Penske helping to maintain the trucks–and the partner firms can learn how to integrate robotic trucks into their operations. (Ohnsman, 2020)

If all goes as planned, TuSimple will expand the network from Los Angeles to Jacksonville, Florida, along U.S. Interstate-10 by 2022 and then start operating Level-4 self-driving truck services across the U.S. by 2023. "The network is the first of its kind to address how

you can bring autonomy to the market at scale," TuSimple President Cheng Lu tells Forbes. (Ohnsman, 2020)

Figure 3.15 TuSimple Autonomous Truck

Source: (Ohnsman, 2020)

Can you be sued for flying a Drone over Private Property – The New Tort Law

The draft of the proposed tort law relating to drones, due to be discussed by the Uniform Law Commission (ULC) soon, is out – and drone operators should be paying very close attention. What is Tort Law, and Who is the ULC? Why is this new Tort law important to drone owners?

The definition of "Tort," according to the Cornell Legal Information Institute, 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," and the point of a tort law is "to provide relief to injured parties for harms caused by others, to impose liability on parties responsible for the harm, and to deter others from

committing harmful acts." That relief, says the Institute, is typically, "damages in the form of monetary compensation." (McNabb, 2019)

The ULC, by their own definition, "provides states with non-partisan, well-conceived and well-drafted legislation that brings clarity and stability to critical areas of state statutory law." ULC is proposing a tort law relating to drones, which would give homeowners the right to sue drone operators for flying over their private property under certain conditions. (McNabb, 2019) See figure 3.16.

Figure 3.16 Drone footage over a private house and barn
Source: (McNabb, 2019)

Background on the Tort Law Relating to Drones – Draft One

The first draft of the tort law drew nearly universal condemnation from the drone industry. According to one expert "If the draft Act became law, the mere presence of a drone in the airspace up to 200 feet over private property would be, by definition, injuring the landowner and committing aerial trespass. Essentially, the draft Act does not recognize a distinction between a drone which harasses

the property owners by hovering feet from a window and a drone, operated by a certificated professional, hovering one foot inside a neighbor's property line to snap a photo of an adjacent property." That draft received many comments from drone industry stakeholders and failed to pass when the ULC met to discuss it. (McNabb, 2019)

The New Draft

The new draft does attempt to address some of the issues found in the first draft: for example, it creates a more narrow definition of aerial trespass that includes the terms "substantial interference with the use and enjoyment of the property," and defines "substantial interference." The new draft also includes clauses about the accidental or unavoidable landing of a drone on private property and specifies that landowners must return a drone that lands on their property to the operator. This proposal has such potential to materially impact legitimate drone operation that it behooves drone operators to take the time to educate themselves. (McNabb, 2019)

See additional quoted verbiage below from the new proposed ULC draft Tort law relating to drones. (McNabb, 2019)

Definition of "Airspace Intrusions" from the draft:

SECTION 5: AIRSPACE INTRUSIONS.

(a) An aerial trespass occurs when a person intentionally and without consent of the landowner operates an unmanned aircraft in the airspace over the landowner's property and by so doing causes substantial interference with the use and enjoyment of the property.

(b) The determination of whether an unmanned aircraft's operation over property has caused substantial interference with

the use and enjoyment of property shall be based upon a review of the totality of the circumstances, including:

(1) The amount of time the unmanned aircraft was operated over the landowner's property.

(2) The altitude at which the unmanned aircraft was operating.

(3) The number of times unmanned aircraft have been operated over the property.

(4) Whether the unmanned aircraft recorded or captured audio, video, or photographs while in operation over the property.

(5) Whether the landowner has regularly allowed operation of unmanned aircraft over the property.

(6) Whether the operation of the unmanned aircraft caused physical damage to persons or property.

(7) Whether the operation of the unmanned aircraft caused economic damage.

(8) The time of day the unmanned aircraft was operated over the landowner's property.

(9) Whether an individual on the land saw or heard the unmanned aircraft while it was over the property; and,

(10) The operator's purpose in operating the unmanned aircraft over the property.

(c) Repeated or continual operation of an unmanned aircraft over a landowner's property shall not give rise to prescriptive rights in the airspace

Definition of "Intrusions on Land":

SECTION 6: INTRUSIONS ON LAND.

(a) Except as provided in subsection (b), a person who, without permission, intentionally lands an unmanned aircraft on the land of another, or who intentionally causes an unmanned aircraft to come into physical contact with a structure, plant life, or individual on the land of another, commits a trespass to land.

(b) A trespass to land does not occur under subsection (a) when:

(1) the unmanned aircraft operator is forced to land the unmanned aircraft because of unexpected circumstances that reasonably justify such a landing; or,

(2) the unmanned aircraft malfunctions or otherwise touches down upon the surface of the land because of weather or other factors beyond the operator's control.

(c) A person asserting the privileges provided in subsection (b) is liable for any damage caused by the unmanned aircraft's operation.

(d) Regardless of how an unmanned aircraft came to rest upon the property of another, the owner or operator of the unmanned aircraft has a right to recover the unmanned aircraft upon a request to the owner of such property. A landowner shall not unreasonably refuse a request to return the unmanned aircraft or to permit the unmanned aircraft's operator to recover the unmanned aircraft from the property.

Definition of "Violations of Privacy":

SECTION 8: UNMANNED AIRCRAFT AND VIOLATIONS OF PRIVACY.

(a) Privacy related civil actions may be based upon the operation of an unmanned aircraft.

(b) A determination of whether an unmanned aircraft's operation over property was used to violate a privacy-related right shall be based upon a review of the totality of the circumstances, including:

(1) Whether by hovering or repeated flights the unmanned aircraft was likely to have provided the operator with the opportunity to use the unmanned aircraft to view, listen to, record or capture by camera, microphone or other device, individuals who were present at that place and time; and,

(2) Whether the operator made statements or took other overt actions indicating a desire to use an unmanned aircraft to infringe upon rights of privacy recognized in this state.

The full draft of the proposed Tort law on drones (which is still being debated) can be obtained at this link: https://www.uniformlaws.org/viewdocument/march-2019-committee-meeting-draf-1?CommunityKey=2cb85e0d-0a32-4182-adee-ee15c7e1eb20&tab=librarydocuments (McNabb, 2019)

Drone owners should take note of above. This may be the restrictive direction that drone tort law is heading.

GPS Interference crashes drone in UK – Ligado debate rages

Staying on the trend of legal interest, the next story is about GPS interference crashing a survey drone in the US. An expensive drone crashed into a house in December when it lost GPS signals due to interference, according to an accident investigation by the United Kingdom. The drone, a DJI M600 Pro was surveying a construction site when the mishap occurred. The DJI M600 Pro can weigh as much as 34lbs (15.5kg) and is listed at $5,699 on the vendor's website. (Goward, 2020)

According to D.A. Goward ((Goward, 2020), The mishap has given added impetus to those in the United States opposed to the Federal Communications Commission (FCC) decision to allow Ligado Networks to transmit on a frequency near to that of GPS. U.S. government tests have shown that high precision GPS receivers, like those used on some survey drones, may not have reliable signals whenever they are within 3,400 meters (2+ miles) of a Ligado transmitter. Drones with less precise, general purpose GPS receivers could be impacted within 1,040 meters (.6 miles).

Drones with unreliable GPS can wander into areas they are not allowed and eventually crash. The larger and heavier the drone, the more dangerous this can be. Most commercial drones are less than 100 lbs (45kg), though some models can weigh in at 200 lbs (90 kg) or more. While drones are supposed to remain within the line of sight of the operator, when GPS navigation is lost, many enter an "attitude mode." This results in the aircraft maintaining its height above the ground and its wings level using on-board barometric and inertial sensors. It cannot hold its position over the ground though, without GPS and so will drift with the wind. Unless the operator takes manual control right away the drone can drift out of the operator's sight. That usually also means it is unable to receive radio commands sent by the operator. (Goward, 2020)

This is precisely is what happened in this case, according to the UK's Aircraft Accident Investigation Board's report. A survey of a construction site by drone was in its second day. The first three flights were without incident. On the fourth flight the drone took off and reached about 65 feet above the ground. The pilot's controller then showed a GPS compass error. At that point, the drone stopped climbing and began drifting away in the wind at about 15 miles per hour. The pilot repeatedly selected the "return home" function to no avail before the aircraft flew beyond a line of trees and was out of sight. It hit the roof of a home several hundred yards beyond the trees and crashed in the backyard. (Goward, 2020)

After notifying police of the missing drone, the pilot prepared another drone to search for the lost one. However, shortly after takeoff, the controller again showed a signal-interference error message and the pilot immediately landed it. The accident report's analysis cites signal interference with GPS as cause of the malfunction of the drone that crashed and the second one that was to look for it. It says the source of the interference was not identified. The report also observes that serious injury or death could have resulted. (Goward, 2020) The report indicates:

"… analysis indicated that a mass of more than 2 kg falling from the roof of the house could have resulted in a serious or even fatal injury to people if they had been struck. The aircraft mass, at 12.8 kg, was well in excess of this figure and therefore it is very likely that serious injuries would have occurred even if the person struck was wearing a hard hat for protection." (Goward, 2020)

Aviation interests in the United States had for years opposed the FCC granting Ligado Networks' application. Despite this and the formal and strong opposition of the executive branch of government, the FCC approved Ligado's request in April. The FCC's approval of Ligado Network's application has not silenced opposition. Rather it has caused opposition to spread across many industries and sectors. Vocal opponents now include agricultural, maritime, vehicle and industrial interests.

Legislation is under consideration in Congress that would cause the FCC's decision to be re-examined and prevent the Defense Department from doing business with any company that interferes with GPS signals. Some proposals would put a hold on the FCC's approval. While the drone mishap in the United Kingdom can be seen as a relatively minor event, as a portent of things to come, it is *MIGHT* [8] have a huge impact in the United States. (Goward, 2020)

Time to move from air to sea – specifically UUVs.

Autonomous Underwater Glider

Teledyne Marine's Slocum G2 Glider autonomous underwater vehicle (AUV) has completed a four-part circumnavigation of the Atlantic Ocean that lasted for over four years. The glider, named Silbo, covered a total of 22,744 km and spent approximately 1,273 days at sea. The trip is the first such journey to ever be undertaken by an AUV. (Ball, Autonomous Underwater Glider Circumnavigates Atlantic Ocean, 2020) See Figure 3.17

Over the four legs of its journey, Silbo interacted with international science teams from several countries, and collected scientific and critical engineering data for a variety of programs. During its three stops, the glider received repairs to a scratched hull, an external cleaning, and a fresh set of batteries, and required no other maintenance. (Ball, Autonomous Underwater Glider Circumnavigates Atlantic Ocean, 2020)

Following a factory upgrade to install an extended energy bay and thruster in preparation for its voyage, Silbo was launched in the early spring of 2016 from Cape Cod, Massachusetts. The first leg of its journey took it from Cape Cod to Ireland, covering a distance of 6557 km in 330 days. While in Ireland, Silbo participated in a Glider Training session hosted by the Marine Institute and P&O Maritime Services, Galway. (Ball, Autonomous Underwater Glider Circumnavigates Atlantic Ocean, 2020)

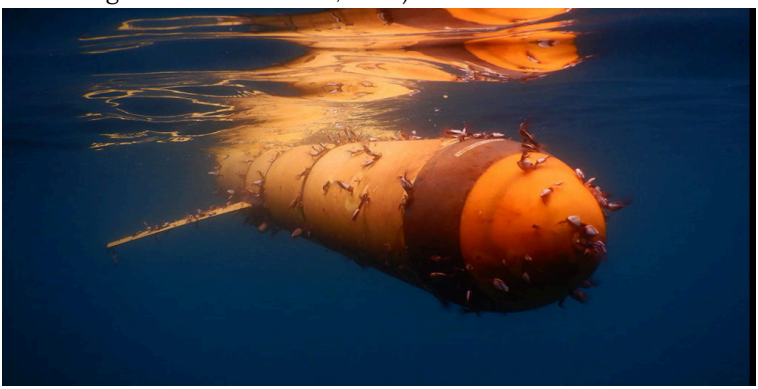


Figure 3.17 Teledyne Marine's Slocum G2 Glider autonomous underwater vehicle (AUV)

Source: (Ball, Autonomous Underwater Glider Circumnavigates Atlantic Ocean, 2020)

On the second leg, Silbo travelled from Ireland to the Canary Islands, covering 3695 km in 178 days, and participated in a "glider school" at the research facility Oceanic Platform of the Canary Islands (PLOCAN) and the University of Las Palmas de Gran Canaria (ULPCG). The third leg lasted 418 days, taking Silbo from the Canary Islands back across the Atlantic to St. Thomas, U.S. Virgin Islands, gliding 6256 km. Supported by staff and students from University of the Virgin Islands (UVI), St. Thomas, Teledyne technicians recovered, re-batteried and re-deployed Silbo in less than 24 hours. (Ball, Autonomous Underwater Glider Circumnavigates Atlantic Ocean, 2020)

Silbo's fourth and final journey from St. Thomas began on July 18, 2019 and concluded on June 29, 2020 south of Martha's Vineyard, completing the final 6236 km trek in 348 days. During this transit Silbo spent three months flying a butterfly pattern south of Bermuda contributing data to Bermuda Atlantic Time-series Study (BATS). Silbo then joined the Gulf Stream, becoming the season's first storm glider as Tropical Storm Arthur passed directly over the glider. (Ball, Autonomous Underwater Glider Circumnavigates Atlantic Ocean, 2020)

During this circumnavigation, Silbo collected hurricane data, corrected current models, and provided close to 5000 CTD (conductivity, temperature, and depth) casts that aided meteorological forecasting. With partners from Rutgers University and its student base, UVI, PLOCAN, UGCLP, the Marine Institute, and others, Silbo also participated in the Challenger glider mission. Silbo has also been used as a test bed for many new engineering hardware and software features for both existing and next generation Slocum gliders. Recent legs have provided data on new battery configurations, advanced software, and techniques for piloting long endurance missions and minimizing biofouling. (Ball,

Autonomous Underwater Glider Circumnavigates Atlantic Ocean, 2020)

Very cool![9]

New Autonomous Guard USV

Author Mike Ball gives us another cool view. This time for a new autonomous Guard USV unveiling.

A design for a new unmanned surface vessel (USV) concept, created by Sea Machines and a consortium of partners including C-Job Naval Architects, LISA Community, Seazip Offshore Service, Maritime Research Institute Netherlands (MARIN) and eL-Tec Elektrotechnologie, has been unveiled. The Autonomous Guard Vessel (AGV) is designed to provide a small, lighter, and more efficient alternative to current manned guard vessels used to protect maritime and offshore operations such as wind farms and cabling routes. (Ball, New Autonomous Guard USV Unveiled, 2020) See Figure 3.18.

Figure 3.18 Sea Machines USV Concept

Source: (Ball, New Autonomous Guard USV Unveiled, 2020)

The AGV can continuously monitor nearby marine traffic visually as well as via radar and AIS (automatic identification system) data, taking measures to secure the area in order to avoid collisions and damage to offshore infrastructure. The USV will attempt communications with any vessel that approaches the area, providing information on how to safely navigate the area as well as physical escort away from the site. The encounter will be recorded to provide video footage in case of any violation or accident. (Ball, New Autonomous Guard USV Unveiled, 2020)

As the autonomous platform does not require an onboard crew, it is considerably smaller than equivalent manned guard vessels. This lowers the operational cost and also allows it to be sustainably powered by batteries, which can be recharged via a charging station. This station can be moored independently or connected to existing onsite equipment, such as an offshore transformer platform. Depending on the situation, charging could be performed either via a cable connection to the on-site equipment, or locally generated using renewable fuels. (Ball, New Autonomous Guard USV Unveiled, 2020)

The consortium envisions that a typical offshore site will require a number of AGVs, which can take turns in monitoring the area and recharging. In addition to autonomous operation, remote control is also being considered for the vessel, in order to deal with situations that require human intervention. The AGV would be connected to a command center on a mothership or at a shore-based location, where a human operator will control the AGV remotely to ensure correct action is taken. In addition, all data collected by the AGV will be sent to the command center. (Ball, New Autonomous Guard USV Unveiled, 2020)

Frank Relou, business development manager at Sea Machines, stated: “Smart vessel technology will have the most significant initial impact on small workboats, such as this guard vessel. The development of autonomous technology for vessel operations are

occurring on an international level but namely in niche segments, such as the guard vessel and other examples, currently operating in (with supervised autonomy), *marine survey*, *fire*, *patrol*, *aquaculture and offshore wind operations*[10]." (Ball, New Autonomous Guard USV Unveiled, 2020)

Protecting Undersea Cables – A National Security Priority

Nadia Schadlow and Brayden Helwig [11]of Defense News (opinion) present a compelling national security case for protecting data transiting via underseas cables. (Schadlow & Helwig, 2020)

Data is arguably the most important strategic asset to emerge in the 21st century. Access to data and the ability to protect its integrity are vital to American security and prosperity. As 5G and artificial intelligence transform our societies into highly integrated networks, protecting data will become even more crucial. In recent years, American efforts have focused on preventing Huawei, the party-controlled Chinese telecommunications giant, from gaining ground as the world's largest supplier of 5G infrastructure. But defending a less understood part of our digital infrastructure – undersea fiber-optic cables – should be an equal priority. Without the approximately 750,000 miles of cables that crisscross the world's oceans, our interconnected, digitally driven societies would be unable to function. (Schadlow & Helwig, 2020)

In 1858, when the first submarine cable was installed, sending a message across the Atlantic took nearly 18 hours. Today, the fastest undersea cables can transfer data at speeds upward of 25 terabytes per second – more than twice the amount of data generated by the Hubble Space Telescope each year.

Undersea cables make instant communications possible, transporting some 95 percent of the data and voice traffic that crosses international boundaries. They also form the backbone of the global economy – roughly $10 trillion in financial transactions

are transmitted via these cables each day. And undersea infrastructure is not just for civilian use. The U.S. government relies on cables to transmit information. (Schadlow & Helwig, 2020)

America's competitors consider undersea cables strategically significant. Tapping undersea cables could provide foreign leaders with valuable intelligence, while severing cables could slow communications between the U.S. and its NATO allies significantly – perhaps by even months. (Schadlow & Helwig, 2020)

Data can also be siphoned from undersea cables. This is most easily done during the cable manufacturing process, when backdoors could be inserted to collect information. Similar vulnerabilities exist at onshore landing stations, where cables connect to terrestrial networks. Cables can be tapped at sea, though this is relatively difficult to do. (Schadlow & Helwig, 2020)

Russia and China have developed capabilities in these areas. Russian submarine activity near undersea cables is well-documented: The Yantar, a Russian spy ship, carries mini submersibles that can either sever or tap them. Russian activity often clusters around crucial, yet hard-to-reach cables because these are difficult to repair. (Schadlow & Helwig, 2020)

Chinese officials view control of undersea infrastructure as part of a broader strategic competition for data. One official Chinese Communist Party outlet explained that "although undersea cable laying is a business, it is also a battlefield where information can be obtained." Huawei Marine, a Huawei subsidiary, is a major player in the undersea cable industry. The company has built or repaired almost a quarter of the world's approximately 400 submarine cables. But American officials worry that cables laid or serviced by the company may be accessed by the Chinese government. In 2019, amid increasing scrutiny from the U.S. and its allies, Huawei sold its subsidiary to Hengtong Optic-Electric, a Chinese fiber and cable manufacturer. But the sale failed to alleviate national security concerns: Hengtong's director and founder is a Chinese government official. (Schadlow & Helwig, 2020) China could also integrate undersea cable disruption into its military strategy. Last year, a

Taiwanese think tank warned that in the early stages of a Chinese invasion of the island, the People's Liberation Army may sever Taiwan's undersea cables, isolating it from the U.S. and regional allies. (Schadlow & Helwig, 2020)

Protecting undersea cable infrastructure must become a priority for U.S. officials and lawmakers. According to Schadlow and Helwig, there are several steps they can take to address the problem.

First, the U.S. government should take more responsibility for repairing undersea infrastructure. Currently, cable repairs are considered a commercial responsibility, rather than a national security concern. Classifying cable repairs as matters of national security and developing a public-private operational plan – that includes a division of resources – to repair them is one step toward reducing the response time to a disruption or an attack. (Schadlow & Helwig, 2020)

Second, as a 2017 report from the Office of the Director of National Intelligence suggested, the U.S. should push for stronger protections for undersea infrastructure in international law, including criminalizing attacks on submarine cables. These efforts should be coordinated closely with America's allies, especially those in Europe and East Asia. (Schadlow & Helwig, 2020)

Third, telecommunications companies must better secure cable infrastructure against potential attacks. Companies such as Google, Microsoft, Facebook, and Amazon now own or lease nearly half the world's undersea bandwidth. Companies could begin by securing cable landing stations, while investing in technologies that detect and deny undersea espionage. The executive branch could consider tax incentives to spur these steps. (Schadlow & Helwig, 2020)

Finally, the Trump administration should sound a louder alarm on Huawei Marine. In order to reduce or prevent the exfiltration

of data, telecommunications companies should be required to use undersea infrastructure from verified suppliers. At the very least, owners of data transmitted this way should be aware of the undersea path their data is taking – and potential vulnerabilities. Ultimately, undersea cables help keep Americans connected, prosperous and safe. Protecting them from sabotage and espionage is a vital national security interest of the United States. (Schadlow & Helwig, 2020)

Navy Large Unmanned Surface and Undersea Vehicles: Background and Issues for Congress

Although too large to summarize in this chapter, the author would like to bring to attention a report to congress by Ronald O'Rourke, Specialist in Naval Affairs entitled: *Navy Large Unmanned Surface and Undersea Vehicles: Background and Issues for Congress, R45757.* It can be found at: https://fas.org/sgp/crs/weapons/R45757.pdf (O'Rourke, 2020)

This report provides background information and potential issues for Congress for three types of large unmanned vehicles (UVs) that the Navy wants to develop and procure in FY2021 and beyond:

- Large Unmanned Surface Vehicles (LUSVs).
- Medium Unmanned Surface Vehicles (MUSVs); and
- Extra-large Unmanned Undersea Vehicles (XLUUVs).

The Navy wants to acquire these large UVs as part of an effort to shift the Navy to a new fleet architecture (i.e., a new combination of ships and other platforms) that is more widely distributed than the Navy's current fleet architecture. The Navy is requesting $579.9 million in FY2021 research and development funding for these large UVs and their enabling technologies. (O'Rourke, 2020)

The issue for Congress is whether to approve, reject, or modify the Navy's acquisition strategies and FY2021 funding requests for

these large UVs. The Navy's proposals for developing and procuring them pose a number of oversight issues for Congress. Congress's decisions on these issues could substantially affect Navy capabilities and funding requirements and the shipbuilding
and UV industrial bases. (O'Rourke, 2020)

In addition to the large UVs covered in this report, the Navy also wants to develop and procure smaller USVs and UUVs, as well as unmanned aerial vehicles (UAVs) of various sizes. Other U.S. military services are developing, procuring, and operating their own types of UVs. (O'Rourke, 2020) The O'Rourke is a treasure trove of USN design, architecture, and strategic information.

Drone Sightings: The Actual Non-Hyped Numbers Analyzed

On Linkedin via sUAS News, a solid report by Jonathan Rupprecht popped up on 5 August 2020 exposed the disinformation, double counting and misinformation about drone sightings based on analyses of six (6) years of reported data from FAA and local government data / reports. It is an eye-opening report! (Rupprecht, 2020) Here is a summary of findings:

Background

For years and years, many have been talking about the FAA's drone sightings reports. The drone sightings reports have been cited many times by the news media and elected officials who were rather alarmed about the data. Others in the industry cite the drone sightings as evidence of the greater need for the government(s) to do something by creating regulations. Some counter-drone companies have used it to show a need for their product. Others say it is hype and the sightings data is greatly flawed and overblown because after all, they are only sightings, not impacts.

Regardless of where you come from in the industry and your motives, we need to accurately understand the drone sightings

data. The report critically considers the growth of drone sightings, where they typically are located, and whether the data is alarming as many have said. (Rupprecht, 2020)

Quick Summary of the Drone Sightings:

- The reported drone sightings over time are NOT growing. They are decreasing.
- The FAA has inaccurately reported on the drone sightings data and this is proven by their own data they released(more on that later).
- There are more drone sightings reported in populated areas than unpopulated areas.
- There are more drone sightings reported in warmer months than colder months.
- States with larger populations have more reported drone sightings.
- There are more medium or large animal impacts with manned aircraft than mere reported drone sightings.
- Any discussions we have on this topic should be using numbers and not just percentages or words. (Rupprecht, 2020)

Basically, population and weather/climate are the determining factors of when and where you will have drone sightings. The data also shows that we are past a peak in sightings and they are currently consistently decreasing. But how many of these sightings are verified sightings of drones and not white balloons, seagulls, etc.? (Rupprecht, 2020)

How many of these reported sightings are of drones actually flying unlawfully, dangerously, or nefariously? Is there like a giant ? face on the drone that tells you it is bad? A drone being flown by a

good guy and one being flown by a bad guy are extremely difficult to tell apart. (Rupprecht, 2020)

What Does the Word "Sighting" Mean?

Sightings are just that….mere sightings. A pilot, person on the ground, law enforcement officer, etc. sees a drone and reports it to the FAA. It gets logged. The drone could be lawfully flying, safely flying, carelessly flying, or flying with criminal intent. It is all lumped into one thing – a sighting.

"The accuracy of the reports cannot be verified. You could report you saw a drone all you want. No one can check. It is literally a giant hearsay list. And here is a very thought-provoking question….is there any way we can prevent people who would stand to benefit from higher drone sighting numbers from calling in false sightings? Who is to stop the FAA employees, FAA contractors, people working in counter UAS industry, or manned pilots from calling in more sightings that cannot be verified? Who is to stop over reporting where anything just gets reported as a drone?" (Rupprecht, 2020)

"Keep in mind that 18 U.S.C. 1001 makes it a criminal offense to make false statements to the FAA so many will be deterred from doing that. Some of the reports have identifiable information so they are not really anonymous and less likely to false report. On the other hand, the Department of Transportation's Inspector General's Office does investigate FAA officials for illegal activity and police arrest people all the time for fraudulent activity." (Rupprecht, 2020)

"Provide what weight you will to the sightings. We are in a predicament. There is no evidence to prove that any of those groups reported falsely, but there is also no evidence to prove that everyone reported truthfully AND accurately. We need to be balanced in approaching this data." (Rupprecht, 2020)

The rest of the Rupprecht report analyzes data from multiple FAA and LEO publicly available sources available from 2014. All the resources are available for the reader to follow the threads so engaged.

Skyborg and Boeing's Loyal Wingman Drone Projects

Let us end our palate tasting with two of the newest CUAS Drone programs from the USAF.

First up is Skyborg. It is USAF's future AI fleet. According to analyst Harry Lye, The US Air Force is flying at supersonic speeds towards an AI-enabled fleet. Under project Skyborg's direction, future fighter jets will not be supported by a wingman, but by an unmanned combat aerial vehicle. Harry Lye finds out more about the unmanned wingman of the future. (Lye, 2019)

Finger four has been the dominant fighter aircraft formation since the 1930s. The world's most advanced fighter jet, the Lockheed Martin F-35, costs around $100m per jet. Four of these in formation means almost half a billion dollars of hardware in the air (not including the per hour cost of flying them). Losing just one fighter would be catastrophic for the US Air Force's budget. (Lye, 2019)

The US Air Force's (USAF) project Skyborg aims to address this cost risk by replacing some of these expensive fighter jets with more affordable unmanned combat aerial vehicles (UCAVs) acting as unmanned wingmen.

Teaming up with drones

Under the project, the Kratos-built XQ-58 Valkyrie drone will team up with the F-35 and F-15EX, cutting the number of highly valuable fighters in the air, as well as cutting costs and risk to human life. See Figure 3.19. At a cost of a few million dollars per unit, the

autonomous Valkyrie drones are more easily replaceable, and could form a central role in the USAF's air power. The F-35 is billed as a force-multiplier; when partnered with a Valkyrie it could get a new capability boost. (Lye, 2019)

Skyborg program manager Ben Tran explained the significance of the program: "There is heavy investment by our near-peer adversaries in artificial intelligence (AI) and autonomy in general. We know that when you couple autonomy and AI with systems like low-cost attributes, that can increase capability significantly and be a force multiplier for our air force. The 2023 goal line is our attempt at bringing something to bear in a relatively quick time frame to show that we can bring that kind of capability to the fight." (Lye, 2019)

With Skyborg the manned aircraft is the center of the network, with the drones augmenting around it. Think of the fighter as Skynet and the Valkyrie UCAV as the T-100, only with added wings and less Arnold Schwarzenegger. AI will govern the autonomous wingman, reading telemetry, flight plans and weather, all the while acquiring targets and supporting the manned aircraft. (Lye, 2019)

Cultural questions facing the air force

If an autonomous combat drone is to act as a wingman who pulls the trigger? The US, UK, and Russia have pushed against the UN trying to ban autonomous killing machines, which gives a clue to where the Pentagon is currently leaning.

"With the adoption of autonomous systems becoming imminent, armed forces will need to confront serious ethical issues. On the one hand, it makes sense to give the drone trigger control. A pilot in an F-35 performing counter-maneuvers to avoid an enemy fighter may not have time to pull the trigger. On the other, if an AI system

accidentally fires at a civilian site who is held accountable?" (Lye, 2019)

The pilot, of the networked fighter, or someone higher up the staffing chain. The US Air Force has not said it plans to give the Skyborg drones control of any weapons systems, but this could be regarded as the natural evolution of the system in the future.

Figure 3.19 Kratos-built XQ-58 Valkyrie Drone
Source: (Lye, 2019)

Boeing *Loyal Wingman* Drone

Finally, we end this chapter with the Boeing Loyal Wingman Drone. The Royal Australian Air Force has its first Boeing-built drone-jet hybrid prototype, which will use artificial intelligence to conduct intelligence, surveillance, and reconnaissance missions to supply fighter pilots with more information during a conflict.

The company delivered its first “loyal wingman” prototype to Australia this week (7 May 2020); it is expected to be used in tandem with fourth- and fifth-generation fighters on the battlefield, officials said in a release. See Figure 3.20. (Pawlyk, 2020)

Figure 3.20 Boeing Loyal Wingman Drone
Source: (Pawlyk, 2020)

It is also the first aircraft “to be designed, engineered and manufactured in Australia in more than 50 years,” Boeing said, adding that it is the company’s “largest investment in an unmanned aircraft outside of the United States.” (Pawlyk, 2020)

The aircraft, which Boeing is co-developing with the government of Australia, was unveiled at the Avalon Airshow last year. Australia is investing roughly $40 million into the program, CNN reported. The jet is 38 feet long and can fly more than 2,000 nautical miles, according to its fact sheet. (Pawlyk, 2020)

It uses artificial intelligence “to fly independently or in support

of manned aircraft while maintaining safe distance between other aircraft, the fact sheet states. The first prototype was constructed using digital engineering concepts, allowing developers to simulate parts via computer models, according to the company.

The concept is similar to an ongoing U.S. military effort. The U.S. Air Force has been working to develop its own "Loyal Wingman" program, featuring unmanned fighters that could think autonomously sent out alongside F-35 Joint Strike Fighters, for example, to scout enemy territory ahead of a strike, or to gather intel for the aircraft formation. In January 2020, the Air Force conducted test flights of the XQ-58A Valkyrie drone at Yuma Proving Ground, Arizona, taking the unmanned aerial vehicle, made by Kratos Defense, to higher altitudes than previous tests. (Pawlyk, 2020)

Conclusions

We end our tour de force having traveled through a palate of air and sea stories which should indicate to the student the diversity, complexity, technological growth, and ubiquitous nature of the unmanned industry. Definitely tip of the spear. No homework or discussion questions. Build your own library of information "Bullets" on UAS , UUV and UGT systems.

REFERENCES

Ball, M. (2020, July 20). *Autonomous Underwater Glider Circumnavigates Atlantic Ocean.* Retrieved from www.unmannedsystemstechnology.com: https://www.unmannedsystemstechnology.com/2020/07/autonomous-underwater-glider-circumnavigates-atlantic-ocean/

Ball, M. (2020, July 21). *New Autonomous Guard USV Unveiled.* Retrieved from www.unmannedsystemstechnology.com: https://www.unmannedsystemstechnology.com/2020/07/new-autonomous-guard-usv-unveiled/

Bombing, C. -C. (2020, August 4). *Recognize Suspicious Unmanned*

Aircraft Systems (UAS). Retrieved from www.CISA.gov/obp: www.cisa.gov/usa-critical-infrastructure

Cole, S. (2020, August 3). *Motherboard Tech: Cops are using drones to make sure people aren't nude.* Retrieved from https://www.vice.com/en_us/article/z3eqv5/minnesota-drone-nude-beach: https://www.vice.com/en_us/article/z3eqv5/minnesota-drone-nude-beach

Goward, D. (2020, July 20). *GPS interference crashed a survey drone in the UK. Will the debate resonate in the US? OPINION.* Retrieved from www.c4isrnet.com/opinion/: https://www.c4isrnet.com/opinion/2020/07/20/gps-interference-crashed-a-survey-drone-in-the-uk-will-the-debate-resonate-in-the-us/#:~:text=An%20expensive%20drone%20crashed%20into,site%20when%20the%20mishap%20occurred.

Greenwood, M. (2019, Jan 19). *Could Drones Be Used to Deliver Transplant Organs?* Retrieved from www.engineering.com/: https://www.engineering.com/DesignerEdge/DesignerEdgeArticles/ArticleID/18325/Could-Drones-Be-Used-to-Deliver-Transplant-Organs.aspx

Kesteloo, H. (2020, July 2). *National Geographic team survey Everest with a drone at 28,300 feet.* Retrieved from https://dronexl.co/2020/07/02/national-geographic-mount-everest-drone/: https://dronexl.co/2020/07/02/national-geographic-mount-everest-drone/

McNabb, M. (2019, March 3). *Pay Attention to This One: Can You Be Sued for Flying a Drone Over Private Property? The Next Draft of that Tort Law.* Retrieved from dronelife.com: https://dronelife.com/2019/03/19/can-you-be-sued-for-flying-a-drone-over-private-property-the-next-draft-of-that-tort-law/

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. M., & & Hood, J. P. (2020). *Counter Unmanned Aircraft Systems Technologies & Operations.* Manhattan, KS: New Prairie Press #31.

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., Ryan, J., Mumm, H., Carter, C., Lonstein, W., & Hood, &. J. (2020). *Counter Unmanned Aircraft Systems Technologies and Operations.* Manhattan, KS: New Prairie Press #31.

Nichols, R., Ryan, J., Mumm, H., Lonstein, W., Carter, C., & & Hood, J. (2019). *Unmanned Aircraft Systems (UAS) in Cyber Domain: Protecting USA's Advanced Air Assets, 2nd Edition.* Manhattan, KS: New Prairie Press #27 .

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.

Ohnsman, A. (2020, July 1). *Robot Trucks To Roam 1,100-Mile Phoenix-Houston Corridor Set Up By TuSimple, UPS, U.S. Xpress.* Retrieved from www.forbes.com: https://www.forbes.com/sites/alanohnsman/2020/07/01/robot-trucks-to-roam-1100-mile-phoenix-houston-corridor-set-up-by-tusimple-ups-us-xpress/?ss=logistics-transport#24e1a00e3a84

O'Rourke, R. (2020, June 24). *Navy Large Unmanned Surface and Undersea.* Retrieved from fas.org/sgp/crs/weapons/: https://fas.org/sgp/crs/weapons/R45757.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

PRBC. (2020, August 6). *PB2-21. – Proper attire required.* Retrieved from minneapolisn.gov: https://library.municode.com/mn/minneapolis/codes/code_of_ordinances?nodeId=PAREBOCOOR_CH2GEREGOCO

Precision AG . (2020, June 11). *precisionagreviews.com.* Retrieved from www.precisionagreviews.com/: https://www.precisionagreviews.com/post/is-swarm-farming-the-future-of-farming

Randall K. Nichols, D. J. (2000). *Defending Your Digital Assets against Hackers, Crackers, Spies and Thieves.* New York: RSA Press.

Schadlow, B., & Helwig, N. (2020, July 1). *Protecting undersea cables must be made a national security priority.* Retrieved from www.defensenews.com/opinion: https://www.defensenews.com/opinion/commentary/2020/07/01/protecting-undersea-cables-must-be-made-a-national-security-priority/

Steffen, A. (2020, March 8). *watch-the-world's-first-manned-aerobatic-drone-loop-and-roll.* Retrieved from https://www.intelligentliving.co: https://www.intelligentliving.co/watch-the-worlds-first-manned-aerobatic-drone-loop-and-roll/

USA weekly. (2020, June 17). *Drone Technology Helps Researchers Count Turtles On The Great Barrier Reef.* Retrieved from https://uasweekly.com/: https://uasweekly.com/2020/06/17/drone-technology-helps-researchers-count-turtles-on-the-great-barrier-reef/

UST Weekly eBrief. (2020, August 4th). *HAPS UAV Completes Basic Flight Tests.* Retrieved from www.unmannedsystemstechnology.com: https://www.unmannedsystemstechnology.com/2020/07/haps-uav-completes-basic-flight-tests/

Zimmer, J. (2020, June 12). *Fighting COVID-19 with Disinfecting Drones and Thermal Sensors.* Retrieved from new.engineering.com: https://new.engineering.com/story/fighting-covid-19-with-disinfecting-drones-and-thermal-sensors

[1] The full citation is : **PB2-21. – Proper attire required.**

No person ten (10) years of age or older shall intentionally expose his or her own genitals, pubic area, buttocks or female breast below the top of the areola, with less than a fully opaque covering in or upon any park or parkway, as defined in PB1-1. This provision does not apply to theatrical, musical, or other artistic performances upon any park or parkway where no alcoholic beverages are sold. (Code 1960, As Amend., § 1010.321; Pk. Bd. Ord. No. 82-102, § 1, 4-21-82)

[2] Lost on Everest Video trailer: https://youtu.be/fyE39a8f2Ao

[3] The full Dunstan et.al research paper for the Raine Island Turtle count entitled: "Use of unmanned aerial vehicles (UAVs) for mark-resight nesting population estimation of adult female green sea turtles at Raine Island" is found at: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0228524

[4] Equipment Involved in the Study : The drones used in the study include the MFD 5000 from Watts Innovation, the Agras MG-1 from DJI, and M6A PRO G200 with a 16-liter tank from Homeland Surveillance & Electronics. North Dakota State University is lending SkySkopes the M6A PRO G200. "Each drone has its unique advantages. The MFD 5000 is extremely customizable. The MG-1 is water-resistant and a "tried and true" (tool) for precise agricultural spraying," said Dunlevy. For example, the M6A PRO G200 is designed specifically for crop dusting and spraying. (Zimmer, 2020)

[5] Maryland Test Confirms Drones Can Safely Deliver Human Organs- A kidney was flown thousands of meters by a drone without incurring any damage at: https://spectrum.ieee.org/the-human-os/robotics/drones/test-run-confirms-that-drones-can-safely-deliver-organs-for-transplant

[6] Author opinion.

[7] Note the Chinese influence here.

[8] Author emphasis

[9] Author emphasis

[10] Author emphasis

[11] Nadia Schadlow is a senior fellow at the Hudson Institute. She previously served as the U.S. deputy national security adviser for strategy. Brayden Helwig is a national security and international affairs summer intern.

PART II

SECTION 2: UNMANNED UNDERWATER SYSTEMS

4. Chapter 4 Underwater Autonomous Navigation & Other UUV Advances [Mumm]

Student Learning Objectives

The student will gain knowledge of the concepts and framework as it relates to how underwater vehicles navigate as well as explore the current and proposed advances in the unmanned underwater vehicle (UUV) arena.

The student will be able to:

- Understand the basic navigation techniques used to operate in underwater environments
- Gain an overview of how UUVs can safely operate around ports and manned vehicles.
- Consider new technologies being developed for use in UUVs and how that may impact UUV future uses
- Examine the direction of UUV technology to assist in exploring its intended and unintended uses and the consequences of these uses on the ocean and humankind.

History of Undersea Navigation-What is it, and Why Does it Matter?

The ability to navigate using roads, bridges coupled with maps, Global Positioning System (GPS), and the ability to see where to go are all modalities that are limited if not unavailable to underwater vehicles. We take for granted that we can see and sense our surroundings, even at night we simply turn on a light to illuminate our path. Underwater environments do not enable the use of so

many modalities, and thus, submarines and UUVs are quite literally navigating blindly most of the time. Unlike other forms of transportation and movement, most submarines and UUVs do not have windows. These vehicles must rely on sensors to guide their path to and from a destination. Near the surface, sailors can use a periscope, which was invented in 1902 by Mr. Simon Lake. Periscopes "are long tubes that have mirrors inside. The mirrors reflect images so sailors can see above the water." (Joanne, 2019)

Modern-day submarines use a "fiber optic imaging mast (which) sits in the sail outside the hull and sends electronic images to the crew…No periscope makes the hull of the ship stronger because it does not need to have an opening to poke through." (Joanne, 2019)

Sonar, which is short for sound, navigation, and ranging, detects undersea objects by transmitting powerful sound waves through the ocean and interpreting the returning signals that bounce off objects. Sonar systems have two modes, active and passive,

"In active sonar, the system emits a pulse of sound, and then the operator listens for echoes. These sonar waves can be varied in frequency and strength in order to allow it to distinguish targets of interest, and sonar can be used as a means of identification of an object as well as offering the submarine or UUV the ability to have its own unique identifier. In passive sonar, the operator listens to sounds emitted by the object one is trying to locate" (Discovery of Sound in the Sea, 2020).

The challenge with active sonar is that by sending out continuous signals through the water, the position of the submarine or UUV can be easily determined. Passive sonar systems simply listen without sending out active signals as "Ships, submarines, marine mammals, and fish all make noise, and this noise can be used by passive Sonar systems to locate them, in much the same way humans use their ears to locate someone speaking in a room (Discovery of Sound in the Sea, 2020).

Submarines and UUVs use "inertial guidance systems use gyroscopes to track the sub's motion from a fixed starting point. These systems are accurate for up to 150 hours of operation. Then

they must be realigned with surface navigation systems such as GPS, radar, or satellite." (Joanne, 2019). Figure 4.1 illustrates a typical gyroscope used in inertial navigation systems.

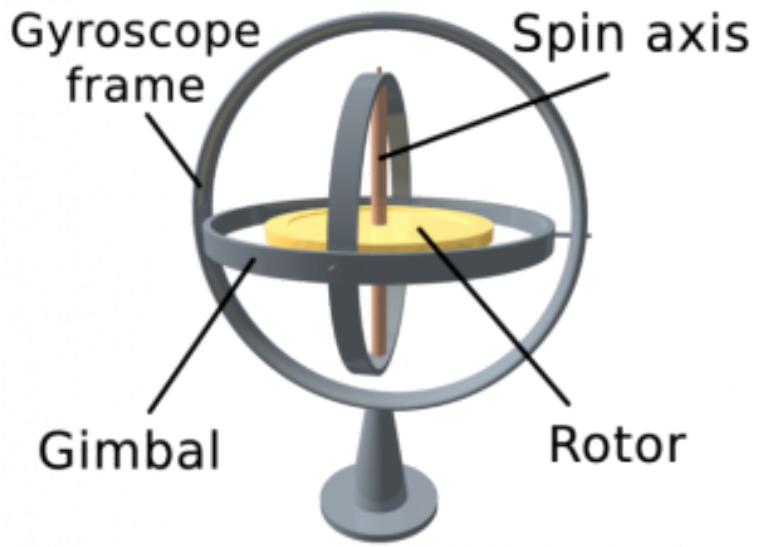


Figure 4.1: Traditional Gyroscope

Source: (Joanne, 2019)

A gyroscope is a wheel or disk mounted to spin rapidly around an axis that is free to turn in various directions. (Joanne, 2019).

A ships inertial navigation systems (SINS) can detect a change in the submarines geographic position (a move east or north, for example), a change in its velocity through the water (speed and direction of movement) and a change in its orientation (rotation about an axis). It does this by measuring the linear acceleration and angular velocity applied to the system. Since it requires no external reference (after initialization), it is immune to jamming and

deception. (Navigating a Submarine: Time and Navigation-The Untold Story of Getting from Here to There, 2020).

An inertial navigation system (based on Newton's second law) is made up of several gyros with accelerometers connected to one or more computers. The initial coordinates (location on the planet) are programmed in at dockside, and the inertial navigation systems is aligned before the submarine is launched. Once the sub is launched, the inertial navigations systems senses the acceleration and movements and reports this information to the computer that can calculate to within one to two nautical miles where the submarine is at on the planet. Generally, an accuracy of 1–2 NM should be acceptable with an accuracy of 1 NM (nautical mile) in 24 hours being a reasonable navigational drift error rate. The submarine can also surface to update its GPS fix or use any landmarks to correct its last known position. (Nobahari, 2017).

USS Alabama has three navigations systems, as seen in Figure 4.2. The three systems are the "ship's inertial navigation system (SINS), a Loran-C receiver, and a Transit satellite receiver system for correcting the inertial system. It has since been fitted with a GPS receiver and the Trident II navigation system." (Navigating a Submarine: Time and Navigation-The Untold Story of Getting from Here to There, 2020).

Figure 4.2: Parts of the USS Alabama Navigation System

Source: (Navigating a Submarine: Time and Navigation-The Untold Story of Getting from Here to There, 2020)

Minute errors in the measuring capabilities of the accelerometers or in the balance of the gyroscopes can introduce large errors into the information that the inertial guidance system provides. These instruments must, therefore, be constructed and maintained to strict tolerances, carefully aligned, and reinitialized at frequent intervals using an independent navigation system such as the global positioning system (GPS) (Inertial guidance system, 2020).

Current inertial navigation systems, such as those used on commercial jetliners, booster rockets, and orbiting satellites, calculate their turning rates measured by ring laser gyroscopes (see Figure 4.3) or by fiber-optic gyroscopes. These laser gyroscopes can be purchased on the open market for less than four thousand dollars. (Inertial guidance system, 2020).

Figure 4.3: Ring Laser Gyroscope

Source: (Inertial guidance system, 2020).

Active motorized precision laser ring gyroscope for inertial navigation system (Laser Ring Gyroscope for Inertial Navigation System , 2020)

Historically, there have always been navigational issues with submarines and the underwater environment. UUV navigation has been particularly hampered due to power requirements and the overall difficulty of communication signals/wave forms traveling through the water, in addition to interpreting caverns and signal instability or interruption from ocean sea life. With the introduction

of smaller, more efficient inertial navigation systems, GPS "suitable satellite communications, compact antennas, more capable underwater sensors, and powerful digital information processing, many other barriers to implementing quite ambitious UUV capabilities have fallen away" (Whitman, 2002). Some UUVs are now using fixed acoustic transponders to assist in triangulating position.

A new acoustic navigation system was developed to determine the position and speed of moving underwater objects such as divers and underwater vehicles. The path of an object and its speed were determined by the Doppler shifts of acoustic signals emitted by a transmitter placed on the object and received by four hydrophones installed at the periphery of the monitored body of water. The position and speed measurements were affected by errors mainly caused by acoustic reflections (returns) from the water body boundaries and surface reverberations. (Ostrowski, 2020).

The Office of Naval Research (ONR) contracted with Penn State Applied Research Lab to research and build enabling technologies for sonar-based continuous subsea autonomous navigation for manned and unmanned submarines. The joint effort is called the Advanced Broadband Navigation Sonar System Future Naval Capabilities program, and its main goals are to "improve undersea position and velocity estimation using sonar to give Navy manned submarines and unmanned underwater vehicles (UUVs) enhanced navigational performance." (Keller, 2019)

Navigation capabilities can also be improved with exteroceptive sensors (optical or sonar) that identify specific landmarks in the environment and use them to localize the UUV. If a map is available, this approach is known as map-based localization. When no map is available, AUVs can perform simultaneous localization and mapping (SLAM), in which the vehicle concurrently builds a map of relevant features and uses it to navigate. (Petillot, 2019).

The challenge facing UUVs is they will need to operate and navigate autonomously; the data collected must be accurate, reliable, and reusable. Using techniques such as SLAM "to help in autonomous navigation, namely in unstructured environments and

when the initial information is poor' in this technique, the robot constructs a coherent map of its environment while, at the same time, determines its location within that same map." (Ana Rita Silva, 2019).

This SLAM method can be used to inform and integrate into "Terrain-aided navigation (TAN), a form of geophysical localization where physical features of the seabed are exploited to localize an AUV within an *a priori* digital elevation model (DEM), or bathymetric reference map." (Salavasidis, 2019).

As the navigation of UUVs moves from past technologies and techniques into the future, "The accuracy and reliability of navigation information are one of the guarantees for AUV's successful execution…and the SINS/ Doppler velocity log (DVL) integrated navigation method can provide continuous and accurate navigation information for autonomous underwater vehicles" (Wang, 2020). However, this navigation method may contain large error or can be inaccurate when certain "beam measurements are inaccurate or outages for complex underwater environment… a novel tightly integrated navigation method composed of a SINS, a DVL, and a pressure sensor (PS) is proposed, in which beam measurements are used without transforming them to 3-D velocity" (Wang, 2020).

The ability to navigate underwater was created for manned systems. In the new frontier of UUVs, precision navigation by both manned and unmanned systems must be able to operate autonomously, alongside of and ultimately integrate with each other resulting in a safe and exciting future.

Advancements in the UUV Arena

Previously UUVs had limited technology available to them, this lack of advanced technology forced simplicity. With the focus now on multiple autonomous systems working in concert with each other and the integrated use of UUV with manned systems and "the sophistication and complexity of these new technologies have

attendant risks. Future strategic submarine navigation development requires attentive observance to ensure that the real benefits of affordability are realized by the insertion of new technologies" (Vajda, 1998)

In examining technology maturity models for the UUV arena, the examination quickly reveals that the technology is truly in its infancy state. As the model in Figure 4.4 indicates, simple automation is step one, and this is now being demonstrated with UUVs; however, UUVs are a long way off from being trusted independent, self-governing, with minimal human intervention.

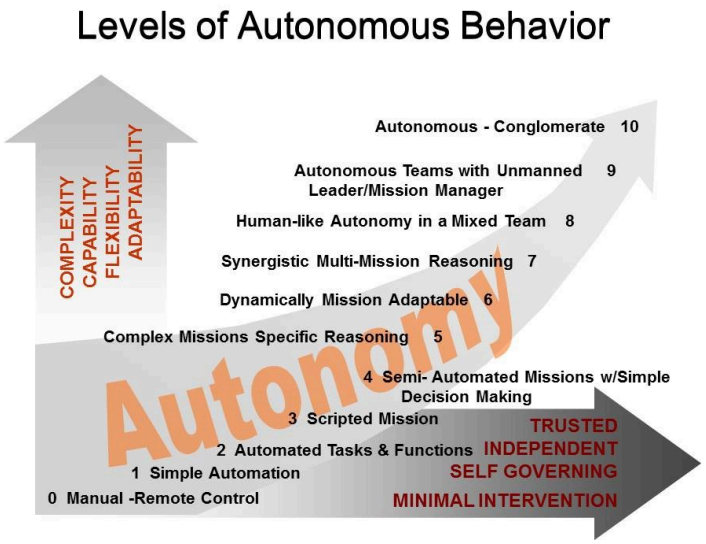


Figure 4.4: Levels of Autonomous Behavior

Source: (Mumm, 2019)

UUV advancements include such technology areas as propulsion, precise navigation, acoustic communication, low-speed vehicle

control, stealth, robotics, and mission control… both traditional and non-traditional navigation technologies, with traditional navigation encompassing improved inertial navigation, Doppler velocity sonar, and data fusion, and non-traditional techniques including terrain following, geophysical, and magnetic lines of position; acoustic underwater communications technologies that feature a high data rate and low bit error rate using channel equalization techniques; low-speed hydrodynamic control that employs an adaptive, nonlinear controller; and finally, command and control systems that utilize an intelligent controller with such capabilities as planning, re-planning, and fault tolerance. (Cancilliere, 1994).

One of the keys to the success of UUVs will be to mature the navigation capabilities as "a profusion of emerging navigation technologies enables us to further advance the strategic submarine navigation system in a more affordable manner" (Vajda, 1998). Several of these new navigation technologies are "based on a simple concept of overlaying maps…what we are defining as the "Geospatial Revolution "" (Kumar, 2014) as Geographic Information System (GIS) "technology, which has long provided effective solutions to the integration, visualization, and analysis of information about land, is now being similarly applied to oceans." (Wright, 2013)

In 2012, Esri launched an Ocean GIS initiative in support of GIS in both coastal and open ocean applications. The ability to map the oceans and the environmental and human physical changes that are occurring will be vital for autonomous UUVs to operate successfully and navigate in the most efficient manner possible. Figure 4.5 offers a glimpse of the layers of information that the Ocean GIS initiative will be able to provide for mapping and navigational aids.

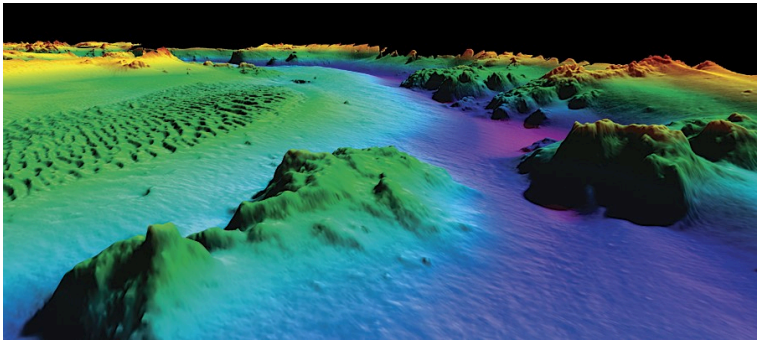


Figure 4.5: The Ocean GIS Initiative

Source:(Kumar, 2014)

The Ocean GIS Initiative: Taking GIS Underwater (Kumar, 2014)

Esri's Ocean GIS initiative is developing mapping and spatial analysis tools, geospatial data with the ocean's community in five main areas:

- Research and Exploration- Seafloor mapping and sampling, geomorphological studies, and tectonophysics
- Benthic habitat mapping for estimating species abundance, identifying essential fish habitat, and ultimately conserving sensitive or endangered areas
- Shoreline analysis, including calculation of rate-of-change statistics from multiple shoreline positions to analyze historical shoreline change
- Climate change, including measuring or simulating the potential impacts of sea-level rise on shorelines and wetlands, impacts of storms due to increasing ocean temperatures, impacts to ecosystems due to increasing ocean acidification, and global energy transfer
- Hazards, including the analysis of risk and potential loss of buildings and infrastructure due to hurricane winds, coastal

> floods, tsunamis, and nearshore or onshore earthquakes. (Wright, 2013)

Marine debris mapping and tracking is another area that GIS is attempting to assist with small plastics and other debris as they are not detectable with satellite imagery. In that past, it was not possible to integrate all of this data "Over 90% of cargo is shipped via Ships, and at least a hundred million people world over depend on the oceans for their living. Oil spills and other disasters in the past could not be modelled using GIS, but now we have the means to model them." (Kumar, 2014)

The different classes of UUVs is moving the industry from small hobby and research size vehicles of just a few meters in length into what is now known as an extra-large unmanned undersea vehicles (XLUUVs) "which are among the largest unmanned submersibles ever conceived, will be for long-endurance surveillance missions or undersea cargo vessels to deliver other sensor payloads and other UUVs." (Keller, 2019). Figure 4.6 offers a glimpse as to how fast the defense industry is moving towards XLUUVs. These large unmanned undersea vehicles could be used as motherships to deploy and recover smaller surveillance UUVs or be used to pair and team with manned submarines in the open ocean or along coastlines and inside harbors.

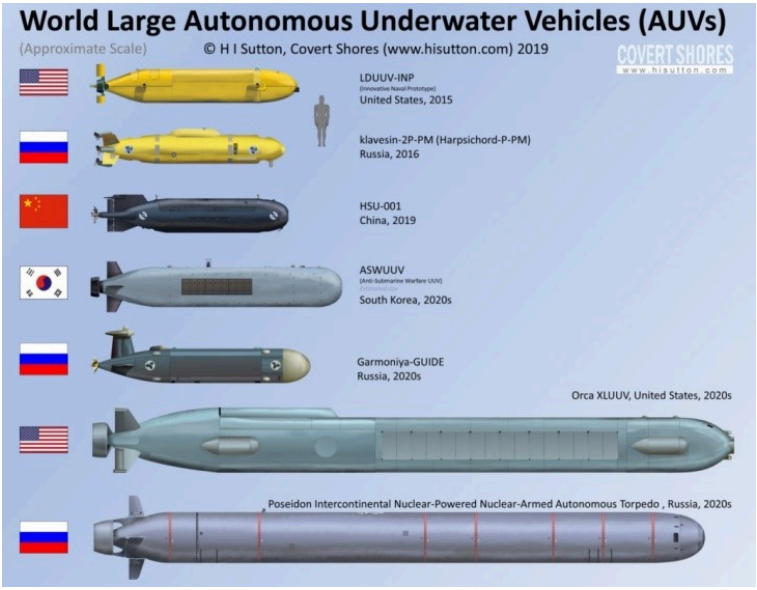


Figure 4.6: World Large Autonomous Underwater Vehicles
Source: (H, 2019)

The Orca project is being built by Lockheed Martin and Boeing, and it "is developing a delivery system for payloads that could involve persistent-surveillance sensors, weapons, or other UUVs and UAVs." (Keller, 2019). The Orca is being designed with modular construction principles and "will be an open-architecture reconfigurable UUV with the core vehicle providing guidance and control, navigation, autonomy, situational awareness, core communications, power distribution, energy and power, propulsion and maneuvering, and mission sensors." (Keller, 2019)

The advances in the UUV arena are notable from the control theories that will offer a gradual movement towards full autonomy, to the navigation, a real key to the ability for the UUV industry to become more mainstream in the defense, logistics, and commercial

arenas. The increasing investments in UUV technologies clearly signal the overall market acceptance of this unmanned system. The rapid escalation of both size and complexity of UUVs offers a glimpse of the integration of UUVs into the overall autonomous systems architecture and the emerging trust factor to team manned and unmanned systems together for the mutual success of all involved.

New Challenges Require New Thinking for Underwater Bases, Ports and Inland Waterways

Underwater bases for UUVs simply makes sense, as surface ships already operate in a known and agreed upon fashion in ports and waterways throughout the world. Attempting to add in UUVs to these already busy locations can add complexity that may create safety and economic issues that are not tenable in many locations.

In the underwater domain … achieving interoperability is currently impossible due to the lack of common standards and protocols for wireless communication.

Almost all underwater vehicles or sensors currently use proprietary interfaces and protocols for communication, especially for wireless communication in water.

This implies that UUVs made by different manufacturers cannot communicate with each other, even if they operate in the same area and human operators afloat or ashore cannot control these UUVs unless they use the control systems supplied by each manufacturer. (Wilson, 2019).

Up to this point, UUVs have been relatively benign sensor platforms; however, weaponization cannot be far behind. UUVs can quickly become formidable tactical and strategic weapons. Current UUV technology allows them to become a precision weapon that can be used in many varied ways. They can be used at different levels of warfare and eventually by either or both sides in a conflict.

The U.S. Navy's top officer has ordered his staff to develop a comprehensive strategy to field unmanned systems in the air, on the water and under the sea over the coming years. Dubbed

"unmanned campaign plan," it looks to tie together all the disparate programs into a coherent way forward, Chief of Naval Operations Adm. Michael Gilday told Defense News in a July 16 [2020] interview. "We've got … a family of unmanned systems we're working on," Gilday said. "Undersea we've got extra-large, large and medium [unmanned underwater vehicles]; on the surface, we have small, medium and large [unmanned surface vessels]; and in the air, we have a number of programs. (Larter, 2020)

At the lowest offensive conflict level, UUVs can be used to blockade a port, close off a straight, shadow ships or submarines or lie in wait around underwater bases. All these activities can be done with or without conventional warheads. Defensively, UUVs can provide a barrier to submarines, ships, and other UUVs. With a slight increase of the conflict level, UUVs can detonate enemy mines, eliminate enemy UUVs, and interfere with sonar systems on enemy ships or submarines. Should a UUV passively interfere with another vessel's navigation system, this leaves the UUV blind to possible submarine attacks. To save a lot of power and significantly increase the potential danger to enemy ships and submarines, the UUVs can also act like Remora fish and attach themselves to the enemy vessel. Subsequently, the UUVs can detach at their leisure to avoid capture and remain viable for the next vessel. In a more combative action, the UUV could have a targeted minor collision with a submarine's propeller; this in turn could cause significant increase in that submarine's signature to passive sonar detectors.

Rogue nations and non-state actors could likely occupy the next level of conflict by using UUVs to attack commercial shipping, oil platforms, undersea communication cables, offshore wind turbine power cables, undersea oil and gas pipelines or other defenseless targets. In this new type of asymmetric warfare, there are exponentially higher impact targets not traditionally defended. Government organizations and commercial entities will need to reassess how ocean assets are protected from this new threat. Organizations need to consider it is not only the UUVs abilities but

the UUVs host's capabilities that need to be considered for threat analysis.

In addition to the asymmetrical conflicts, there are also indirect levels of conflict. Cyber, drones, and some types of bioweapons are the current leaders in this arena. UUVs could soon be added to the list. Weaponized UUVs can render regional and international port facilities extremely vulnerable to disruption or even destruction. Additionally, vehicle and rail bridges, critical infrastructure on or adjacent to inland waterways could also severely disrupt the transportation system should a weaponized UUV find its' target.

Dams are difficult to attack from downstream. However, they are potentially vulnerable to lakeside attack. In this case, the release vehicle would be a boat or truck upstream of the dam leaving a large vulnerable area. Drones could also be considered as a potential release vehicle, however due to size, the drone would most likely be detected before the release point.

Inland waterways are often essential sources of water for towns and cities as well as to the commercial fishing industry and irrigation. These items can render the population vulnerable to a biological attack using a UUV as the release vehicle. These biological attacks may not be chemical but have the potential to use natural invasive species.

Direct Warfare Port Scenario

Direct warfare involves offensive and defensive operations directly related to the enemy's military and war-making capabilities. UUVs would be relevant sensor platforms, offensive and defensive weapons systems. Defensive operations would include not only manned vessels but enemy UUVs. All combatants on the water or under the water would become potential targets and would require defensive capabilities to survive. A primary survival technique is likely to be speed. UUVs generally lack the speed of military vessels. Short UUV sprints by specifically designed attack UUVs could still create some danger for those vessels or cause them to be fast and noisy for easier detection by manned attack vessels.

Imagine this scenario: as tensions between Taiwan and China spike, U.S. intelligence reports that PLA Navy warships will soon sortie from various Chinese ports. In response, U.S. submarines discreetly place a set of large unmanned undersea vehicles – one per port – on the seabed floor of the Taiwan Strait. Once settled, each UUV waits for the order to release a half-dozen smaller craft, each armed with explosives and non-kinetic effectors.

The order comes and the small craft deploy, maintaining connections to a command module via acoustic and satellite links. These tactical craft loiter just outside the ports, until one by one, they detect the unique acoustic signature of their assigned Chinese warship and break off to intercept it. Once in position, three feet under a Chinese keel, each tactical UUV signals its status back to a command center and awaits the order to immobilize its target. (Frandrup, 2019)

Leveraging Underwater Bases

As the rest of the world watches the scenario unfold, nations would establish underwater UUV bases to thwart these types of attacks. These same bases could also be leveraged to address the threat of quiet, cheap, manned attack submarines from rogue nations or illegal commercial activities. Quiet diesel-electric and fuel cell manned submarines could likely become a threat to coastal areas or that of our allies. Underwater UUV bases would allow continuous and routine UUV operations in the area. “The U.S. Navy is developing an underwater charging station for its unmanned undersea vehicles. The technology, which does away with cables, will make it easier for drones to recharge at sea.” (Mizokami, The Navy Is Working on Underwater Wireless Charging Stations for Robot Subs, 2017) The UUVs could also use these remote recharging stations to receive new mission instructions. UUVs with maintenance issues would be gathered up on a routine schedule by surface vessels, repaired, and released back to the base.

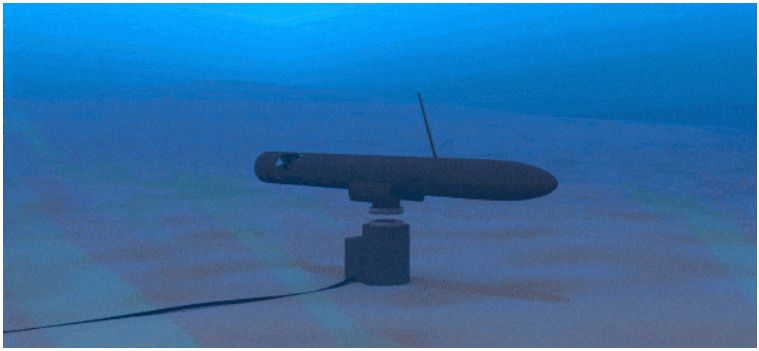


Figure 4.7: UUV Charging Station

Source: (Mizokami, Why Russia's Unique Supercavitating Torpedoes Are so Fast, 2019)

Underwater UUV bases similar to Figure 4.7 would become a significant force multiplier for the Navy. Powering and communicating with these underwater bases have several technical challenges. Power is potentially the easier issue to solve as there are geothermal, current turbines and even nuclear options available. Communications is often more challenging to achieve. For bases near to shore, a buried cable could be established. For those bases that are more remote, perhaps a dedicated UUV that surfaces randomly away from the base to communicate with a scheduled satellite link. Once the information is received from the satellite, the UUV could return to the remote base and download the information. Underwater optical links can be added if a distribution source is nearby, such as a modified undersea communications cable or a support ship.

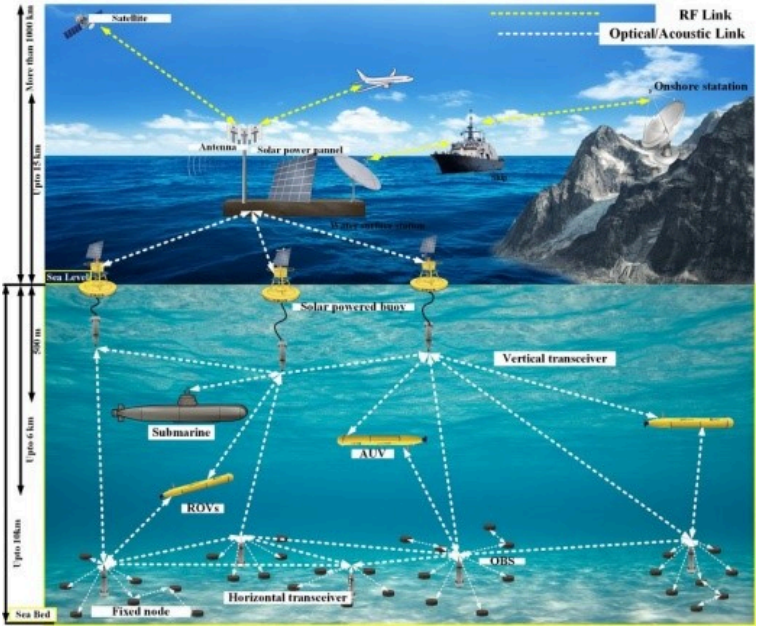


Figure 4.8: Optical Links for UUVs

Source: (Mohammad Ali, 2019)

Mission Planning with Swarming UUVs

The concept of swarming has been around for decades. Nature has led the way in providing successful examples of swarms with bees and ants. Part of the swarming theory is that no single entity has enough information to carry out a complex mission; however through mutual cooperation the swarm can successfully complete complex maneuvers in a multitude of environments. The swarming capability of unmanned systems has been demonstrated at rudimentary levels. Swarming capabilities are maturing as several UUVs are able to team with each other, as well as with manned submarines, surface vessels, and aircraft. See Figure 4.8 for how

UUVs could be linked together as a swarm. The capability for UUVs to act on their own mission objectives, and as a collaborative set with other UUVs to obtain a goal offers an almost limitless range of abilities for this technology. An example of this is the SwarmDiver, manufactured by Aquabotix Technology Corporation.

The Swarm Driver test vehicle can dive as deep as 600 feet while working in synch with other UUVs submersibles. "The swarming algorithm allows vehicles to communicate with each other to make decisions as a group. This allows SwarmDiver to quickly and accurately self-arrange in various swarm formations, as well as dive simultaneously to collect synoptic data sets," according to Aquabotix (Wilson, 2019).

Curiously, the ability for multiple unmanned systems to be assigned specific mission parameters as a single unit, and then sense the need to swarm with other systems to successfully complete a task is quite difficult to program. The technology to act as a single unit, swarm, and then again as a single unit has not been demonstrated to the level of confidence to believe that the technology is ready for real world implementation.

Current UUV operations almost exclusively involve a single vehicle performing a single task. In the future, UUVs will be able to operate in groups or even swarms. Size, speed, and range of UUVs coupled with the vastness of territory to be covered drive many offensive and defensive UUV scenarios to leverage the swarm theories. The possible exception to swarming is a category of very large UUVs or small manned hybrid powered submarines.

Perimeter Protection Planning Considerations

Swarms can be made up of homogeneous or heterogeneous UUVs. Unlike typical manned crafts where sensors, weapons, and decision-making authority are collocated, UUVs can split these functions up as required. Both homogeneous and heterogeneous UUV types are useful; however, these functions use power, take up space, and can be difficult to implement; this tends to drive the

heterogeneous UUVs towards swarms. Where some UUVs are the sensor platforms, some are the weapons platforms, and the decision making is distributed and collaborative.

The primary sensors for these UUVs will most likely be a variety of active and passive sonar coupled with cameras for close up operations. There are several sonar techniques for single vehicles, but when multiple vehicles are leveraged in the swarm environment, the bi-static method becomes very useful. One UUV pings and the others listen. The UUV that pings rotates in a preplanned manner to best cover the area and provide additional data for processing. Several sonar strategies will need to be developed for swarm detection and engagement operations. Will the engagement be active, passive, or bi-static? How many UUVs will commit to the engagement? Will more than one UUV be actively pinging? Will there be unique ping frequencies, or will a type of unique pulse repetition be used like with radar?

The term "asymmetric threat" is now familiar in the lexicon, and terrorist actions are a frequent occurrence. For naval forces, the classical terms "blue water" threat and "major threat axis" no longer hold the significance they once did. The threat environment has moved from the "blue water" to "brown water," or littoral regions, placing emphasis on power projection, force protection, and expeditionary operations in littoral areas. (Board, 2005)

Prior to the engagement, there must be several things to consider including identifying what types of weapons the UUVs might use? These weapons options can be divided into destructive and non-destructive. The destructive can be further decomposed into those that have warheads, those that have an integrated directional warheads but survive the attack to be reused, those that attach the warhead and leave before detonation, and those that expend ordinance from a distance that can be reused.

The first type of weapon may be a smart torpedo during the attack phase. The swarm is either deployed from a ship, sub, or underwater base and work as a team to acquire the target then determines the tactics to destroy the target using one or more of

the deployed UUVs. The next type of weapon would typically have a shaped charge as its destructive mechanism. This is most useful for eliminating mines, and it can also attack targets that are slow compared to the UUV. The weapon with an attack shaped charge warheads to targets are most useful in going after ships,

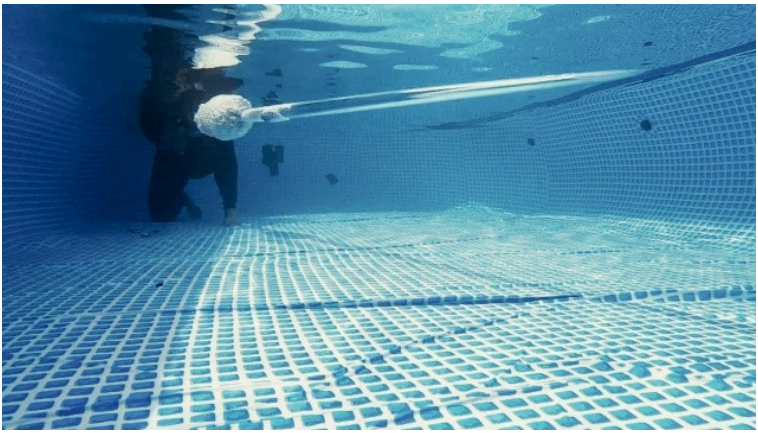


Figure 4.9: Supercavitating Bullet

Source: (Blain, 2019)

submarines, pipelines, or other stationary targets in a port scenario. They can also place open ocean fiber optic cables, pipelines, and oil rigs at risk. Each type can put these valuable items at risk. The last type allows for expanded tactics set and can engage targets faster than they are with enhanced success by operating as a swarm. The most common solution for this type of UUV is one that is large enough to deploy standard torpedoes. There are short and long standard torpedoes. It would be more likely for the UUV to use a shorter variety, but they could efficiently be designed for longer torpedoes. A less common, but more compact solution for this set of UUVs are the super cavitating weapons. These cavitating weapons come in two types: bullets or rockets. Bullets have a shorter range

and a smaller target set, but would be very effective against other UUVs, USVs (Unmanned Surface Vehicles), and other small boats. See Figure 4.9 as an example of a cavitating bullet underwater. "Norway's DSG has used the drag-reducing abilities of super-cavitation to produce some truly extraordinary projectiles that'll hit submerged targets up to 60 m (200 ft) away, opening up some interesting new mission capabilities" (Blain, 2019). The super cavitating rockets would have a longer range and potentially an extensive target set. The Russian VA-111 Shkval torpedo is a large version of this type of weapon. Water creates a lot of drag and typically limits torpedoes to about 50 knots.

Shkval solves this problem by diverting hot rocket exhaust out of its nose, which turns the water in front of it into steam. As the torpedo moves forward, it continues vaporizing the water in front of it, creating a thin bubble of gas. Traveling through gas, the torpedo encounters much less drag, allowing it to move at speeds of up 200 knots. (Mizokami, Why Russia's Unique Supercavitating Torpedoes Are so Fast, 2019)

One type of warhead was intentionally left out of the previous discussion, and that is a nuclear warhead. This type of warhead is unlikely to be used by the U.S. and its allies. However, it could easily become a weapon of choice for terrorists or rogue nations. It is not by chance, that many of the world's economic centers are located on coastal waters or major inland lakes and rivers. The threat acknowledgement by these cities would increase the need for new and different active defenses and additional channels for intelligence collections.

Strategies and tactics for UUVs are only limited by the type of UUV, the sensors, the weapons (if any), the target set, and the mission planner's creativity. It is expected that UUVs will expand significantly in both numbers and capabilities in the near future.

UUV Policies and Governance for Consideration

The ability to create UUV navigation lanes and standard operating procedures will require laws, policies, governance and leadership

from many organizations, host nations and port owners around the world. The U.S. National Geospatial-Intelligence Agency (NGA) is already tasked with providing geospatial intelligence (GEOINT) for navigable seaways as part of the Maritime Safety Office. The mission of the office is to "Provide global maritime geospatial intelligence in support of national security objectives, including safety of navigation, international obligations, and joint military operations" (Maritime Safety Information, 2020). Currently, there are no discernable leaders at the intersection of GEOINT and autonomous technology, security, and protocols – whether public, private, commercial, or international. There appears to be minimal government coordinated efforts that are actively examining the entire unmanned architecture and its massive GEOINT data needs.

The amount of information that NGA will be required to supply in the future is not well documented. NGA must capture future needs and GEOINT collection requirements for navigational safety in the new world of autonomous infrastructures. Spatial-temporal anomalies will become the norm, and NGA must document and engage in the construction of autonomous communal infrastructures and what data is required to allow these infrastructures to act and react accordingly for the safe operation of all autonomous systems.

The current autonomous system framework is fragmented without coherent oversight, direction, documented requirements, and lacks defined authorities, "Unmanned undersea operations continue to be limited by the complex, dynamic conditions of the ocean environment and the unique operational constraints they engender. Three critical capabilities – communication, energy, and autonomy – will drive future developments in this domain" (Analysis: Cyber in the Undersea, 2020). Advanced coordination and collaboration endeavors must be focused to include determining the responsibilities and authorities of an unmanned architecture, its specific uses, exceptions, and allowances for robotics operations; including studying the unintended consequences, future use, and misuse of such technologies.

Clear policies, laws, and governance are required as a danger to the nation, and a global response to UUVs is becoming undeniable. There is currently no single agency on a national or international level in charge of this issue. Currently, there are no policies, governance or doctrines in place for tracking or identification capable of offering reliable defenses against teamed autonomous systems. There is no single sensor type, defense posture, or reliable countermeasure to stop this evolving threat, although "The Navy also is moving forward with its new Unmanned Maritime Autonomy Architecture (UMAA) program to evaluate levels of autonomy in unmanned submarines, enable commonality of autonomy technologies, and reduce acquisition costs" (Wilson, 2019). This program will take years to solidify and become a part of the modern navy. The consequences can be catastrophic as asymmetric warfare becomes more asymmetric should governments fail to take a more pronounced leadership role in the autonomous arena.

Conclusions

UUV are an up and coming technology with many military and civilian uses already being explored. The technology breakthroughs that will allow UUVs to move towards their full potential will lag behind other autonomous systems; however UUVs will be included, integrated and connected to manned and unmanned systems within the next few years. Without ongoing, real-time communication with controllers, other vehicles and the framework to operate under "operators unmanned undersea systems will rely heavily on autonomy and artificial intelligence, and as operations increase in sophistication, intensity and complexity, the greater will be the need for trustworthy systems that can "OODA" (Observe, Orient, Decide, Act) in a dynamic and challenging environment" (Analysis: Cyber in the Undersea, 2020). The reliance on real time communication, the need for AI in UUVs and the immature nature of the laws, policies and governance for this unmanned technology (and all autonomous

systems) that will be so fully integrated into the waterways, economy and warfare in our world will slow the adoption of UUVs into everyday marine life. This slowness of adoption does not appear to be affecting the innovation, research and development and employment of the technology at the rudimentary level.

Questions

1. What is the difference between the navigation requirements for a manned submarine and a UUV?
2. What mission are UUVs best suited for in lieu of a manned counterpart?
3. Does the UUV size and composition matter? Why or why not?
4. Describe examples of how a UUV could be used to protect a port area?
5. Are optionally piloted submarines safer than deploying UUVs on their own?

References

Ana Rita Silva, G. &. (2019). Simultaneous Underwater Navigation and Mapping. *U.Porto Journal of Engineering*, pp. 5(2), 1-9. doi:10.24840/2183-6493_005.002_0001.

Analysis: Cyber in the Undersea. (2020). Retrieved from www.strikepod.com: https://www.strikepod.com/cuber-implications-for-microsubmarines/

Blain, L. (2019). *DSG's supercavitating underwater bullets annihilate ballistics tests.* Retrieved from newatlas.com/: https://newatlas.com/military/dsg-cavx-supercavitating-underwater-bullets/

Board, N. S. (2005). AUTONOMOUS VEHICLES IN SUPPORT OF NAVAL OPERATIONS. National Academies Press.

Cancilliere, F. M. (1994, September 13). Advanced UUV technology. *Paper presented at the Proceedings of* OCEANS'94. (pp. (1994, 13-16 Sept. 1994)). OCEANS'94.

Discovery of Sound in the Sea. (2020, August 1). Retrieved from

dosits.org/science/: https://dosits.org/science/sounds-in-the-sea/how-do-people-and-animals-use-sound-in-the-sea/sonar/#:~:text=In%20active%20sonar%2C%20the%20system,one%20is%20trying%20to%20locate.&text=When%20a%20sound%2

Frandrup, C. E. (2019). *The US Navy Needs Offensive Undersea Drones.* Retrieved from www.defenseone.com: https://www.defenseone.com/ideas/2019/11/us-navy-needs-offensive-undersea-drones/161548/

H, S. (2019). *Large_AUVs_Poster.* Retrieved from www.hisutton.com: http://www.hisutton.com/Large_AUVs_Poster.html

Inertial guidance system. (2020). In Encyclopaedia Britannica: Encyclopaedia Britannica.

Joanne, M. (2019). *Engineering Wonders Submarines and Submersibles.* Vero Beach: Rourke Educational Media.

Keller, J. (2019). Lockheed Martin to capitalize on XLUUV work for future unmanned undersea vehicles. *Military & Aerospace Electronics*, pp. 30(9), 35-37. .

Kumar, M. (2014). *The Ocean GIS Initiative: Taking GIS underwater.* Retrieved from geoawesomeness.com/gis-underwater/: https://geoawesomeness.com/gis-underwater/

Larter, D. B. (2020, July 7). *US Navy to develop drone deployment strategy.* Retrieved from www.defensenews.com/naval: https://www.defensenews.com/naval/2020/07/21/the-us-navy-is-trying-to-get-its-act-together-on-unmanned-systems/

Laser Ring Gyroscope for Inertial Navigation System . (2020). Retrieved from mh-elec.en.alibaba.com/: https://mh-elec.en.alibaba.com/product/62231832543-802666356/Buy_active_motorized_precision_laser_ring_gyroscope_for_inertial_navigation_system.html

Maritime Safety Information. (2020). Retrieved from msi.nga.mil/: https://msi.nga.mil/

Mizokami, K. (2017, August 29). *The Navy Is Working on Underwater Wireless Charging Stations for Robot Subs.* Retrieved from www.popularmechanics.com:

https://www.popularmechanics.com/military/research/news/a27986/the-navy-is-developing-undersea-wireless-charging-stations-for-robot

Mizokami, K. (2019). *Why Russia's Unique Supercavitating Torpedoes Are so Fast.* Retrieved from nationalinterest.org/: https://nationalinterest.org/blog/buzz/why-russias-unique-supercavitating-torpedoes-are-so-fast-101627

Mohammad Ali, D. J. (2019). *Archives of Computational Methods of Engineering*, pp. doi:10.1007/s11831-019-09354-8.

Mumm, D. H. (2019). *Artificial Intelligence and the Human Race…Can They Co-Exist in Your Marketplace?* Boston, MA.: Evanta.

Navigating a Submarine: Time and Navigation-The Untold Story of Getting from Here to There. (2020). Retrieved from timeandnavigation.si.edu/: https://timeandnavigation.si.edu/satellite-navigation/reliable-global-navigation/first-satellite-navigation-system/navigating-a-submarine

Nobahari, H. &. (2017). *Accuracy Analysis of an Integrated Inertial Navigation System in Slow Maneuvers.* Retrieved from onlinelibrary.wiley.com/doi/abs/10.1002/navi.195: https://onlinelibrary.wiley.com/doi/abs/10.1002/navi.195

Ostrowski, Z. S. (2020). Underwater Navigation System Based on Doppler Shift – Measurements and Error Estimations. *Polish Maritime Research*, pp. 27(1), 180-187. doi:10.2478/pomr-2020-0019.

Petillot, Y. R. (2019). Underwater Robots: From Remotely Operated Vehicles to Intervention-Autonomous Underwater Vehicles. *IEEE Robotics & Automation Magazine*, pp. 26(2), 94. .

Salavasidis, G. M. (2019). Terrain-aided navigation for long-endurance and deep-rated autonomous underwater vehicles. *Journal of Field Robotics*, pp. 36(2), 447-474. doi:10.

Vajda, S. &. (1998). Survey of existing and emerging technologies for strategic submarine navigation. *IEEE 1998 Position Location & Navigation Symposium* , pp. (Cat No98CH36153), 309. .

Wang, D. X. (2020). A Novel SINS/DVL Tightly Integrated Navigation Method for Complex Environment. *IEEE Transactions on*

Instrumentation and Measurement, pp. 69(7), 5183-5196. doi:10.1109/TIM.2019.2955187.

Whitman, E. C. (2002). *Unmanned Underwater Vehicles: Beneath the Wave of the Future.* Retrieved from www.public.navy.mil/subfor/: https://www.public.navy.mil/subfor/underseawarfaremagazine/Issues/Archives/issue_15/wave.html

Wilson, J. R. (2019). Unmanned submarines seen as key to dominating the world's oceans: Unmanned underwater vehicles (UUVs) are driving pioneering research in artificial intelligence (AI) underwater communications, autonomous navigation, and unmanned swarms. *Military & Aerospace Electronics*, pp. 30(8), 10-19. .

Wright, D. (2013). *The Ocean GIS Initiative.* Redlands CA: ESRI Incorporated.

5. Chapter 5 Autonomous Maritime Asymmetric Systems [Hood]

Student Learning Objectives

1. Students will be able to understand what asymmetric warfare is and how autonomous underwater systems can be utilized to conduct it.
2. Current applications for autonomous maritime vehicles.
3. Introduction to emerging AUV / UUV technologies and programs that will allow the student to better understand the potential for growing threats.

Asymmetry in Warfare:

War between belligerents whose relative military power differs significantly, or whose strategy or tactics differ significantly. This is typically a war between a standing, professional army and an insurgency or resistance movement militias who often have status of unlawful combatants.

Asymmetric warfare can describe a conflict in which the resources of two belligerents differ in essence and, in the struggle, interact and attempt to exploit each other's characteristic weaknesses. Such struggles often involve strategies and tactics of unconventional warfare, the weaker combatants attempting to use strategy to offset deficiencies in quantity or quality of their forces and equipment. (Thomas, 2010) Such strategies may not necessarily be militarized. (Stepanova, 2016) This is in contrast to *symmetric warfare*, where two powers have comparable military power and resources and rely on tactics that are similar overall, differing only in details and execution. (Thomas, 2010)

This chapter was written to expose the reader to current and envisioned autonomous maritime technologies under development. The likes of which could potentially be used in non-standard or asymmetric methods. With the unspoken goal of possibly subvert or attack US naval forces and the Department of Homeland Security.

Naval Asymmetric Warfare

The US Navy remains arguably the most powerful naval force in the world. With the ability to project global power and reach while influencing US foreign policy by its mere presence, potential state and non-state adversaries continually seek ways to mitigate, undermine or even attack US naval forces that pose a threat to their regional interests. Cost effective autonomous underwater vehicles have been identified by adversarial military and domestic criminal organizations as a means to cheaply subvert US naval capabilities and prowess.

Autonomous Underwater Vehicle

An **autonomous underwater vehicle** (**AUV**) is a robot that travels underwater without requiring input from an operator. AUVs constitute part of a larger group of undersea systems known as unmanned underwater vehicles, a classification that includes non-autonomous remotely operated underwater vehicles (ROVs) – controlled and powered from the surface by an operator/pilot via an umbilical or using remote control. In military applications an AUV is more often referred to as an **unmanned undersea vehicle** (**UUV**). Underwater gliders are a subclass of AUVs.

Until relatively recently, AUVs have been used for a limited number of tasks dictated by the limited technology available. With the development of more advanced processing capabilities and high yield power supplies, AUVs are now being used for more dynamic applications / tasks with current roles and missions constantly evolving.

Applications

Illegal Drug Trafficking:

Submarines that travel autonomously to a destination by means of GPS navigation have been made and are currently in use by illegal drug traffickers. This would limit the need for "go fast" boat operators reducing overall cost, electromagnetic signature and risk to personnel. Recent semi-submersible seizures by the US Coast Guard in the Gulf of Mexico may be prompting criminal organizations to shift to autonomous operations.

Air Crash and Maritime Search Investigations:

Autonomous underwater vehicles, for example AUV ABYSS, have been used to find wreckages of missing airplanes, e.g. Air France Flight 447, and the Bluefin-21 AUV was used in the search for Malaysia Airlines Flight 370. (Mason, 2014) Developing technologies may soon provide a long endurance persistent presence throughout vast swaths of open ocean that could be used to detect downed aircraft or sinking / sunk surface / subsurface vessels.

Military Applications:

The U.S. Navy Unmanned Undersea Vehicle (UUV) Master Plan (NAVY, 2004) identified the following UUV's missions:

- Intelligence, surveillance, and reconnaissance
- Mine countermeasures
- Anti-submarine warfare
- Inspection/identification
- Oceanography
- Communication/navigation network nodes
- Payload delivery
- Information operations
- Time-critical strikes

Recently, The Navy Master Plan divided all known UUVs into four classes (Johns Hopkins APL Technical Digest, 2015):

- Man-portable vehicle class: 25–100 lb displacement; 10–20 hours endurance; launched from small water craft manually (i.e., Mk 18 Mod 1 Swordfish UUV)
- Lightweight vehicle class: up to 500 lb displacement, 20–40 hours endurance; launched from RHIBusing launch-retriever system or by cranes from surface ships (i.e., Mk 18 Mod 2 Kingfish UUV)
- Heavyweight vehicle class: up to 3,000 lb displacement, 40–80 hours endurance, launched from submarines
- Large vehicle class: up to 10 long tons displacement; launched from surface ships and submarines

Underwater Gliders

In addition to the list of standard UUV's, the underwater glider (UG) is a type of autonomous underwater vehicle that uses small changes in its buoyancy to move up and down and uses wings to convert the vertical motion to horizontal, propelling itself forward with very low power consumption. (See Figure 5.1)

In 2004, the US Navy's Office of Naval Research began developing large gliders that were designed to quietly track diesel electric submarines in littoral waters, remaining on station for up to six months. (XRay)

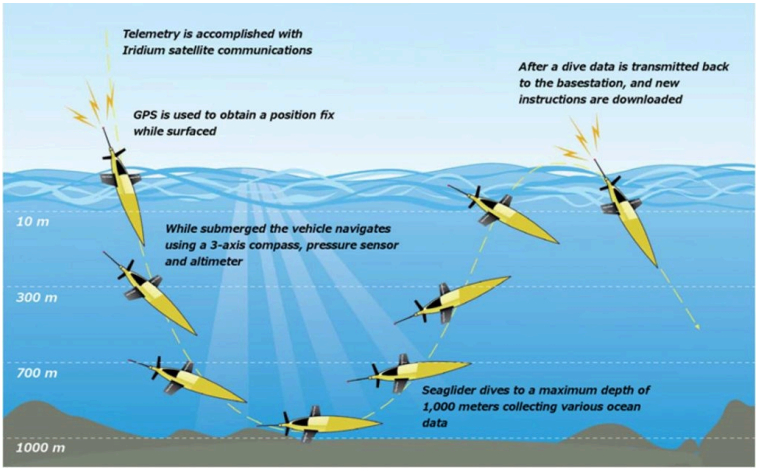


Figure 5.1 UUV US Navy Underwater Glider

Source: (NOAA, 2020)

Gliders are currently being used by NOAA to track oceanic data to help with hurricane forecasting. NOAA hopes the data collected from these gliders will help enhance our understanding of air-sea interaction processes during hurricane force wind events. In 2020 a network of hurricane underwater gliders was implemented to assess the impact hurricane force winds on upper ocean density structure, and assess the impact of ocean profile data from underwater gliders in operational intensity forecasts. (XRay)

Gliders remain a simple way to establish a persistent networks of sensors at low cost that could potentially carry payloads for various mission sets. They could then be used for tracking potential adversarial threats, while presenting multiple dilemmas the enemy would have to respond to at a very low cost compared to manned vessels that only have a fractional durational use. As sea glider technology continues to mature, communication and electromagnetic signature reductions for these suites will have to be taken into consideration in order to maintain a low observable

persistent presence. Figure 5.2 shows how sea gliders can be deployed in formations to create a network of arrayed sensors.

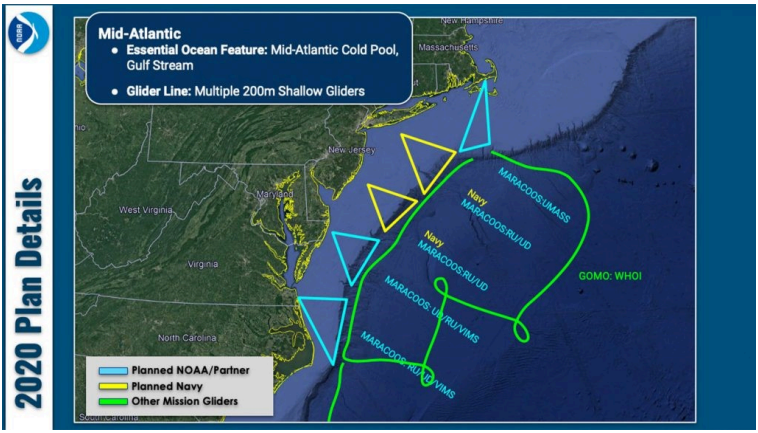


Figure 5.2 Underwater Glider Deployment

Source: (NOAA, 2020)

US Navy's NEMESIS Program

The US Navy is currently working to develop an advanced electronic warfare program that uses drone swarms in the air and sea to cooperatively fool a wide variety of sensors dispersed over a large area. Known as "Netted Emulation of Multi-Element Signature against integrated Sensors" or NEMESIS.

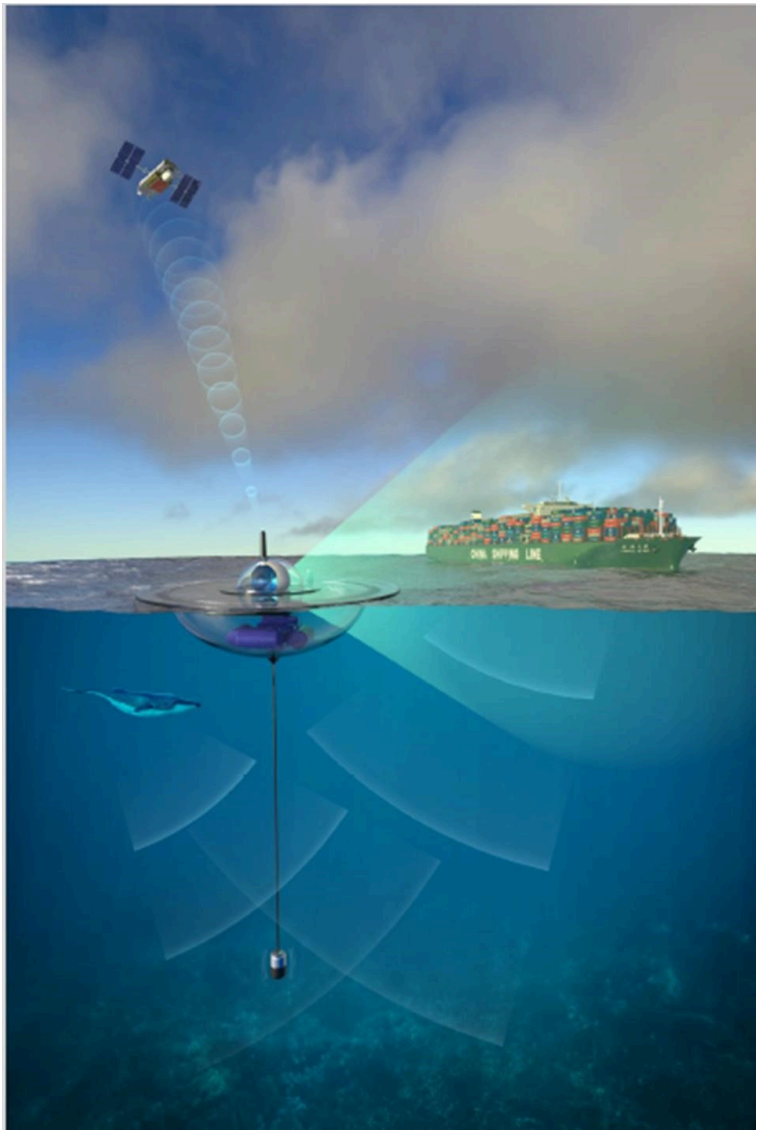
The Navy has spent the last several years developing and integrating multiple types of unmanned vehicles, shipboard and submarine systems, countermeasures, electronic warfare payloads, and communication technologies to give if the ability to give it the ability to project what is, in essence, phantom fleets of aircraft, ships and submarines. These realistic-looking false signatures and decoys have the ability to appear seamlessly across disparate and geographically separated enemy sensors systems located both above and below the ocean's surface. As a result, this networked and cooperative electronic warfare concept brings an unprecedented level

of guileful fidelity to a fight. It's not just about disrupting the enemy's capabilities or confusing them at a command and control level, but also making their sensors tell them the same falsehoods across large swathes of the battle space. (Tingley, 2020)

DARPA's Ocean of Things

The name is a play on the *Internet of Things* and the aim is to achieve persistent maritime situational awareness over large ocean areas. While satellites can provide some information, DARPA project manager John Waterson points out that there are gaps in their coverage – optical satellites cannot see through clouds, radar satellites only have limited coverage, and none of them can say much about what is going on underwater. (Hambling, 2020)

Figure 5.3 Ocean of Things (OoT) Concept – floating sensors



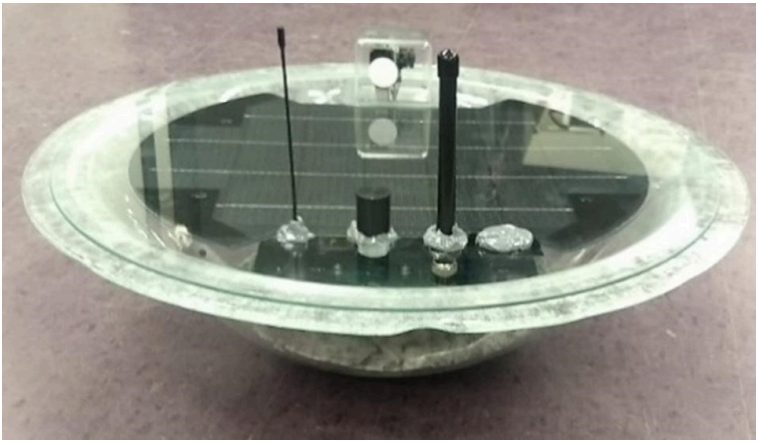
Source: (Hambling, 2020)

Ocean of Things concept of operations, as the float senses activity on and under the water and passes back details via satellite – DARPA image.

Floating sensors, known as floats, can gather far more detailed information, and can remain at sea for months at a time. There is a network of almost 4,000 Argo science floats around the world, gathering data on ocean temperature and salinity. Waterson wants to see much larger arrays of low-cost floats with more sensors, floats which would carry out missions lasting up to a year before scuttling themselves and degrading. The floats are environmentally friendly, avoiding the use of toxic materials. (Hambling, 2020)

The cellphone industry has developed plenty of affordable, miniature sensors, and the OoT is leveraging this technology. The new contract was awarded at the end of July to technology company PARC, whose 18-kilo, solar-powered glass float design won out ahead of two others in the first phase. The floats are sensor nodes which will pass data via satellite to a cloud network for real-time analysis. The OoT will combine data from multiple floats, seeing the whole picture rather than the single pixel gathered by one sensor. (See. Figure 5.4)

Figure 5.4. The eighteen-kilo float houses a variety of sensors and operates for up to a year on solar power



Source: (Hambling, 2020)

A key element of the OoT is its hydrophone, a sensitive underwater microphone or passive sonar which can pick up engines, screws and other sounds from ships and submarines. Floating sonobuoys dropped from aircraft have been used to locate submarines since WWII, but these only operate for a few hours. The OoT hydrophone has to operate for a whole year – and it has to be affordable. In 2019, researchers from Scripps Institution of Oceanography made a prototype high-fidelity hydrophone for the OoT which they estimated could be mass produced for $100-$150. (Hambling, 2020)

DARPA plans to carry out tests with thousand-float arrays in the Southern California Bight and Gulf of Mexico later this year. Initially they will be arranged at about one float per three square kilometers. Waterson believes separation can be increased to one float per twenty square kilometers while maintaining coverage. He is also talking about much bigger arrays in future, of tens of thousands of floats. (Hambling, 2020)

In addition to obvious military and border protection use – no

vessel could slip through the dense field of OoT sensors, on or under the water – the OoT will produce a mass of data of interest to oceanographers, meteorologists and biologists, with plans to share raw data online with researchers. The OoT may be able to monitor marine mammal like whales, watch hurricanes form from the inside, and track changes in ocean temperature. (Hambling, 2020)

In this context, Waterson says that people often mention Flight MH370, the Malaysia Airlines Boeing 777 that disappeared in Southern Indian Ocean in 2014. If there had been an OoT in the area, a plane crash could have been detected and the crash site located. However, DARPA's main interest is likely to be in military applications. (Hambling, 2020)

"The persistent coverage provided by dispersed sensors provides round-the-clock coverage that other sources of data like an MPA [maritime patrol aircraft] or a SAR [synthetic aperture radar] satellite, which cover a given area for a certain amount of time before moving on, cannot," says Dr. Sidharth Kaushal, an expert on sea power at the U.K. defense think tank RUSI. (Hambling, 2020)

Kaushal notes that as well as directly observing vessels and aircraft, the OoT will be able to measure variables like temperature, ocean salinity and ambient underwater noise, which are important for calibrating sonar during anti-submarine operations. The OoT will not be limited to any specific role; the variety of sensors, coupled with powerful data-processing techniques, mean it might be reconfigured to deal with emerging threats. For example, OoT might form a defensive picket to detect, track and locate incoming Russian Poseidon nuclear torpedoes so they could be intercepted. (Hambling, 2020)

"This fits into a wider concept of Mosaic Warfare creating a system the components of which can reform and interact in multiple ways rather than relying on a hierarchical system," says Kaushal. (Hambling, 2020)

In some ways the OoT parallels the network of surveillance platforms China is building in the South China Sea, which are also gathering scientific and military data. However China's Blue Ocean

sensors are tethered in place and appear to be mainly for radar and optical observation; there are believed to be hydrophone arrays on the sea bed. By contrast the OoT is much smaller and expendable, and could be deployed anywhere that the U.S. requires detailed, persistent observation of maritime activity, thousands of floating eyes to see over, on and under the sea. (Hambling, 2020)

Conclusions

Autonomous underwater vehicle applications continue to grow and expand as fast as emerging maritime technology allows. While the United States maintains naval supremacy throughout the world and the Department of Homeland Security continues to grow and develop, potential adversarial and criminal entities will seek ways to subvert and penetrate and exploit known and unknown weaknesses. This could be done by overt air and sea attacks against maritime vessels and infrastructure or most likely by low profile, low signature and low cost autonomous systems. These autonomous systems will be used to track surface and subsurface vessels, providing potential adversaries a clear picture of how US naval forces are arrayed. They will also be used to covertly strike by means of delivering small payloads to specific targets while remaining undetected.

As other advancing nations continue to conduct similar research as DARPA, NOAA and the Office of Naval Research, the growth of autonomous under water vehicles will remain constant for the foreseeable future. The next new wave of technological advances will be centered on how to effectively counter these AUV / UUV systems before they can be effectively employed against US naval and maritime assets across the world's oceans.

Questions

1. Give an example of asymmetric warfare from recent world events that would have benefitted from UUV technologies that

DARPA and the US Navy are developing.

2. Which application in the text has the most potential for successful employment against US interests?

3. What countermeasures would be indicated for Item 2?

References

Hambling, D. (2020, August 25). DARPA Progress With "Ocean of Things" All-Seeing Eye on the High Seas.

Johns Hopkins APL Technical Digest. (2015). *John Hopkins*, Volume 32, Number 5 (2014)" .

Mason, M. (2014, April 15). Robot Sub Deployed in Search for malaysian Plane. *Associated Press*.

NAVY, U. (2004). The Navy Unmanned Vehicle (UUV) . *Master Plan*.

NOAA. (2020, August 18). *Hurricane Gliders*. Retrieved from www.aoml.noaa.gov/: https://www.aoml.noaa.gov/hurricane-glider-project/

Stepanova, E. (2016). 2008 Terrorism in Asymmetrical Conflict. *SIPRI Report 23*.

Thomas, R. (2010). Relearning Counterinsurgency Warfare. *Parameters*, PDF.

Tingley, B. (2020, August 18). *The Navy's Secretive and Revolutionary Program to Project False Fleets From Drone Swarms*. Retrieved from thedrove.com/: https://thedrove.com/the-war-zone29505/the-navys-secretive-nemesis-electronic-warfare-capability-will-change-naval-combat-forever

XRay, L. (n.d.). Underwater Gliders. *Office of Naval Research*.

6. Chapter 6 UUV Integrated Autonomous Missions & Drone Management [Mumm]

Student Learning Objectives

The student will gain knowledge of the concepts and framework as it relates to the unmanned underwater vehicle (UUV) missions, including military and civilian uses for surveillance and reconnaissance, research, as well as offensive and defensive employment of such technology. The student will be able to:

- Understand the historical nature of underwater missions and why UUVs are becoming more important to the military and industrial arena.
- Discuss the differences in manned versus unmanned underwater vehicle deployment.
- Analyze and differentiate missions that are best suited for UUV missions and which missions might be best served by manned submarines.
- Explore the ever-increasing list of sensors and mission packages available for UUVs, which allow UUV deployment envelopes to expand and occupy more of the underwater marketplace.

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

This chapter explores the differences and similarities of how manned and unmanned underwater vehicle technology is employed for different mission sets and some of the challenges the industry faces as UUVs become the norm, and manned submarines become more focused on specialized missions, as well as tasking and

integrating UUVs into existing manned architecture. UUVs come in all shapes and sizes, starting from about a meter in length going up to what is now known as an "Extra Large Unmanned Undersea Vehicle" (XLUUV). The wide variety of sizes and shapes of UUVs offers mission flexibility in an arena that is at its infancy stage.

The mysteries of the seas fascinate humankind. The vastness of the seas with all of its wonders spawned ancient Greek religion to believe in Poseidon; known as the "king of the seas…lord of the sea-gods, as he dwelt in a golden palace on the sea bed with his queen Amphitrite and son Triton" (Sea Gods, 2017). For centuries sailors prayed to "Amphitrite, goddess who spawned the sea's rich bounty–fish and shellfish–as well as dolphins, seals, and whales" (Sea Gods, 2017). Sailors also prayed to these deities for a safe journey and a bountiful catch. Humankind's desire to learn, conquer, and use the sea for its betterment creates the need for technologies and techniques to allow humans to obtain their goals.

As early as 1578, an "English mathematician and royal navy gunner published a book that described his idea for engineering a submarine" (Joanne, 2019). In 1620 the first working submarine known as the Drebbel was invented by Cornelis Drebbel and was propelled by oars that were under the vehicle. By "1623, Drebbel's watercraft carried 16 passengers under the River Thames in London…staying underwater for about three hours" (Joanne, 2019). Forty years later, the first submarine with an engine was created known as the Diver. This submarine engine used compressed air. The air was forced from a tank into a cylinder, and this air movement pushed a piston that turned the propeller. John Philip Holland improved the design and "engineered a submarine that used battery power…batteries created electricity-powered a motor to turn the propeller" (Joanne, 2019).

Submarine inventors took great risks even with their own lives as they worked to perfect the ability to survive underwater for longer time frames. In 1850 "Wilhelm Bauer built his first submarine… but only narrowly escaped with his life after it sank in 50 feet of water during a demonstration" (Andrews, 2018).Wilhelm Bauer would be

undeterred by this setback as he received financial backing from the Russian government and went on construct the "Sea Devil." The Sea Devil made more than one hundred and thirty successful dives and "boasted several technological breakthroughs including multiple ballast tanks for added buoyancy, a crude airlock and a propeller that was powered by crewmen operating an internal treadmill" (Andrews, 2018).

Early American Submarine Usage

For almost two hundred and fifty years, submarines have been used as a wartime vessel. The first attempt to use submarines as an attack vessel was during the American Revolutionary War; and on "September 6, 1776, an American named Sergeant Lee tried to attack a British ship using the Turtle. Lee drilled a hole in the ship, but he ran out of air before he could attach the mine" (Joanne, 2019). In 1863, a privately funded venture in Mobile, Alabama, using a recycled iron steam boiler ushered in the first successful primitive attack submarine known as the H.L. Hunley. This attack submarine offered new naval tactics to be introduced during the US Civil War. Breaking the stronghold of the Union naval blockades allowed the Confederacy to move supplies and keep the Union naval ships at risk. The Hunley was known as the "peripatetic coffin"—and for good reason. It sank on two occasions during its trial runs, killing a total of 13 crewmen including its namesake, marine engineer Horace Lawson Hunley" (Andrews, 2018).

Commissioned on October 12, 1900, the USS Holland became the first US Navy submarine. Although the USS Holland was never employed in combat, "The ship's armaments consisted of a single torpedo tube and pneumatic cannon known as a "dynamite gun." It was powered by a 4-cylinder gasoline engine for surface travel, but also included a 160-horsepower electric motor to move underwater" (Andrews, 2018).

World War I saw the introduction of the German U-boats, better known as "undersea boats." Built on production lines to allow for economies of scale and training of its crew, the U-boats were

introduced into the German fleet to attack enemy military ships. Later, the U-boats were used to "attack merchant ships and passenger liners. In just one day in September 1914, a German U-boat sank three British ships. Between February and April 1917, U-boats sank more than 500 merchant ships" (Joanne, 2019).

New technologies such as sonar and radar allowed submarines to take an important leap forward in their importance in contributing to military successes. Submarines became a key component to WWII as "Nazi Germany and Imperial Japan were major sea powers during World War II by adding submarines to their surface fleets. That combination remains the key to sea power today" (Wilson, 2019)

Submarines were used in the Gulf War (1990-1991) to launch land-attack missiles, and submarines are currently used in the ongoing War on Terror. The ability to be stealth and persistent allows mission planners flexibility in employment, and UUVs will broaden this flexibility envelope in future years.

Submarines and UUVs continue to illustrate their importance to the world although "it is only in the last thirty years that progress in propulsion; control, hydrodynamics, and sensor technology have enabled the development of more broadly capable vehicles and free the imaginations of naval planner to propose new and innovative operational applications for them" (Whitman, 2002).

The ability to remove the human from a submarine and allow the vehicle to be remotely operated by wire and later fully autonomously is still in a formative stage, as illustrated in Table 1; however, the capability increase is being heavily funded and is moving quickly to the forefront of the UUV arena.

Table 6.1: The Evolution of UUVs and Their Capabilities

Table 1. The evolution of UUVs and their capabilities.

Vehicle	Year	Sensing	Navigation	Communications	Autonomy and Planning	Manipulation
Jason ROV	1988	Side-scan sonar, altimeter, black-and-white camera	LBL, INS, dynamic positioning	Optical-fiber tether	Remotely controlled and preplanned track following	Teleoperated
REMUS AUV	1997	Acoustic Doppler Current Profiler, side-scan sonar, conductivity temperature profiler, light scattering sensor	DVL, INS, LBL	Acoustic modem	Preplanned missions and acoustic commands	No manipulation capabilities
Girona 500 I-AUV	2011	Profiler sonar, side-scan sonar, video camera	DVL, attitude and heading reference system, USBL	Acoustic modem and optional tether	Preplanned missions and autonomous inspection	Autonomous free-floating manipulation

Source: (Petillot, 2019)

In the modern-day US Navy, it has taken nearly three decades of development and experimentation in the unmanned systems arena; however, "unmanned underwater vehicles are close to joining the fleet in meaningful numbers and substantive roles…UUVs are rapidly gathering momentum and critical mass of supporters" (Whitman, 2002).

Submarine and UUV Current Military Missions

The primary roles and missions for the U.S. submarine force are peacetime engagement, surveillance and intelligence, special operations, precision strike, battlegroup operations, and sea denial using naval or port blockades.

Keeping in mind that in the current global security environment, naval forces have an ideal disruptive technology in UUVs that offers "many challenges both in the form of asymmetric threats and confrontations between peers" (Newswire, 2018) while allowing human assets to stay out of harm's way. UUVs will have "initial emphasis on minefield reconnaissance, intelligence collection, trailing, tagging, deception, and attack capabilities are potential future options" (Whitman, 2002). These UUV capabilities will include a range of command and control options including creating

an optionally piloted submarine with the on the fly ability to transition to near-total autonomy or full autonomy.

The US Navy published The Navy Unmanned Undersea Vehicle (UUV) Master Plan in 2004 and then updated the plan in a February 18, 2016, Congressional report "using Sea Power 21 for guidance, nine Sub-Pillar capabilities were identified and prioritized:

1. Intelligence, Surveillance, and Reconnaissance
2. Mine Countermeasures
3. Anti-Submarine Warfare
4. Inspection / Identification
5. Oceanography
6. Communication / Navigation Network Node
7. Payload Delivery
8. Information Operations
9. Time Critical Strike" (*The Navy Unmanned Undersea Vehicle (UUV)* . See Figure 6.1, US Navy UUV Systems Vision.

The UUV Master Plan identifies four basic signature capabilities and provides an outline for the development of the underlying technologies required to implement these signature capabilities for littoral operations. The signature capabilities include:

- Maritime Reconnaissance (MR) – centers on the Intelligence, Surveillance, Reconnaissance (ISR) functions, target designation; launch and coordination of UUVs for battle damage assessment; and intelligence collection.

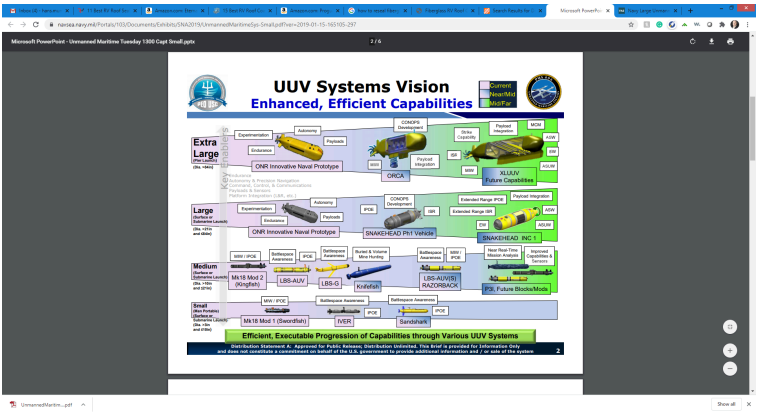
Undersea Search and Survey (USS) – provides the ability to rapidly survey selected areas through the use of networks of small UUVs, performing functions

- such as mine hunting/neutralization, underwater object location and recovery, and hydrographic/bathymetric surveys.
- Communication/Navigation Aid (C/NA) – provides a

communication/navigation relay for other underwater vehicles operating within the immediate area and is expected to serve as a gateway for an autonomous underwater communication/navigation network.

- Submarine Track and Trail (ST&T) – provides a mobile cueing function, but could grow into a fully autonomous system offering multiple levels of engagement (Wenli, 2000).

Figure 6.1: US Navy UUV Systems Vision



Source: (Clark, 2020)

Anti-submarine warfare (ASW) is a difficult mission the Navy must perform, and this is a good reason why the Navy should increase the use of UUVs in the performance of ASW. Although sonars are used to detect submarines; sonars have only a "fraction of the range and precision possible using radars or visual sensors against ships above the water. Unmanned aircraft could deploy sonobuoys or stationary sonar arrays, and unmanned undersea or surface vehicles could tow passive sonar arrays" (Clark, 2020). The integration of UUVs with unmanned surface vehicles would allow the deployment of "low-frequency active sonars like those carried by U.S. undersea

surveillance ships that can detect or drive off submarines from dozens of miles away" (Clark, 2020).

In a March 9, 2020 article by Lyle Goldstein titled "*New UUSs: China's plan to 'attack from the seafloor*," Mr. Goldstein explains, "The robot submarine (and unmanned surface ship) era is now nearly upon us. Chinese naval strategists have stated explicitly that they intend to circumvent their long-recognized weakness in submarine warfare by cultivating undersea AI and by developing highly capable UUVs" (Goldstein, 2020).

In an August 2019 article published by Military & Aerospace Electronics it was disclosed that

In 2018, China announced it was working on an AI-run underwater base, equipped with autonomous submarines to extend its reach. According to published reports, the submarines would deploy for investigation and scientific surveillance missions, then return to the unmanned base to download data and recharge. The base itself, located on the ocean floor as deep as 36,000 feet, also would conduct research on the immediate area, process and fuse all collected data, and transmit the results to a surface ship or land station (Wilson, 2019).

The Chinese government is also conducting an interesting counter tactic to UUVs as "the secretive world of naval underwater surveys rarely breaks the surface" (Sutton, 2020). The Chinese government rewards its fishing industry when vessels are able to capture (or report on) foreign UUVs operating near its coast (international waters). "China has been holding the annual awards ceremonies since 2016. This year 11 (2020), fishermen were rewarded for handing over unidentified underwater vehicles which they had found" (Sutton, 2020).

Submarine and UUV Civilian/Academic Missions

The academic and environmental research communities are steadily increasing their use of UUVs as "interest in using UUVs in private industry is growing simultaneously, and internationally,

at least half-dozen firms have begun to commercialize UUV technology developed in university and military laboratories" (Whitman, 2002). Although oceans cover most of our planet, humankind's knowledge of its mysteries appears to be small in scale as "only a fraction of these vast waters has been explored, and much of the underwater world is little understood" (Loria, 2016). The Aquarius Reef Base is currently the only permanent underwater research laboratory in the world. It is operated by Florida International University in cooperation with NASA, the US Navy, and other research facilities around the world.

Poised for rapid growth, the list of commercial uses of UUVs continues to increase. Some of these commercial and civilian missions for UUVs include underwater tourism, logistical movement of goods, infrastructure monitoring of bridges, oil pipelines, underwater sea cables, undersea mining, and bottom mapping. Additional missions are being explored, such as law enforcement applications, long term monitoring of environmental issues, and sea traffic management in shipping lanes.

As Mr. Stockton Rush explained in an April 17, 2017, Popular Science Magazine article titled "*Deep Sea Tourism Could Become a Thing*", Humankind has explored only about five percent of the ocean, and the federal government isn't doing much to improve that… There's a huge demand for travel that's different," he says. "People want to do something meaningful" (Fecht, 2017).

UUV technology, along with most submarine technology is commercially available and sometimes can be used in unintended applications such as human trafficking or illegal drug smuggling. In November 2019, Spanish authorities captured a drug-smuggling submarine and indicated that "This new attempt to use the narco submarine to bring drugs into Europe in the first place is a much more ambitious undertaking and appears to have largely succeeded on a general technical level" (Trevithick, 2019). In 2010 a drug smuggler was found in Africa building a $20 million submarine to smuggle illegal drugs to the United States. As UUV technology becomes more reliable and affordable, illegal uses are sure to

increase as illustrated by international drug smugglers "it is a clear indication that the use of narco subs in those activities may be an increasingly viable tactic" (Trevithick, 2019).

UUV Markets

The majority of the Earth's surface is covered by water, and approximately "40% of the population living near coastlines, with many energy resources found in the sea and with shipping being the arteries of global commerce" (Newswire, 2018). the potential for UUV manufacturing, parts, service, research and development, and future uses is almost limitless.

Although the larger markets for UUVs is clearly the defense sector, the private sector use will drive profitability of the manufacturing and services support channels. Several mission enhancements will boost these markets "in the fields of autonomy, batteries and power management, underwater telecommunications, underwater charging, sensors, and most importantly in Artificial Intelligence" (Newswire, 2018). The UUV markets are poised for rapid expansion and growth. In 2018, the international market value was estimated to be worth US $9.4 billion. This estimate was based on growing requirements, availability, manufacturing and other industrial indicators (Newswire, 2018).

Senior officials have a stated goal of pursuing a 355-plus-ship fleet of manned vessels, but unmanned systems are "probably the future of the Navy," according to Robert Levinson, a senior defense analyst at Bloomberg Government, during a recent webinar.

It is estimated that about $7.9 billion in the future year's defense program would support drones…An additional $2.2 billion would be allocated toward unmanned surface vessels, or USVs, and $1.9 billion for unmanned underwater vessels, or UUVs. Navy plans call for spending $941 million on USVs and UUVs in 2021 alone, a 129 percent increase over 2019 spending allocations (Harper, 2020).

Unmanned vessels are generally expected to be less expensive to procure, operate, and maintain than manned platforms, which

make them attractive as the sea service invests in new capabilities (Harper, 2020).

The world's economy and its' ability to fund research and development to expand markets and encourage innovations such as UUV underwater tourism, UUV transportation of goods and passengers, and undersea UUV bases will have a deciding impact on the speed and overall success of the UUV industry. This global UUV market is heavily influenced by political turmoil as the importance of the seas cannot be understated. The South China Sea is a good example where "Amid the growing push for decoupling and economic distancing, the changing relationship between China and the rest of the world will influence competition and opportunities in the Unmanned Underwater Vehicles (UUV) market" (Research, 2020).

Teaming UUV with Manned Equipment

As UUVs become more capable and societies continue to seek "bloodless wars," the militaries of the world will work to integrate "unmanned underwater vehicles (UUVs) as adjuncts to conventional manned platforms in many of the submarine missions that arise in expeditionary warfare" (Whitman, 2002). This transition will start slowly with simple minefield reconnaissance, intelligence collection, and deception mission; however, as confidence in the UUV rises, "attack capabilities are potential future options, with command modalities that range from simple remote control to near-total autonomy" (Whitman, 2002).

Optionally piloted UUVs will allow the expansion of manned and unmanned teaming and will bring it into the normative technologies for military and civilian missions alike. This teaming arrangement will only work if the manned operator can understand and trust what the unmanned systems actions are or will be during the missions. Pre-planned missions will be the start of this relationship, however as AI is introduced and the need for mission deviation and flexibility is required, pre-planned mission execution will give

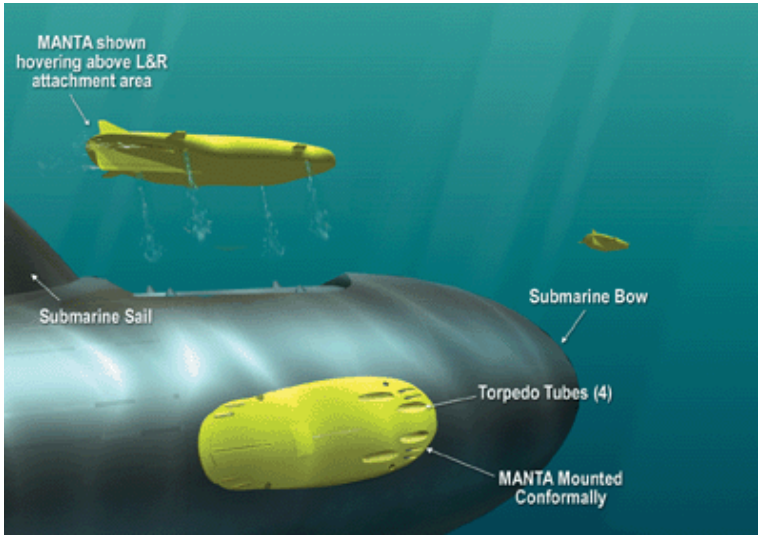
way to AI goal seeking with extended mission capabilities. These extended capabilities and teaming opportunities are being explored as a “detection method for submarine oil pipeline leakage under complex sea conditions by UUVs… the usual practice is to check whether there is oil spill on the sea surface by chartering ships to patrol the line regularly or in the event of leakage accidents” (Zhao, 2019).

Navy special forces conduct missions that require shallow-water reconnaissance in support of amphibious landings and other intelligence-gathering activities. The Navy is looking to pair manned and unmanned systems for this type of an operation, and “small UUV denoted the Semi-Autonomous Hydrographic Reconnaissance Vehicle (SAHRV) has been identified as a leading solution” (Whitman, 2002).

The Naval Undersea Warfare Center is working on concepts that would allow teaming to occur in a seamless way including have “several very large, flatfish-shaped UUVs mated externally to a “mother” submarine could provide a powerful and flexible adjunct to the combat power of their host in off-board operations” (Whitman, 2002) as seen here in Figures 6.2 and 6.3.

Figures 6.2 and 6.3 demonstrate the Notional MANTA concept developed by the Naval Undersea Warfare Center that MANTA vehicles could carry significant payloads of sensors and heavyweight weapons (Whitman, 2002).

Figure 6.2: Notional Manta Concept



Source: (Whitman, 2002)

Figure 6.3: Notional Manta Layout Capabilities

Sources: (Whitman, 2002)

AI and its Influence in the Future of the Integrated Architecture of UUVs

Advances in sensor systems, hull materials, propulsion technologies, and data science will drive the UUV missions to places that have not even been considered at the moment. These technologies will include all the subsystem level technology developments allow for the increase in "survivability and adaptive control of vehicles in complex/dynamic/tactical environments; reduce communication and human supervision requirements; enable cooperative, multi-vehicle operations with navigation aids and communication relays; and provide increased levels of situational awareness" (Wenli, 2000).Specific areas of interest in autonomy include:

- Planning and control architectures
- Path planning (including obstacle and dynamic threat avoidance, adaptive route planning)
- Behavior development
- Mission planning/re-planning
- Multiple vehicle behavior and control
- Multiple vehicle imaging, localization, and data fusion
- On-board mapping of environmental variability, identified objects and moving contacts
- Effective man-machine interface with a limited communication capability.

(Wenli, 2000)

The traditional navigation pattern is depicted in Figure 6.4, however, this scheme is limited, and it is being improved upon through the use of a communication bridge which "allows vehicles to send information from a distant operating area back to a remote operator" (Lockheed Martin, 2017) as seen in Figure 6.5.

Figure 6.4: The scheme of a navigation, guidance, and control architecture for a UUV

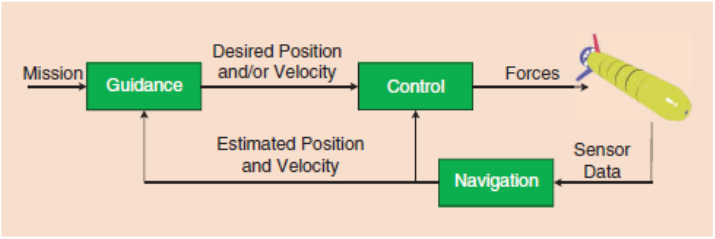
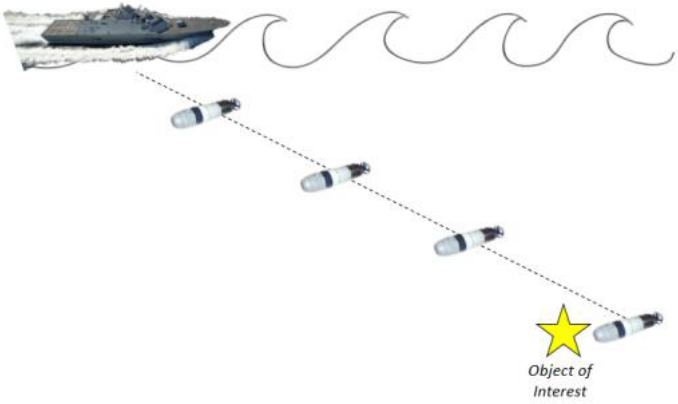


Figure 3. The scheme of a navigation, guidance, and control architecture for a UUV.

Source: (Petillot et al., 2019)

Figure 6.5: Depiction of an Undersea Communication Bridge



Source: (Lockheed Martin, 2017)

Figure 6.5 displays the ability for UUVs to autonomously create a communication bridge in order to relay data back to the host ship (*Unmanned Underwater Vehicle Collaborative Missions A Decentralized Approach to Operating UUV Teams*, 2017).

The underwater environment is not conducive to real-time command and control, and this communication limitation makes some form of AI use mandatory. UUVs are driving pioneering research in artificial intelligence, unmanned swarming technology, navigation, and underwater communications. The U.S. Navy is seeking additional AI capabilities, especially undersea:

"As the current submarine force trusts mechanical and electrical technology to execute the mission, the future force will need to trust AI to extract and exploit actionable patterns among an ocean of data," the session says. "The advent of big data and deep learning technology has rendered signal detection and classification an

increasingly automated process. Furthermore, advances in autonomous navigation have enabled unmanned platforms to operate alone or in swarms (Wilson, 2019).

Extending trust to AI systems is one of the goals of the DARPA's Explainable Question Answering System (EQUAS) Project. The EQUAS Project will show users which data mattered most in AI decision-making, and it was created "to build trust, we have to give the user enough information about how the recommendation was made, so they feel comfortable acting on the system's recommendation" (Wilson, 2019). The idea is that "We know why humans may mess up a decision; there's no intuitive way to know when machines are wrong," says Bill Ferguson, lead scientist at Raytheon BBN Technologies" (Wilson, 2019).

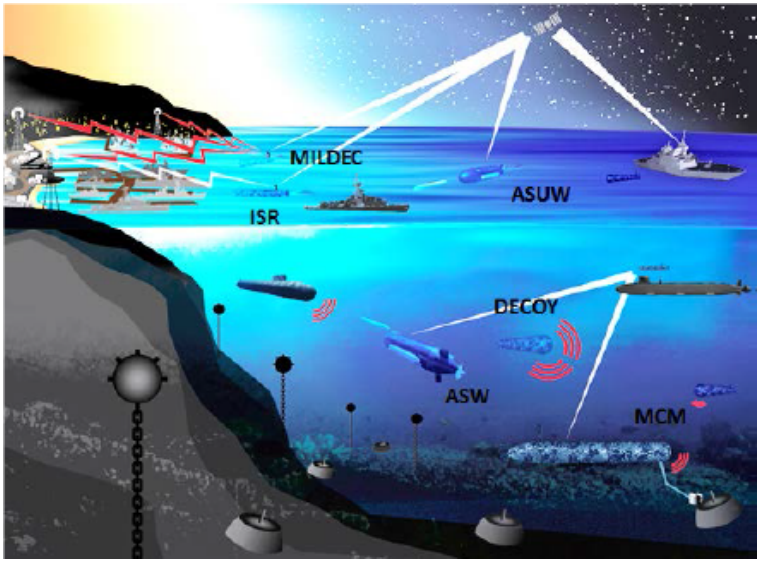
DARPA is also working on the "Ocean of Things" Project that will analyze information from thousands of float sensors in the ocean. This project is targeting towards "affordable ocean sensing at large scales and high resolution, the project's analytics portion seeks to provide detailed understanding of the ocean environment to protect natural resources and enable the military to operate more effectively on the high seas" (Keller, 2020). This information can then be used to train UUV AI systems and allow for as close to real-time updates as technically available in the oceanic environment. Continuous information updates from the Ocean of Things Project can move the UUV arena towards full autonomy with the ability of on the fly mission deviations and re-tasking of the UUVs as required as "only speed, endurance, and the adequacy of onboard autonomous control and decision-making will limit what UUVs can do" (Whitman, 2002). The Ocean of Things can build capabilities that can become key to UUVs "because today's naval and commercial ships typically can use only their onboard sensors for situational awareness" (Keller, 2020).

The future missions of UUVs is discussed at length at the U.S. Post Naval Graduate School and it was the subject of a 2013 paper titled "2024 *Unmanned Undersea Warfare Concept*". Coupling AI into this concept would allow UUVs to "remain one of the top priorities

of the Chief of Naval Operations, as UUVs serve as effective force multipliers, while greatly reducing

risk, in critical missions in A2AD environments" (Blandin, 2013) as illustrated in Figure 6.6.

Figure 6.6: 2024 UUV Concept of Operations



Source: (Blandin, 2013)

Figure 6.6 illustrates what undersea warfare might look like in FY2024 and how forward operating UUVs would autonomously function in hostile A2AD environments with multi-layered enemy defenses including submarines, aircraft, ASCMs, ASBMs, and mines. (Blandin, 2013).

The scalability of future missions and full integration of UUVs into an operating architecture will require a several technologies to mature at once and work in concert with each other for the mutual success of all involved systems. AI is the component that

will sew all of these technologies together and allow UUVs to reach their full potential in the shortest amount of time. The security of these systems, along with the laws, policies, and worldwide agreed-upon governance of UUVs, is work that has barely even begun to be tackled, and a much more concerted effort is required to move forward on these fronts.

Personnel/Human Implications

The human aspect of UUVs should not be overlooked as the training and re-training of personnel will affect the overall readiness of seaborne operations. While this chapter is not focused on this issue, it is an issue that must be factored into the current and future mission planning cycles and technology refresh cycles for seaborne operations, including UUVs. The psychological effects of turning over a traditional manned mission to a robot and allowing that robot at times to operate with more autonomy than allowed by manned systems can create distrust and resentment within the workforce. A March 30, 2020, Congressional Research Service report offered the following:

Another oversight issue for Congress concerns the potential personnel implications of incorporating a significant number of large UVs into the Navy's fleet architecture. Potential questions for Congress include the following:

- What implications might these large UVs have for the required skills, training, and career paths of Navy personnel?
- Within the Navy, what will be the relationship between personnel who crew manned ships and those who operate these large UVs? (O'Rourke, 2020)

Additional thought must be given to issues such as liability boundaries, acceptable losses of UUVs when the traditional calculation is acceptable human losses. Environmental, economic, and economic disparity must be considered in the personnel/human implication of UUV missions and mission expansion.

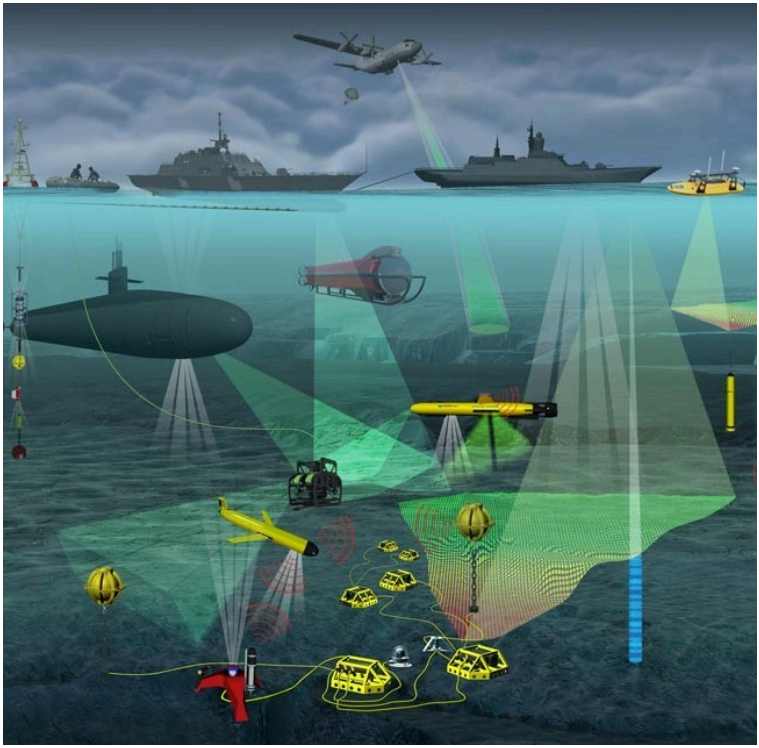
Conclusions

The UUV arena is still very much in its infancy stages. The ability to transverse over, on top of, and under the vastness of the oceans offers humankind learning opportunities that are boundless. As the strategic importance of the world's oceans continues to grow, so will the desire to understand, control, and harness this importance.

The military aspects of UUVs are driven by the ability to use the technology to carry out dull, dirty, and dangerous missions without putting human operators in danger. The missions assigned to UUV will grow exponentially as trust in the systems becomes as commonplace as using a smartphone.

The advent of UUV underwater basing operations and the use of AI in UUVs will usher in a new era in manned/unmanned and optionally piloted submarines missions and uses for military, commercial and academic research. The ability to team with these systems with other manned platforms at sea as well as air and land assets are already accounted for in future integration architectures. As UUVs and all unmanned systems become trusted agents, their utility, as seen in Figure 6.7, is almost limitless; the issue will become one of laws, regulations, policies, and how different countries deploy such technology against each other.

Figure 6.7: Teledyne Technologies portfolio of undersea products, capabilities, and systems



Source: (Teledyne, 2018)

UUV missions are only beginning to be discovered, the advent of underwater tourism, commercial shipping, commercial transportation, and the academic support of UUVs all will keep pace if not rival the missions assigned to UUVs by the world's militaries.

Questions

1. List four advantages and disadvantages of using an autonomous UUV and a manned submarine.
2. What are some of the integration challenges facing UUVs as they integrate into the world's military arena?
3. For surveillance and reconnaissance, does the UUV size and

composition matter? Why or why not?

4. How would you position multiple sensors to surveil a given area with a UUV?
5. Would you consider a UUV a military instrument or a civilian research tool?

References

Andrews, E. (2018). *9 Groundbreaking Early Submarines.* Retrieved from /www.history.com/: https://www.history.com/news/9-groundbreaking-early-submarines

Blandin, M. B. (2013). *2024 Unmanned undersea warfare concept – Naval Postgraduate School.* Retrieved from calhoun.nps.edu/handle/10945/34733.: https://calhoun.nps.edu/handle/10945/34733.

Clark, B. (2020). *US Navy Should Turn to Unmanned Systems to Track and Destroy Submarines.* Retrieved from Defense News. .

Fecht, S. (2017). *Deep sea tourism could become a thing soon.* Retrieved from Popular Science.

Goldstein, L. (2020). *New UUVs: China's Plan to 'Attack from the Sea Floor'.* Retrieved from The National Interest.

Harper, J. (2020). *Navy Wants $12 Billion for Unmanned Platforms.* Retrieved from National Defense. .

Joanne, M. (2019). *Engineering Wonders Submarines and Submersibles.* Retrieved from Vero Beach: Rourke Educational Media.

Keller, J. (2020). *Analyzing data from thousands of floating sensors is goal in second phase of DARPA Ocean of Things project.* Retrieved from Military & Aerospace Electronics. .

Lockheed Martin. (2017). *Unmanned Underwater Vehicle Collaborative Missions A Decentralized Approach to Operating UUV Teams.* Retrieved from lockheedmartin.com: https://lockheedmartin.com/content/dam/lockheed-martin/eo/documents/webt/Unmanned-Underwater-Vehicle-Collaborative-Missions.pdf

Loria, K. (2016). *What it's like inside the only permanent undersea research lab in the world.* Retrieved from Business Insider.

Navy, U. (2004). *The Navy Unmanned Undersea Vehicle (UUV) Master Plan- Washington DC: Department of the Navy.* Retrieved from www.navy.mil/navydata/technology/uuvmp: https://www.navy.mil/navydata/technology/uuvmp.pdf.

Newswire, P. R. (2018). *Market Forecast provides a detailed analysis of the military Unmanned Underwater Vehicles (UUV) market in the years 2018 through to 2025. In UUV-Military.* Retrieved from In UUV-Military: Y.

O'Rourke, R. (2020). *Navy Large Unmanned Surface and Undersea Vehicles: Background and Issues for Congress.* Retrieved from fas.org/sgp/crs/weapons/R45757: https://fas.org/sgp/crs/weapons/R45757.pdf.

Petillot, Y. R. (2019). Underwater Robots: From Remotely Operated Vehicles to Intervention-Autonomous Underwater Vehicles. IEEE Robotics & Automation Magazine, 26(2), 94. *IEEE Robotics & Automation Magazine*, pp. 26(2), 94. Retrieved from Petillot, Y. R., Antonelli, G., Casalino, G., & Ferreira, F. (2019). Underwater Robots: From Remotely Operated Vehicles to Intervention-Autonomous Underwater Vehicles. IEEE Robotics & Automation Magazine, 26(2), 94. : Petillot, Y. R., Antonelli, G., Casalino, G., & Ferreira, F. (2019). Underwater Robots: From Remotely Operated Vehicles to Intervention-Autonomous Underwater Vehicles. IEEE Robotics & Automation Magazine, 26(2), 94.

Research, &. M. (2020). *Unmanned Underwater Vehicles (UUV) Market Outlook to 2027 Including the Impact of COVID-19 on the Industry* . Retrieved from ResearchAndMarkets.com. In.

Sea Gods. (2017). Retrieved from www.theoi.com/greek-mythology/sea-gods.html: https://www.theoi.com/greek-mythology/sea-gods.html

Sutton, H. (2020). *China Discovers Underwater Spy Drones In Its Waters.* Retrieved from www.forbes.com: https://www.forbes.com/sites/hisutton/2020/01/15/china-discovers-underwater-spy-drones-in-its-waters/#34a3453c6990

Teledyne. (2018). *Teledyne Brown Engineering Awarded Next Generation UUV Contract Vehicle*. Retrieved from tbe.com/news_and_events/press_release_view/teledyne-brown-engineering-awarded-next-generation-uuv-contract-vehicle: https://tbe.com/news_and_events/press_release_view/teledyne-brown-engineering-awarded-next-generation-uuv-contract-vehicle

Trevithick, J. (2019). *The First Narco Submarine Ever Seized Off A European Coast Is A Monster*. Retrieved from www.thedrive.com/the-war-zone/: https://www.thedrive.com/the-war-zone/31248/the-first-narco-submarine-ever-seized-off-a-european-coast-is-a-monster

Wenli, R. L. (2000). *Low Cost UUV's for Military Applications: Is the Technology Ready*? Retrieved from Washington DC: Defense Technical Information Center: https://apps.dtic.mil/sti/citations/ADA422138.

Whitman, E. C. (2002). *Unmanned Underwater Vehicles: Beneath the Wave of the Future*. Retrieved from www.public.navy.mil/subfor/underseawarfaremagazine/Issues/Archives/issue_15/: https://www.public.navy.mil/subfor/underseawarfaremagazine/Issues/Archives/issue_15/wave.html

Wilson, J. R. (2019). Unmanned submarines seen as key to dominating the world's oceans: Unmanned underwater vehicles (UUVs) are driving pioneering research in artificial intelligence (AI) underwater communications, autonomous navigation, and unmanned swarms. *Military & Aerospace Electronics*, pp. 30(8), 10-19. . Retrieved from Military & Aerospace Electronics, 30(8), 10-19. .

Zhao, H. &. (2019). Detection Method for Submarine Oil Pipeline Leakage under Complex Sea Conditions by Unmanned Underwater Vehicle. *Journal of Coastal Research*, 97, 122-130. doi:10.2112/SI97-017.1.

7. Chapter 7 Principles of Naval Architecture Applied to UUVs [Jackson]

Student Learning Objectives

The student will understand the concepts of applying naval architectural principles to the design of unmanned underwater vehicles (UUVs).

The student will be able to:

- Gain an understanding of the design processes associated with UUVs and the role of the naval architect.
- Be aware of the application of naval architectural principles to the dynamics and control of UUVs.
- Examine the need for functional design tools to design UUVs.

Introduction

Unmanned underwater vehicles (UUVs) are categorized as two types of drone (Button, 2009). The first is the autonomous underwater vehicle (AUV) and the second is the remotely operated underwater vehicle (ROUV) (Department of the Navy, 2004). Both types serve different purposes but are designed using the same naval architectural principles (Pengelly, 1956). Multiple navies are using these types of vehicles and include the United States of America (US), United Kingdom of Great Britain and Northern Ireland (UK), France, Russia, and China. Figure 7.1 shows a battlespace preparation autonomous underwater vehicle (BPAUV) used by the US Navy and manufactured by Bluefin Robotics Corporation. The propeller is protected by a nozzle casing and two appendages are seen in top of the craft, one being the bridge fin.

Figure 7. 1. Battlespace Preparation Autonomous Underwater Vehicle (BPAUV) in use during a US Navy exercise.

Source: Courtesy of Bluefin Robotics Corporation (Copyright belongs to Bluefin and used with permission **(**https://commons.wikimedia.org/wiki/File:BPAUV-MP_from_HSV-.jpg**).**

Military applications of UUVs include collecting information, timed strikes, oceanography, payload delivery, mine hunting, network navigation modes, surveillance, anti-submarine operations, reconnaissance, inspection, intelligence gathering, communications enhancement and identification of foreign objects (Department of Defense, 2011) (Department of Defense, 2012). Figure 7.2 shows the Pluto Plus AUV used for mine identification and destruction by the Norwegian Navy.

Figure 7.2. Pluto Plus **AUV for underwater mine identification and destruction used by the Norwegian mine hunter, KNM Hinnøy.** CC BY-SA 3.0**.**

Source: Created by KEN (https://commons.wikimedia.org/wiki/File:MiniU.jpg**)**

They are also used for civilian applications such as oil and gas exploration (mapping the sea floor), research vehicles to monitor movements of fish and inspect fauna such as reefs, drug trafficking, air crash investigations, oceanography and many more uses. UUVs are equipped with sensors such as sonars, thermistors, conductivity probes and magnetometers. Biological sensors include chlorophyll sensors, turbidity sensors and sensors that measure acidity, PH, and the magnitude of dissolved oxygen.

Typically, UUVs lose their GPS signal quickly due to the attenuation of radio waves in water, so they rely on dead reckoning to navigate in water. Acoustic underwater position systems are

based on long baseline navigation techniques that can be connected to GPS by allowing the UUV to surface in order to establish its position globally. Owing to the need for surfacing, UUVs are equipped with brush or brush-less motors connected to a gearbox that rotates a propeller that is protected by lip seals and a nozzle. Rechargeable batteries are used and are typically lithium-ion or lithium polymer. Larger UUVs are equipped with fuel cells, but the latest trend is to combine different types of electrical power sources to a supercapacitor.

Role of the Naval Architect

The role of the naval architect is complex and becoming quite broad due to the effects of extreme weather and the minimization of using the earth's scarce resources (Rydill, 1994). The naval architect will need to work more closely with natural scientists, such as marine biologists and environmentalists, in order to design vessels that work with nature to minimize the impact on the natural world (Comstock, 1967). The role will continue to work with engineers from other disciplines, project managers and business administrators and we may see the development of new academic programs that blend the principles of naval architecture with business studies that includes the commercial aspects of naval systems such as 'naval systems architecture' or 'marine systems engineering' (Lewis, 1988) (Taylor, 2006). In addition to teaching naval architecture from a systems approach, the development of 'forensic naval architecture' may provide the safety, reliability and regulatory aspects of naval architecture with the information needed to create naval architects whose design function is clearly guided by knowledge gained from failures using incident/accident reports of submarines that provide valuable data that are contained in codes and standards that allows the design of UUVs that are fit-for-purpose. When designing UUVs, the naval architect must pay special attention to hull shape and to the dynamics of control and its effect on hull shape and associated dimensions.

Naval Architectural Design of UUVs

The design of traditional underwater vehicles (submarines) are based on vessel requirements, weight estimates, initial size, weight and buoyancy balance, arrangements, longitudinal balance, vertical balance and stability, speed and power, propeller, propulsion coefficient, equilibrium polygon, and dynamic stability. The design of UUVs are very sensitive to weight and buoyancy and the naval architect must balance the cumulative weights with buoyancy of the hull form. A standardized system is used to describe hull structure, propulsion system, electrical system, command and surveillance, auxiliaries, furnishings, armaments, margins and acquisition, and loads (Hughes, 2010).

The use of software in the design of UUVs is prevalent especially when one considers the interdependency of the various aspects of design. Specialized modules of programs are designed to focus on the hull, resistances, loads, and control aspects of the UUV. The major features of a UUV include the control surface, hull, battery pack, pressure vessel and stiffeners, the battery system, ballasting, controllers, and the payload. Current designs of UUVs have variable hull geometries based on torpedo shapes but some are rectangular shaped that can be hydrodynamically very challenging.

The standard hull envelope for a UUV is axisymmetric having an ellipsoid fore-body, a parallel mid-body and an aft-body shaped like a parabola (Figure 7.3). This is known at the Jackson hull-form and the diameter of the hull envelope (Eq. 7.1):

$$\mathbf{D = L / (L/D)} \qquad (7.1)$$

Where, D is the diameter of the hull envelope and L is the length of the hull. The length of the fore-body, L_{fwd}, is a function of the forward hull section length factor, C_{fwd}, and the diameter of the hull (Eq. 7.2):

$$\mathbf{L_{fwd} = D.C_{fwd} = C_{fwd} . (L/(L/D))} \qquad (7.2)$$

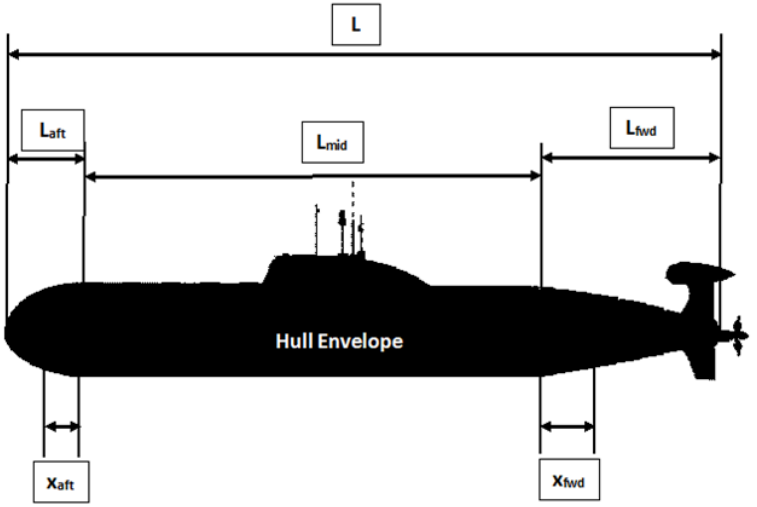


Figure 7.3. Jackson hull-form geometry.

Source: [Adapted from Openclipart Vectors by Pixabay (Public Domain Image)]

Also, the length of the aft-body, L_{aft}, is a function of the hull-section length factor, C_{aft}, and hull diameter, D, (Eq. 7.3):

$$L_{aft} = D.C_{aft} = C_{aft}.(L/(L/D)) \quad (7.3)$$

The parallel mid-body length, L_{mid}, (Eq.7.4)

$$L_{mid}=L-(L_{fwd}\ L_{aft})=L-\{(D.C_{fwd})\ (D.C_{aft})\}=L[1-((C_{fwd}\ C_{aft}))/((L/D))] \quad (7.4)$$

The sum of the forward and aft length factors must be less than the length-to-diameter ratio. If it is equal, then the UUV will have no mid-section. Ellipsoidal forward sections have a radial offset, y_{fwd}, from the centerline of the full length of the UUV body at a local

distance, x_{fwd}, measured from the aft component of the forward body and the forward hull section curvature factor, n_{fwd} (Eq. 7.5)

$$y_{fwd}=D/2\ [1-(x_{fwd}/L_{fwd}\ )\hat{}(n_{fwd}\ )\ ]\hat{}(1/n_{fwd}\ ) \quad (7.5)$$

Paraboloid aft-sections have a radial offset, y_{aft}, from the centerline of the full length of the UUV body at a local distance, y_{fwd}, measured from the aft-component of the forward body and the forward hull section curvature factor, n_{aft} (Eq. 7.6)

$$y_{aft} = D/2\ [1-(x_{aft}/L_{aft}\ )\hat{}(n_{aft}\ )\ ] \quad (7.6)$$

The construction of tables of offsets allows one to calculate principal characteristics in accordance with naval architectural practices such as prismatic coefficient ($C_{prismatic}$), wetted surface area (S), sectional area, and area of the UUV envelope ($V_{effective}$).

The resistance to motion is a function of the basic control surface and its propeller. The calculated resistance allows the naval architect to select the appropriate battery power for the UUV, so it is important to calculate propulsion resistance.

The total ship resistance, R_{total}, is composed of a number of collective resistances that are expressed as non-dimensioned coefficients. The total resistance coefficient, C_{total}, is a function of water density, ρ, the wetted surface area, S, and the velocity of the UUV, (Eq. 7.7)

$$C_{total} = R_{total}/(1/2\ \rho S V\hat{}2\ ) \quad (7.7)$$

When the UUV is operating near to the air-water surface, the resistance is dominated by wave-making resistance and viscous resistance of the fluid. The wave-making resistance is a function of the Froude number (Fr) and viscous resistance is a function of the Reynolds' number (Re). Froude number is a function of velocity, V, gravitational acceleration, g, and length of the hull, L (Eq. 7.8)

$$Fr=V/\sqrt{(g.L)} \quad (7.8)$$

Viscous resistance is given by Re which is a function of velocity, V, length of the hull, L, and the kinematic viscosity of water, υ, (Eq. 7.9)

$$Re=(L.V)/\upsilon$$

(7.9)

The total resistance coefficient, Ctotal, is a function of the Froude number and the Reynolds' number and is approximated as the sum of the coefficients of wave-making and viscous resistances (Eq. 7.10)

$$C_{total} \approx C_{(wave.)}\, Fr + C_{viscous}.Re$$

(7.10)

It is noted that the wave-making resistance is work done by the hull on the surrounding fluid to generate waves. However, there is no resistance of this kind when the UUV is submerged three diameters from the surface of the air-water boundary. Therefore, at lower depths, resistance is purely viscous and is composed of frictional and residual resistances (Eq. 7.11)

$$C_{total} = C_{viscous} = C_{friction}+C_{residual}$$

(7.11)

Frictional resistance in water is a function of Reynolds' number (Eq. 7.12)

$$C_{friction}=0.075/(\log 10.\,(Re)-2)^{\wedge}2$$

(7.12)

Equation 7.12 is based on tank towing models and not full-scale models. It is important to calculate empirical resistances that approximate to a value that is similar to actual conditions of submerged motions. Therefore, the following models provide an estimation of total resistance of UUVs assuming that the hull form is deeply submerged.

Bottaccini Model:

$$C_{total}=[(S.C_{friction})/(A.(L/D)^{\wedge}4\,)].[(L/D)^{\wedge}4+1/2\,(L/D)^{\wedge}3+6]$$

(7.13)

The hull form is deeply submerged in a viscous fluid operating at small angles of motion. The maximum cross-sectional area, A, is function of hull diameter, D, such that (Eq. 7.14)

$$A = (\pi D^{\wedge}2)/4 = \pi/4\,(L/\{L/D\}\,)^{\wedge}2$$

(7.14)

The coefficient of total resistance is also considered to be a function of the coefficient of frictional resistance, the geometry

of the hull and the roughness of the surface of the UUV. This is incorporated in the Gilmer and Johnson model (Eq. 7.15)

Gilmer and Johnson Model:

$$C_{total} = C_{viscous}+C_{roughness} = \{C_{friction}\ [1+D/2L+3(D/L)\hat{}3\ ]\}+C_{roughness} \quad (7.15)$$

The Jackson Curve-Fit Model is a model that is a function of the non-dimensional hull parameter, K (Eq. 7.16), which is based on the length, L, diameter, D, and wetted area, S, of the UUV

$$K = (L/D)-(S/(\pi D\hat{}2\ )) \quad (7.16)$$

And the coefficient of residual resistance is (Eq. 7.17)

Jackson Curve Fit Model:

$$C_{residual}=0.0008/((L/D)-K) \quad (7.17)$$

Another model that accounts for the residual resistance is the Jackson-Hoerner model that is a function of frictional resistance, hull diameter and the length of the aft-body (Eq. 7.18)

Jackson-Hoerner Model:

$$C_{residual}=C_{fwd}\ \{[1.5(D/L_{aft}\ )\hat{}1.5\ ]+[7(D/L_{aft}\ )\hat{}3\ ]\} \quad (7.18)$$

Eq. 7.18 is used when the aft end of the UUV has a significant wake, or a large effect on the form coefficient owing to the separation of flows. The shape of the UUV in terms of its prismatic coefficient is described by the Jackson Parallel-Mid Body model (Eq. 7.19)

Jackson Parallel Mid-Body Model:

$$C_{total}=\{C_{fwd}\ (1+[1.5(D/L_{aft}\ )\hat{}1.5\ ]+[7(D/L_{aft}\ )\hat{}3\ ]+[0.002(Cprismatic-0.6)])\}+C_{aft} \quad (7.19)$$

And to include the effects of the forward and aft hull section curvature factor of the UUV, the Martz model is used to account for the effect of shape of the UUV (Eq. 7.20)

Martz Model:

$$C_{total}=\{C_{fwd}\ (1+(1/2(L/D)\ )+[3(D/L)\hat{}((7-n_{fwd}-(1/(2n_{aft}\ )))\ )\ ])\}+C_{aft} \quad (7.20)$$

Design algorithms incorporate the resistance models to predict the total bare hull resistance of the UUV (Eq. 7.21)

$$R_{(hull\ total)}=0.5\rho SV\hat{}2\ [0.2(C_{total})]$$

(7.21)

The appendages that are attached to the control surfaces produce their own contribution to flow resistance of UUVs. The equation accounts for hull geometry (length and diameter) and the wetted surface area, S, (Eq. 7.22)

$$C_{appendages} = (L.D)/(1000.S_{appendages})$$

(7.22)

The total appendage resistance is given by Equation 7.23

$$R_{appendages}=0.5\rho Sappendages\ V\hat{}2$$

$$C_{appendages}=(\rho LDV\hat{}2)/2000 \quad (7.23)$$

For the total control of the UUV, the lateral surface area must be known (Equation 7.24)

$$A_{(control\ surface)} = 0.028.A_{(control\ surface\ hull)} = 8.A_{(control\ surface\ lateral\ area)} \quad (7.24)$$

The size of all control surfaces is important when specifying the amount of power needed to move the UUV through the fluid and the effective horsepower associated with the UUV is (Eq. 7.25)

$$P_{effective} = V(R_{hull}-R_{appendages})/550 \quad (7.25)$$

For the set operating velocity, the shaft horsepower is that used to provide the primary propulsion in the direction of travel, thus (Eq. 7.26)

$$P_{shaft}=P_{effective}/C_{propulsion}$$

(7.26)

Once the amount of power is known based on the resistances and the shape and size of the UUV, then an estimate of how many batteries and the type of batteries to be used in the UUV can be calculated.

Control and Dynamics of UUVs in Water

The shape of a UUV has significant effects on hydrodynamic signatures and places limitations on the control surfaces relative to the center of gravity. The shape can be changed by adding appendages and the positioning of rudders and spaces for

hydroplanes, which usually affects the dynamics and control of such vehicles when submersed. This also changes the amount of power required to provide thrust (MAN Energy Solutions, 2018). The motion in the six degrees-of-freedom is usually referred to as heave, yaw, sway, roll, surge, and pitch (Figure 7.4).

EQUATIONS OF MOTION FOR UUVs

The equations of motion describe the axes that are aligned to UUVs such as longitudinal, vertical, athwartships that allow the UUV to move in three dimensions in hydrospace, the center of which is set by the center of the geometric center of the UUV, or the center of gravity (Mollard, 2013). The following equations describe the equations of motion in accordance with the convention shown in Figure 7.4.

Surge equation:

$$\mathbf{m\dot{u} = X_P + X_U + X_M + X_A} \qquad (7.27)$$

The surge equation describes the mass of the UUV multiplied by its acceleration being equal to the sum of its forces acting in the longitudinal direction, where X_P is the propulsive thrust force, X_U is the hydrodynamic resistance force, X_M is the drag force due to lateral motion and X_A is the hydrodynamic force due to lateral acceleration.

Horizontal plane equations:

$$\mathbf{m(\dot{v} + rU) = Y_V + Y_{\dot{V}} + Y_R + Y_{Control}} \qquad (7.28)$$

And

$$\mathbf{I_{zz}\dot{r} = N_V + N_R + N_{\dot{R}} + N_{Control}} \qquad (7.29)$$

Equation 7.28 represents the action of mass of the UUV and its sideways acceleration through the horizontal plane of motion and Equation 7.29 describes the product of rotating inertia about the vertical axis through the center of gravity and its angular acceleration in yaw to the sum of horizontal moments of hydrodynamic forces acting on the hull of the UUV.

Vertical plane equations:

$$m(\dot{w} + qU) = Z_W + Z + Z_\theta + Z_{Control} \quad (7.30)$$

And

$$I_{yy}\dot{q} = M_W + M_Q + M_{\dot{\theta}} + M_{Control} \quad (7.31)$$

Equation 7.30 represents the action of rigid mass of the UUV and its acceleration in the vertical plane of motion to the sum of the hydrodynamic forces acting on the hull and Equation 7.31 describes the product of rotating inertia about the horizontal axis through the center of gravity and its angular acceleration in pitch to the sum of vertical moments of hydrodynamic forces acting on the hull of the UUV, supplemented with a restoring moment due to movements away from the horizontal (Rydill, 1994).

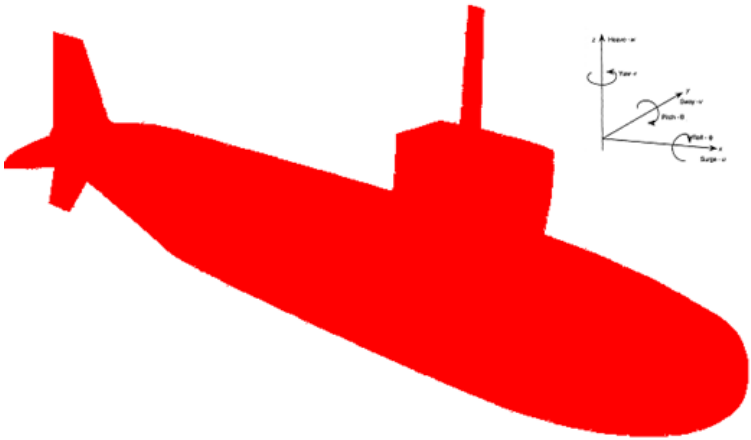


Figure 7.4. Freedom of motion for UUV.

Source: [Adapted from Open Clip art Vectors by Pixabay (Public Domain Image)]

Roll equation:

$$I_{xx}\Phi = K_v + K_R + K_\Phi \quad (7.32)$$

The roll equation (Eq. 7.32) describes the product of rotating inertia about the longitudinal axis and its angular acceleration in roll to the sum of athwartships moments acting on the hull due to hydrodynamic restoring moments owing to movements away from the vertical axis. Control forces are those that account for rigid body forces and those considered control forces owing to motions in vertical, horizontal, and longitudinal directions. Hydrodynamic forces should also be considered as they are considered to be directly proportional to small changes in velocity when UUVs depart from initial straight-line motions. They are known as derivatives owing to those small changes from the straight-line path of motion (Lewis, 1988).

HYDRODYNAMIC DERIVATIVE FORMS

$$Y'_v = Y_V/(0.5\rho UL^2) \quad (7.33)$$

The derivative form is dimensional and as an example, Equation 7.33 is dimensionless owing to its constant characteristic of the UUV's geometry. In its dimensioned form, hydrodynamic derivatives are dependent on the square of the velocity of the UUV.

STABILITY AND CONTROL IN THE HORIZONTAL PLANE

When the derivative approach is applied to the equations of motion and adapted to include control terms appropriate to the rudder's deflection to the angle, δ, the linear equations is sway velocity, v, and yaw rate, r, are defined (Eq. 7.34 and 7.35).

Equations in derivative form:

$$m(\dot{v}+rU)=Y_v v+Y_{\dot{v}} \dot{v}+Y_r r+Y_\delta \delta \quad (7.34)$$

And

$$I_{zz}\dot{r} = N_v v+N_r r+N_{\dot{r}} \dot{r}+N_\delta \delta \quad (7.35)$$

Equations 7.34 and 7.35 show two unknowns, v, and r (sway velocity and yaw rate), as a function of the control term, δ. For

dynamic stability, it is assumed that the UUV is moving in water on a straight path with no control input (δ=0).

Dynamic stability:

$$v\dot{}\,(m-Y_{\dot{v}})=Y_v v + r(Y_r-mU) \quad (7.36)$$

And

$$r\dot{}\,(I_{zz}-N_{\dot{r}}) = N_v v+N_r r \quad (7.37)$$

The equations shown here can be solved using transformations into a single linear equation for either v and r. The general form of equations can be expressed in real or imaginary terms and tend to indicate whether the UUV is stable or unstable along its path of motion. The control effectiveness of the rudder can be understood by analyzing steering motions as function of rudder force (Lewis, 1988).

Steering motions:

$$Y_v v+(Y_r-mU)r+Y_\delta \delta=0 \quad (7.38)$$

And

$$N_v v+N_r r+N_\delta \delta=0 \quad (7.39)$$

And

$$r/\delta = Y_\delta/((Y_r-mU)\,)\,(x_v-x_\delta)/(x_r-x_v\,) \quad (7.40)$$

Here, it is understood that all terms associated with derivatives are omitted and we are left with constant velocity terms. Equations 7.38 and 7.39 can be solved to give a steady state turn, r, as a function of rudder deflection, δ, (Equation 7.40). The equation tells us that the rudder should be placed aft of the body as far as possible in order to gain the best control of the UUV due to the sway of the hydrodynamic forces on the hull (Comstock, 1967).

STABILITY AND CONTROL IN THE VERTICAL PLANE

For vertical control of the UUV at velocity, w, and pitch angle, θ, the rate of change of pitch angle is needed. It is also required to know two sets of control surfaces with two deflection angles of δf on the forward and aft hydroplanes (Eqs. 7.41 – 7.43).

Equations in derivative form:

$$m(\dot{w}+rU) = Z_w w+Z_q q+Z_{\delta f}\delta f+Z\delta a\ \delta_a \quad (7.41)$$

And

$$I_{zz}\dot{q} = M_w w+M_q q+M_\theta \theta+M_{\delta f}\delta_f+M_{\delta a}\ \delta_a \quad (7.42)$$

$$M_\theta = W.(\overline{BG}) \quad (7.43)$$

The hydrostatic restoring moment in Equation 7.42 is associated with the pitch angle that indicates a preferential motion in the vertical plane. The UUV can be considered moving along a straight line with no input from the rudder (δf and δa = 0), which leads us to define dynamic stability.

Dynamic stability:

$$(\dot{w}-qU)=Z_w w+Z_q q \quad (7.44)$$

And

$$I_{yy}\dot{q} = M_w w+ M_{\dot{w}}\dot{q} +W.(\overline{BG}.\theta) \quad (7.45)$$

Equations 7.44 and 7.45 are simplified forms of the equations of motion and have three roots that will be dependent on the speed of the UUV. When the control surfaces are operating in response to rudder motions, Equations 7.46 – 7.50 apply. The combined effects of control forces are shown in Equation 7.46.

Motion control with surfaces operating:

$$Z_\alpha\alpha+Z_{\delta c}\delta_c=0 \quad (7.46)$$

And

$$M_\alpha\alpha+M_\theta\theta+M_{\delta c}\delta_c=0 \quad (7.47)$$

Equation 7.46 allows us to derive the vertical velocity as the function of control surface angles of deflection (Eq. 7.48).

$$\alpha = -(Z_{\delta c}\delta c)/Z_\alpha \quad (7.48)$$

Here (Eq. 7.48), the vertical velocity is related to the control force and the hydrodynamic resistance of the UUV in vertical and horizontal directions. Using the solution from Equation 7.46 to feed

into Equation 7.47, the pitch angle is a function of angles of deflection of the control surfaces (Equation 7.49):

$$\theta = (Z_{\delta c}\, \delta_c\, (x\alpha - xc))/M_\theta \quad (7.49)$$

Where $x_c=(M_{\delta c})/Z_{\delta c}$ and $x_a=M_\alpha/z_\alpha$ (7.50)

Equations shown in 7.50 are the effective locations of control and heave forces, respectively. The equations shown in this section are used to control pitch and plane setting in UUVs and are critical when coupled with the shape of the hull to reduce flow signatures. It is noted that hull form and shape and appendages are critical aspects of control dynamics, so much analysis is performed by the naval architect to perfect the design of UUVs prior to construction (American Bureau of Shipping, 2019).

Structural Integrity

Once the shape, form and control aspect of the UUV is accepted, the structural integrity of the UUV is calculated by understanding the structure of materials and how they can withstand hyperbaric pressures at known depths (American Bureau of Shipping, 2019).

External hydrostatic pressures are calculated for each control surface and materials are selected by understanding the three primary failure modes (Lewis, 1988):

- axisymmetric yielding of the shell between stiffening frames characterized by elastic-plastic collapse (concertina effect);
- shell buckling between stiffening frames characterized by buckling forming inward and outward bulges of the shell; and
- Instability that occurs between bulkheads and frames and results in elastic buckling of the frame-shell of the hull.

Knowledge of materials are required to select the best material for the UUV shell. This means that design factors such as buckling pressure, yielding pressure at the frame, yielding pressure at mid-bay, general instability, frame instability buckling pressure, frame

hoop stress and total frame hoop stress for the structure need to be calculated (Hughes, 2010). The current ABS Rules governing the design of UUVs considers the following structural design factors:

- Stiffener strength;
- Buckling strength;
- Longitudinal frame strength;
- Inner stiffener strength;
- Local stiffener flange buckling strength;
- Local stiffener web buckling strength; and
- Combined stiffener and shell moment of inertia.

Stiffener and web spacings are calculated to avoid the three modes of failure based on the strength properties of the material(s) selected for the UUV shell (American Bureau of Shipping, 2019).

Discussion / Conclusions

The detailed information generated by the naval architect to design the hull shell and its appendages according to its mission in the water is used to allow the architect calculate how much battery power is needed for the UUV (Rydill, 1994). The selection is based on the propulsive and static loads needed to move the UUV and its apparent and real volume. Batteries need to be carried on board, so the size related to their energy density is critical. Typically, lithium-ion batteries are used because they have such a large energy density (~1300 HP.min/ft3), whereas lead-acid batteries are typically not used because of their low energy density (~160 HP.min/ft3). It should be noted that current battery technology severely limits the naval architect who is responsible for the design of UUVs. Advances in the field of fuel cells and associated systems such as supercapacitors are long awaited.

Questions

1. What is a naval architect and how does it affect the design of

UUVs?

2. Describe the shape of a UUV and how its shape can affect how it operates.
3. Explain the differences in the flow resistance models and how they are incorporated into the design procedures for UUVs.

References

American Bureau of Shipping. (2019). *ABS Rules for Building and Classifying Underwater Vehicles, Systems and Hyperbaric Facilities.* Houston, Texas: American Bureau of Shipping.

Button, R. W. (2009). *A Survey of Missions for Unmanned Undersea Vehicles.* Santa Monica, California, USA: RAND Corporation.

Comstock, J. P. (1967). *Principles of Naval Architecture.* New York, USA: Society of Naval Architects and Marine Engineers.

Department of Defense. (2011). *Unmanned Systems Integration Roadmap: 2011 – 2036.* Washington DC, USA: US Government.

Department of Defense. (2012). *Sustaining US Global Leadership: Priorities for the 21st Century Defense.* Washington DC, USA: US Government.

Department of the Navy. (2004). *The Nay Unmanned Undersea Vehicle Master Plan.* Washington DC, USA: US Government.

Hughes, O. F. (2010). *Ship Structural Analysis and Design.* New York, USA: Society of Naval Architects and Marine Engineers.

Lewis, E. V. (1988). *Principles of Naval Architecture: Volumes I, II and III.* New York, USA: Society of Naval Architects and Marine Engineers.

MAN Energy Solutions. (2018). *Basics of Ship Propulsion.* Berlin, Germany: MAN.

Mollard, A. F. (2013). *Ship Resistance and Propulsion.* Cambridge, UK: Cambridge University Press.

Pengelly, E. L. (1956). *Theoretical Naval Architecture.* London: Longmans.

Rydill, R. B. (1994). *Concepts in Submarine Design.* Cambridge, UK: Cambridge University Press.

Taylor, D. A. (2006). *Merchant Ship Naval Architecture.* London, UK: The Institute of Marine Engineering, Science and Technology.

PART III

SECTION 3 UNMANNED VEHICLES FOR GROUND & LAND OPERATIONS & PENETRATION OF ADS

8. Chapter 8: Unmanned Logistics Operating Safely & Efficiently Across Multiple Domains [Lonstein]

Student Learning Objectives:

Increasingly exposed to the reality that automation, artificial intelligence, and unmanned technology, many of us become simultaneously captivated and concerned by the velocity of new products and technologies introduced daily. Students must prepare to function in a world of near-total connectivity. What happens on the ground and in water, above below, requires a homogenous technology ecosystem? The interaction of humans, machines, and the environment will be a critical concept for students to consider in a world where man, machine, and technology operate in concert safely and economically. That interaction will not only require interaction between humans and machines but will also require interaction between humanoids, humans, unmanned technology, and other intelligent technologies operating at different levels. Students will explore how subterranean automation will impact what may happen in space and at each level of our atmosphere.

Once Completed Students Should:

- Understand that automated technology needs to communicate effectively with its primary control systems and other technology, both manned and unmanned, within the same domain.

- Include in their assessment or design of Unmanned Systems, both commercial and military, significant consideration of the interaction of Unmanned technology within a particular stratum of operation and other systems and humans operating at different levels of the physical world, be it underground, on surface waters, underwater, on land in air, space as well as virtual environments.

- Appreciate that the global reach of automated technology will not only require local and national communication and interoperability; they must also function globally and in space where the environment will have a similar, simultaneous operation by manned and unmanned technology from other nations, commercial entities, non-state actors and individuals.

- Plan for and address the inevitable conflict between civilian, commercial, military, or unknown or undetectable unmanned systems.

Yesterday, Today and Tomorrow

This chapter is a product of the lessons learned from co-author Dr. Hans Mumm. In his writings, teachings, and lectures, Dr. Mumm stresses the importance of robust multi-directional command, communication, and control between manned and unmanned technology operating on land or under it, in the air, on water or under it as well as in space. He refers to the concept known by many as Connectivity and automation in transport ("CAT"). Safe Uniform Traffic Management ("UTM") systems must allow for autonomous vehicles and other intelligent systems such as humanoids to communicate instantly and seamlessly. (European Commission, 2017) As we continue to examine the past, current, and future of

unmanned logistics, it is essential to remember Dr. Mumm's cautionary words.

Commercial delivery by drone is now a reality in many parts of the world. Companies ranging from Fed Ex to United Parcel Service to Amazon and Walmart in the United States currently have or are planning to use autonomous logistics as an essential part of their operations. While in China, food and light package UAV delivery has been in use by companies including SF Express, JD.com, and Ele.me. Similar light package and food delivery by Drone services are underway or anticipated in over 26 different countries globally. Table 8.1 is a partial list of the ongoing and planned parcel and food delivery by drone globally, as compiled by. (Unmanned Aerospace, 2019)

Table 8.1 Partial list of the ongoing and planned parcel and food delivery by drone globally

Country	Operator/ project leader	Type of operation	For more information
Australia	Project Wing	October 2017, first trials of goods deliveries by drone to rural Australian customers. Operations later extended to suburban Canberra.	https://www.unmannedair alphabet-project-x-deliver
Canada	Drone Delivery Canada	August 2018, Transport Canada approves testing of X1400 cargo delivery drone.	https://www.unmannedair regulator-approves-drone-
China	Ele.me	May 2018, Ele.me starts food delivery by drone in Shanghai.	https://www.unmannedair
China	JD.com	2015 – Rural drone deliveries start.	https://www.unmannedair rakuten-and-jd-link-to-pr
China	SF Express	March 2018 – SF Express secured China's first provisional drone operating license to begin deliveries of food within the country's pilot zones approved by the CAAC.	https://www.unmannedair chinas-sf-express-given-li
Dubai	Costa Coffee	September 2017 – First trials of a coffee drone delivery system	https://www.arabianbusin 379426-costa-coffee-tests
Estonia	SESAR GOF program	Parcels deliveries between Helsinki and Tallin planned as part of the SESAR network of demonstrator programs.	https://www.urbanairmob imminent-gulf-of-finland-
Finland	SESAR GOF program	Parcels deliveries between Helsinki and Tallin planned as part of the SESAR network of demonstrator programs.	https://www.urbanairmob imminent-gulf-of-finland-
Finland	Sky ports and partners	March 2019 – K-Maret deliveries to customers in Vantaa	https://www.urbanairmob drone-delivery-trials-start
France	DPD	In January 2018 trials of drone deliveries were announced for launch between Saint-Maximin-La-Sainte-Baume and Pourrières.	https://www.unmannedair special-report-delivery-dr

Germany	Emqopter	February 2019 – Trials began delivering pizza and industrial parts by drones Wurzburg (Germany)-based drone-technology company Emqopter.	https://www.unmannedair germanys-emqopter-deliv
Iceland	Aha and Flytrex	Commercial drone delivery flights began in Reykjavik from 2018, by operator Aha and Flytrex.	https://www.unmannedair flight-drone-least-risky-p
Ireland	A Post and Sky Tango	In July 2018 – A Post starts trials of off-shore drone delivery flights.	https://www.unmannedair irelands-post-autonomous
Indonesia	JD.Com	Drone delivery trials began with JD.com.	https://www.unmannedair chinese-retailer-jd-com-s
Japan	Rakuten	January 2019 – Drone delivery packages in rural Japan.	(https://www.unmannedai rakuten-start-drone-packa
Singapore	Airbus Skyways	February 2018 – Airbus Skyways Singapore parcel delivery drone makes first flight.	https://www.unmannedair airbus-skyways-singapore
Singapore	Airbus and Wilhelmsen	March 2019 – the two companies start shore-to-ship drone deliveries	https://www.urbanairmob airbus-wilmhelmsen-start
South Korea	Korea Post	Remote mail deliveries to start in 2021.	https://www.unmannedair korea-post-develops-utm-
Switzerland	Mercedes Zurich Matternet and siroop	September 2018 –Mercedes Zurich drone delivery program starts.	https://www.unmannedair mercedes-zurich-drone-d
UK	Vodafone	Strat of 4G mobile phone delivery trials in Scottish islands.	https://www.unmannedair vodafone-makes-uks-first
USA	Flirtey	March 2019 – BVLOS drone delivery flight trials start in Reno.	https://www.urbanairmob flirtey-to-conduct-bvlos-d

USA	Project Wing	August 2018 – in Virginia, Project Wing starts BVLOS urban area drone delivery trials,	ttps://www.unmannedairs project-wing-starts-bvlos-
USA	Flytrex	October 2018 – drone deliveries to King's Walk Golf Course in Grand Forks, North Dakota	https://www.flytrex.com/
USA	FAA Integration Pilot Program (IPP) project.	Herndon, VA – the program will facilitate package delivery in rural and urban settings.	https://www.faa.gov/uas/
USA	FAA Integration Pilot Program (IPP) project.	Loveland, OH – Workhorse Group Inc.'s Horsefly truck-launched Autonomous Drone Package Delivery System is now making package deliveries to homes in the Cincinnati area	https://www.faa.gov/uas/
USA	FAA Integration Pilot Program (IPP) project.	for Holly Springs, North Carolina – goods deliveries to resident backyards	https://content.dji.com/ drones-for-good-drone-d
USA	FAA Integration Pilot Program (IPP) project.	Memphis-Shelby County Airport Authority, Memphis, TN: inspection of FedEx aircraft and package delivery.	https://www.faa.gov/uas/

Source: (Unmanned Aerospace, 2019)

While there are many reasons for optimism based upon unmanned logistics' initial global adoption, as we can see in Table 8.1, widespread implementation of autonomous technology in the supply and delivery chain remains in its infancy. Challenges such as payload capacity, environmental considerations, UTM, and overall CAT technology are a few of the challenges which must be met before widespread automated logistics operations can become a reality of our everyday lives.

Yesterday

The noted Scientific Historian James Burke wrote in the 1978 book "Connections: Alternative History of Technology" that "When you read a book, you hold another's mind in your hands." "Why should we look to the past in order to prepare for the future? Because there is nowhere else to look." (Burke, 1978) When introducing new technology to society, there is always a significant dose of wonder, futurism, and promise, which helps drive adoption. Once the theoretical starts its metamorphosis into reality, there will inevitably be challenges and consequences that were not envisioned but need resolution to achieve adoption at scale.

In book one of this series, we examined the delicate balance between innovation and regulation, too much of one can negate the other's value and vice versa.

"Unlike the introduction of the railroads in in the 1800's, automobiles presented a greater challenge. Trains and trolleys were limited to travelling on rails, which made the design of infrastructure and regulation of operation less challenging. By 1920 it was clear that affordable automobiles were the conveyance of the future. People were migrating away from the mass transit staples of trains, busses and trolleys, and opting instead for personalized on-demand, motorized transportation." (Nichols, Mumm, Lonstein, Ryan, & and Carter, 2018)

When considering the widespread introduction of autonomous transportation, the challenge of maintaining order, safety, reliability, and efficiency become far more complex. While they were all incredibly disruptive and transformational technologies, the automobile, mechanically powered sea transport, submarine, subterranean, air and space travel were not simultaneously introduced into day-to-day life. When it comes to unmanned operation we are witnessing the near-simultaneous introduction of technology at every level of our environment and beyond.

One If by Land or beneath it

In his 2008 book Fighting Traffic, Peter D. Norton conducted an extensive analysis of the many considerations which contributed

to the development of rules and regulations for the operations of automobiles on streets previously used for pedestrians and animal-drawn traffic. Almost immediately accidents and death soared largely due to the fact in the early 1900's there were few or no laws for regulating motorized ground transport, many pedestrians were caught by surprise due to the noise, speed and a general public unfamiliarity with the automobile. Norton observed the tension caused by the introduction of this new technology.

"Most historical studies in the social construction of technology examine distinct artifacts that can be produced in quantity and that need not be shared. Streets are different. A mother cannot conceive of a street as a playground for her children while a motorist thinks of it as a path for driving at speed—at least not for long. The incompatibility of different constructions of a shared technology raises the stakes for relevant social groups. In a shared system, when a new construction becomes dominant, one group cannot easily secede from the prevailing denomination into a dissenter group where the minority construction is preserved." (Norton, 2008)

Over the last 125 years, the automobile has gone from something that was primarily for the elite to a ubiquitous technology that most adults in developed nations can either own or access regularly. It has become a staple of modern life. When Henry Ford introduced mass assembly lines in the early 1900s, automobiles became more affordable, and so the number of vehicles operating on roadways grew exponentially. With increased volume came more significant interaction between vehicles, pedestrians, animals, and the environment.

With more frequent operation came more interaction, more mishaps, accidents, and sadly deaths. In the 1950s and '60s, it became apparent something had to change if "a car in every garage" was to become the American dream instead of a nightmare.

1963 and 1964 represented a tipping point of traffic management and automobile safety in the United States. In just one-year automobile, fatalities rose and astronomical ten percent to 47,700

deaths. In response, the Highway Safety Act of 1966 was passed by Congress. Significant safety enhancement followed as Figure 8.1 depicts, between 1966 and 2013 the fatality rate per 100 million miles went from over 5 to just over 1 in 2013. (Federal Highway Administration, 2017)

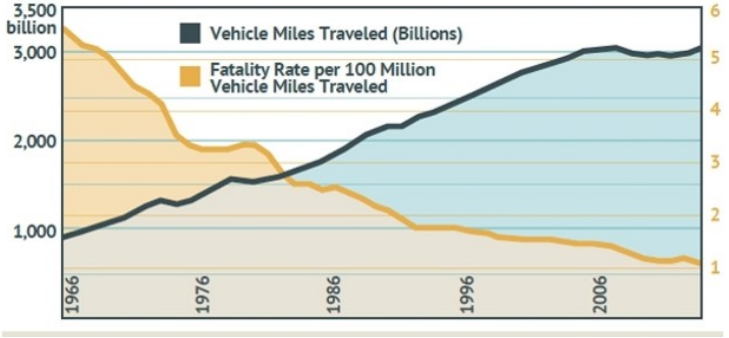


Figure 8.1 Vehicle Fatality Rate per 100 Million miles Travelled
Source:(Federal Highway Administration, 2017)

The success achieved in terms of vehicle safety is impossible to tie to any particular strategy, practice, or regulatory scheme. Instead, it is a multidisciplinary approach that allowed a vast reduction in automobile-related fatalities. The Four E's of Engineering, Education, Enforcement, and Emergency response is primarily credited with the overall success and are essential components of Uniform Traffic Management. (Federal Highway Administration, 2017)

Land-based autonomous transportation is limited to automobiles, busses, and trucks; many new technologies continue to develop, revolutionizing land-based locomotion. Currently, in China, an Autonomous Rail Transit (ART) system began operations in 2018. According to reports, the ART system operates on long-lasting, quick charging batteries and can travel up to 25 miles at up to

43 mph. The ART system can charge at stations along the route or the end of the line in approximately 10 minutes. It also runs on rubber wheels and virtual pathways using sensors so that no fixed rails or tracks are needed, and flexibility of routing can be dynamic. ART's are seemingly the "next big thing" in metropolitan transportation. (Railway-News, 2019)

Autonomous rail systems are not merely limited to inner-city commuter transportation.

Figure 8.2 Rio Tinto – Hitachi Autonomous Freight Train
Source:(Hitachi Corporation, 2020)

The first large-scale autonomous freight rail system commenced operation in the Pilbara region of Western Australia. The Rio Tinto Railway System, in collaboration with Hitachi Corporation, developed what they call the Auto-Haul™ System. According to its Case Study, Hitachi & Rio Tinto claim "more than 7.5 million train kilometers operated fully autonomously – without the need for an onboard driver – all while increasing safety outcomes." (Hitachi Corporation, 2020)

Recently a new reality has begun to evolve where an autonomous technology operates below the earth's surface. Earlier in 2020, the Defense Advanced Research Projects Agency organized and conducted the Subterranean Challenge Urban Circuit (SubT). According to DARPA:

"The SubT Challenge Systems and Virtual competitions aim to create community of multidisciplinary teams from wide-ranging fields to foster breakthrough technologies in autonomy, perception, networking, and mobility for underground environments. The Tunnel Circuit took place in August 2019. The Cave Circuit is planned for August 2020, and the Final Event incorporating all three underground environments is targeted for August 2021." (Defense Advanced Research Projects Agency, 2020)

Figure 8.3 Prototype DARPA SubT

Source: (Carnegie Mellon University, 2019)

Another autonomous technology is operating in the subterranean space in the mining and tunnel construction industries. One recent example can is in Mali, Africa. According to AZO Mining, the Syama Mine has engaged in a three-year partnership with Sandvik to provide:

Syama with its full suite of proven autonomous equipment and digital solutions, some of which include their full fleet of Sandvik TH663i trucks, DL421 autonomous drills, and fully autonomous loaders. Syama will also utilize Sandvik's OptiMine®3D Mine Visualizer, which will provide Resolute Mining workers with a real-time three-dimensional (3D) model of the entire mining environment that can be accessed from remote locations. One of the key advantages associated with the visualization system is that users can effectively analyze and immediately respond to events occurring in the mining environment. The system also allows users to efficiently plan future mining activities and operations, investigate problematic areas of the mine and track the development of the mine over time." (Cuffari, 2019)

Maritime traffic management has also seen a historical arc where a once non-existent and mostly an ad hoc reaction to disasters cost thousands of lives. History is replete with maritime disasters, like the Fleet of Kubla Khan, The Spanish Armada of the 1500s and the R.M.S. Titanic in 1912, related to the sea and environmental conditions or the inability of the crews to navigate, or ships to withstand the conditions. (Marine Insight, 2019) Others, such as the S.S. Andrea Doria, M.S. Stockholm, and the SS Admiral Nakhimov, sank due to collisions with another surface vessel. Finally, the Submarines USS Gatto and the U.S.S.R. K-19 collided approximately 200 feet below the surface. Both survived but were severely damaged. (Mizokami, 2017)

Figure 8.4 R.M.S. Titanic Sinking 2012
Source: (National Geographic)

Most of us are familiar with the R.M.S. Titanic's ill-fated maiden voyage in April of 1912, where over 1500 passengers and crew died in icy waters of the North Atlantic. While the reality is awful, Hollywood has, over the years, both romanticized and dramatized the events on that fateful night. Why did the new ship need to set a speed record? Why had none of the greatest maritime engineers in the world discovered the fatal design flaw of having watertight compartments in its hull, which could be sealed off in case of damage to the hull and thereby making the vessel theoretically "unsinkable." Sadly, in reality, a design flaw did not account for the fact that seawater after a hull breach could flow over the compartments, into the next thereby making the ship extremely vulnerable to sink in the event of a collision. (Bassett, 1998)

The disaster left the world in shock and immediately calls for

investigation and regulation grew. As a result, the International Convention for Safety of Life at Sea ("SOLAS") became law. SOLAS is currently under the aegis of the International Maritime Organization who has modified the Convention numerous times in the century following the sinking to the Titanic. (International Maritime Organization, 2020)

Numerous other maritime disasters have occurred over the years, many of which involved collisions between vessels or environmental obstacles such as icebergs, pack ice, the seafloor, and reefs. As the seas grew crowded, vessels became larger, faster, and ports, canals, and navigational straights became congested, the risk of disaster grew. To that end, Robert Frump, author of "until the Sea Shall Set Them Free," and Pulitzer Prize nominee, said, "Changes occur only when there is a meaningful disaster." "I think that most people will tell you that changes in marine safety are almost exclusively disaster-driven," agrees Dr. Josh Smith, a professor at Kings Point and interim director of the American Merchant Marine Museum." (Keefe, 2014)

Figure 8.5 Panama Canal Backup

Source: (Today Panama, 2015)

Like the automobile, regulation of nascent technology can be a painfully slow process, not only in terms of time but also in the cost of human lives and the environment. History of regulation shows that with time, technology, and safety improvements, and to that end, common-sense regulation is the best way to protect the public, crews, and the environment while allowing for technology to advance. Students should note that the history of maritime safety and traffic management closely parallels that of the automobile. Both technologies vastly improved with the advent of mechanical propulsion and the advances made during the early to mid-1900s.

While subterranean automation is just becoming a reality, Unmanned Underwater Vehicles have a long history of functioning beneath the waves. In 1957 the Applied Physics Lab of the University of Washington developed the Special Purpose Underwater Research Vehicle (SPURV). The SPURV was controlled remotely by acoustic communication. (Gafurov, 2015)

Three if by Air or in Space

A few short years ago, this section would be limited to air traffic. It is now clear that autonomous technology is and will have an increasing role within and beyond Earth's atmospheric airspace. In Chapter 2 of Unmanned Aircraft Systems (UAS) in the Cyber Domain, I wrote extensively about the history of the regulation of new technologies such as automobiles and aircraft. (Nichols, Mumm, Lonstein, Ryan, & and Carter, 2018) While autonomous vehicles continue to rapidly improve and evolve, so too does traffic. What was once considered acceptable UTM in controlled and unregulated airspace has now become less efficacious given the increasing proliferation of UAS in global airspace.

While autonomous vehicles continue to improve and evolve rapidly, so too does traffic. What was once acceptable UTM in controlled and unregulated airspace has become less efficacious given the increasing proliferation of UAS in global airspace.

As a case in point, the issue's complexity has become and why

regulation alone will not ensure that safety or reliability comes from personal experience. On June 29th, 2019, as a passenger on United Airlines Flight 1849 from Newark, New Jersey, to Atlanta, Georgia. Shortly after takeoff and well below 10,000 feet in altitude I noticed an odd and irregular series of maneuvers far different than those many travelers are familiar with as noise avoidance maneuvers and operation at major metropolitan airports. (Port Authority of New York & New Jersey, 2020)

It was a sunny summer day with mostly clear skies and a bit of the haze associated with metropolitan airspace. Since the airspace is complex and crowded with three of the busiest airports in the nation nearby, I like to film takeoff and landing since one never knows what you will see. Towards the east, I saw a small Drone in between my flight and the aircraft depicted
further to the east, just at the time, the odd maneuver occurred.

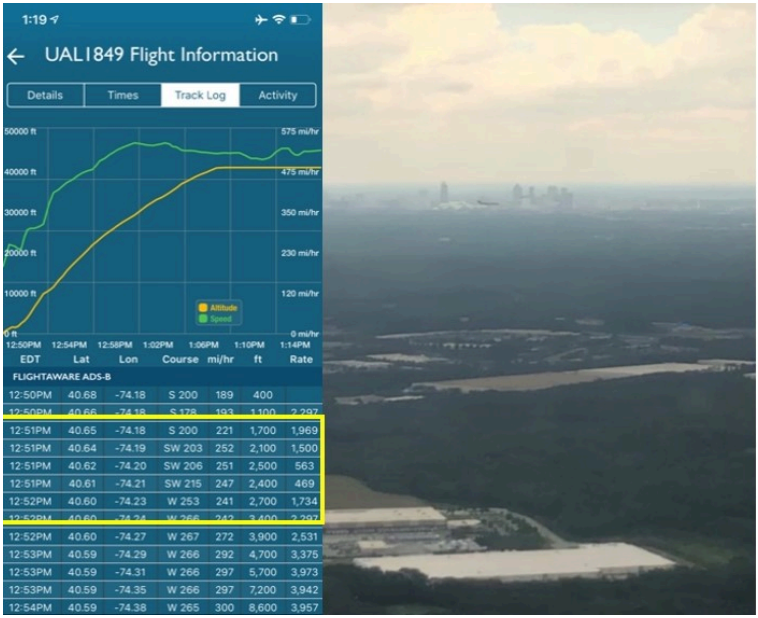


Figure 8.6 Photograph of departure from Newark Airport June 29, 2019

Source: (Lonstein, Takeoff Photo Newark to Atlanta June 29, 2019, 2019)

I recounted the event in a Forbes.com article entitled "Are Drone-Aircraft Collisions a Real Threat to Airline Passengers and Crews?" in August of 2019. (Lonstein, Are Drone-Aircraft Collisions A Real Threat To Airline Passengers and Crews?, 2019)

Merely suggesting the risk of small, unregulated UAVs operating in skies where other commercial traffic also operates is a recipe for collision did not sit well with the "hobbyist," or consumer drone manufacturers. The article's central premise was to point out that even if there are laws and regulations in place to deal with traffic management of unmanned aerial vehicles, it does not necessarily equate that operators will obey the laws much less be aware of them. This more significant challenge today is that the barriers to individual ownership, such as price, availability, and difficulty of operation, served as a natural limitation no longer exist.

Figure 8.7 Major League Drone Delay

Source: (Fox Sports, 2020)

The trend of smaller and smaller UAS also presents a more significant regulatory issue. On August 4, 2020, a Major League Baseball game between the Minnesota Twins and the Pittsburgh Pirates was delayed due to a drone's appearance over the stadium. It is the first known baseball "drone delay." (Fox Sports, 2020)

While controlled airspace and large public venues are a daunting challenge, unmanned aerial traffic management is not strictly limited to the earth's atmosphere. According to a 2019 report from the United States Defense Intelligence Agency entitled Challenges to Security in Space, many instances are cited where near-collisions and actual collisions between manned and unmanned space vehicle and debris. According to Appendix "A" of the report:

"Between 1998 and 2017, the International Space Station, which is in LEO, has maneuvered at least 25 times to avoid potential orbital collisions. With an expected increase in large constellations of satellites and space debris, there is higher potential for satellite collisions, particularly in LEO." (United States Defense Intelligence Agency, 2019)

Are we prepared for Autonomous Logistics?

The answer lies with all of us. Many of today's students will find themselves confronted with the challenge, which has confounded many technologists over the past few centuries. What is sufficient to handle today's technological requirements may be outdated tomorrow, and by "tomorrow," that means the next date on the calendar. The speed with which autonomous technology develops seemingly leads to new products and discoveries each day. What was an acceptable form of military defense on August 5, 1945, was obsolete the next day? What changed? That was the day that the first atomic bomb dropped on Hiroshima, Japan. (British Broadcasting Company, 2020)

What should be done?

Following the suggestions of Dr. Mumm to ensure an

interconnected Multi-Domain across autonomous technology platforms makes much sense. A World that relies upon Multi-Domain Autonomous systems is currently evolving. When considering how best to manage such complex systems, the key to understanding how best to maximize safety and efficacy is communication.

As with much autonomous technology, the military is often a driver of innovation in no small part based upon its need to function on short notice anywhere in the world. In a recent White Paper by Martin Kahn and Sean Thatcher on behalf of Lockheed Martin, the authors summarized the design as follows:

Figure 8.8 Lockheed Martin JADO

Source: Collaboration Strategy (Kahn, 2020)

"Lockheed Martin's Integrated JADO Collaboration Strategy provides a JADO architectural framework for future combat

operations in a joint and coalition environment. Our approach is an open architecture solution designed to incorporate existing systems and new technologies. Spectrum dominance capabilities provide undetectable communications in the HCE as well as a fused common operating picture." (Kahn, 2020)

Figure 8.9 Multi-Domain Traffic Management
Source: (Canstock Photo, Inc., 2020)

Transitioning from the battlefield to static civilian environments provides an opportunity to create Multi-Domain Autonomous Logistical systems, which will allow for commerce to benefit safely

and effectively from automation. In recent years, the debate on how best to accommodate autonomous vehicles on highways has narrowed, at least for the time between two models. The first, known as Self Reliant Vehicles (SRV), uses sensors to create awareness of its operating environment. The sensors include technologies such as "Light Detection and Ranging (LiDAR) and Radio Detection and Ranging (RaDAR) sensors that provide visual and locational data to the car, and possibly to other similarly equipped cars." Recently, the focus has shifted to technology that does not solely rely upon in-vehicle sensors alone; rather, it relies upon the Vehicle to Infrastructure regime or (V2I). (Ray, 2019)

While some might think it makes sense to build a communication and traffic management system for all forms of autonomous transport, very little Multi-Domain technology exists. A significant amount of study needs to occur with adequate foresight into how all autonomous systems can communicate.

That means new roadways, airports, seaports, and other infrastructure must be capable of supporting the autonomous operation; they must also be pre-fitted with the necessary technology to allow data and communication flow on, above and below simultaneously.

Only having traffic management for UAV's will quickly prove to be inadequate and dangerous as soon as multi-domain vehicles enter service. UAV's which are capable of operating on land and in the sky is already a reality. If there is no way to communicate, navigate, and safely operate on land, sky, and water in a safe, efficient, and commercially viable manner. The promise of autonomous technology may never be a reality. As this chapter is written, SpaceX, NASA, and similar technology are repeatedly proving the efficacy of unmanned vehicles operating in multiple domains. Traveling from land to Low Earth Orbit transitioning back into the earth's atmosphere and landing on the sea or land is now a reality. With the success of SpaceX and others, the seas, skies, and space may quickly become much more crowded and require traffic management in order to achieve commercial viability. On August 7,

2020, a Falcon-9 Unmanned Rocket took off from Cape Canaveral, Florida, and successfully deployed 57 Starlink™ internet-beaming satellites. After delivering its payload, the rocket successfully landed in the sea. One mission, five domains, Land, Air, Space, then back to Air, finally landing at sea.

Figure 8.10 SpaceX Falcon 9 Takeoff August 7, 2020
Source: (space.com, 2020)

Conclusions

While the SpaceX mission enjoyed the luxury of governmental authorities maintaining adequate traffic control, when thousands of unmanned logistical activities are co-occurring, the challenge becomes exponentially more challenging. Multiple domains, multiple nations, and multiple autonomous vehicles must function in harmony with each other, manned and human traffic in each domain, not to mention the weather and environmental interaction. With subterranean and underwater automation, the challenge seems daunting. Uniform traffic management systems for effective

logistics must work across the globe in multiple languages and with security. Any network is vulnerable to attack. Network design is far too broad and complex to examine in this chapter; however, it is a subject that must be in the front of all of our minds if the promise of autonomous logistics is to come to fruition.

Questions for students to consider

1. In the event of war, terror attack, dispute, embargo or other what is your vision to best mitigate the risk of calamity should the global UTM system lose functionality?

2. What type of UTM network would you design in order to minimize to the greatest extent possible security flaws and inevitable DDOS and other attacks? Assuming the success of such attacks how would you harden the system and provide for multiple redundant capabilities not dependent on each other to function?

3. Should the global UTM system be operated by nations individually under agreed upon rules, or operate under a multinational body such as the United Nations or a similar organization?

4. Who will pay for this massive infrastructure investment? If paid for solely by governments and private companies using the technology are profiting from it, how would you recoup the investment?

5. If, after much study, planning and debate individual nations decide to establish their own independent UTM systems, will it be possible to reliably and safely operate autonomous logistics between nations? If so, how would the system operate secretive or repressive nations such as North Korea and Iran?

References

Bassett, V. (1998). *Causes and Effects of the Rapid Sinking.* Madison: University of Wisconsin.

British Broadcasting Company. (2020, August 6). *Hiroshima bomb: Japan marks 75 years since nuclear attack*. Retrieved from BBC News: https://www.bbc.com/news/world-asia-53660059

Burke, J. (1978). *Connections.* Boston: Little Brown.

Canstock Photo, Inc. (2020, August 7). 3 Domain UTM Illustration. Canstock Photo, Inc.

Carnegie Mellon University. (2019 , August 12). Carnegie Mellon/ Oregon State Robotics Team Prepares For Subterranean Challenge. Pittsburgh, PA, USA.

Cuffari, B. M. (2019, December 20). *Syama: The First Fully Automated Mine.* Retrieved from azomining.com: https://www.azomining.com/Article.aspx?ArticleID=1519

Defense Advanced Research Projects Agency. (2020, April). *Subterranean Challenge Urban Circuit.* Retrieved from darpa.mil: https://www.darpa.mil/about-us/subterranean-challenge-urban-circuit

European Commission. (2017). *Connected and Automated Transport – Studies and Reports.* Brussels: European Commission.

Federal Highway Administration. (2017). *Road Safety Fundamentals.* Washington: United States DEpartment of Transportation.

Fox Sports. (2020, August 4). DRONE CAUSES DELAY IN PIRATES-TWINS. Retrieved from foxsports.com: https://www.foxsports.com/stories/mlb/drone-causes-delay-in-pirates-twins

Gafurov, S. A. (2015). *Autonomous unmanned underwater vehicles.* Amsterdam: Elsevier, LTD. Retrieved from sciencedirect.com.

Hitachi Corporation. (2020, January). *Robot Trains: How Hitachi Rail Tech Enabled Global First in Heavy Freight Rail Automation* . Retrieved from siocial-innovation.hitachi.com: https://social-innovation.hitachi/en/case_studies/robot-trains/

International Maritime Organization. (2020, July 23). *International Convention for the Safety of Life at Sea (SOLAS), 1974.* Retrieved from International Maritime Organization : http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx

Kahn, M. &. (2020, June). *Integrated Joint All-Domain Operations (JADO) Collaboration Strategy Full Spectrum Operations.* Retrieved from Lockheed Martin.com: https://www.lockheedmartin.com/content/dam/lockheed-martin/aero/documents/mdo/Integrated_JADO_Solution_Whitepaper.pdf

Keefe, P. (2014, June 20). *The history of marine safety is written in blood.* Retrieved from Maritime Reporter and Engineering News: https://www.marinelink.com/news/maritime/robert-frump

Lonstein, W. (2019, August 14). *Are Drone-Aircraft Collisions A Real Threat To Airline Passengers and Crews?* Retrieved from Forbes.com: https://www.forbes.com/sites/forbestechcouncil/2019/08/14/are-drone-aircraft-collisions-a-real-threat-to-airline-passengers-and-crews/#945a3e454f47

Lonstein, W. (2019, June 29). Takeoff Photo Newark to Atlanta June 29, 2019. Newark, NJ.

Marine Insight. (2019, October 4). *15 Famous Shipwrecks in the World.* Retrieved from Marine Insight : https://www.marineinsight.com/maritime-history/10-famous-shipwrecks-in-the-world/

Mizokami, K. (2017, June 21). *A Brief History of U.S. Navy Ship*

Collisions. Retrieved from Popular Mechanics: https://www.popularmechanics.com/military/navy-ships/a27021/ship-collisions-us-navy-history/

National Geographic. (n.d.). Sinking of the Titanic. Retrieved from National Geographic.

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: NPP Books.

Norton, P. D. (2008). *Fighting Traffic.* Cambridge: The MIT Press.

Panama Today. (2015, October 17). *Panama Canal traffic jam.* Retrieved from Today Panama: http://todaypanama.com/panama-canal-traffic-jam/

Port Authority of New York & New Jersey. (2020, July 30). *Aircraft Noise Engagement History*. Retrieved from Aircraft Noise – Port authority of NY & NJ: https://aircraftnoise.panynj.gov/aircraft-noise-engagement-history/

Railway-News. (2019, July 24). *China's Virtual Rail Transit System Put Through Its Paces in Doha.* Retrieved from Railway-News.com: https://railway-news.com/virtual-rail-transit-system-doha/

Ray, K. (2019, Winter). *Driverless Roads.* Retrieved from National Affairs: https://www.nationalaffairs.com/publications/detail/driverless-roads

space.com. (2020, August 7). *SpaceX launches 57 more Starlink satellites, lands rocket at sea.* Retrieved from space.com: https://www.space.com/spacex-starlink-launch-rocket-landing.html

Today Panama. (2015, October 17). *Panama Canal Traffic Jam.* Retrieved from Today Panama: http://todaypanama.com/panama-canal-traffic-jam/

United States Defense Intelligence Agency. (2019). *Challenges to Security in Space.* Washington: United States Government.

Unmanned Aerospace. (2019, April 7). *Drone delivery operations underway in 27 countries.* Retrieved from Unmanned Aerospace: https://www.unmannedairspace.info/latest-news-and-

information/drone-delivery-operations-underway-in-26-countries/

9. Chapter 9: Chinese Advances in Stealth UAV Penetration Path Planning in Combat Environment [Nichols]

Student Objectives

The task of planning a flyable, safe, paths for stealth UAVs to penetrate the US or allied forces Air Defense Systems (ADS) is considered. Students will gain a fundamental knowledge of path planning in terms of computer modelling of the path objective functions and cost of paths from node to node in a network. Constraints of collision avoidance, maneuverability, control, torsion, 2D /3D, communications, kinematics, SCADA are interwoven in the coverage of modeling goals. Special emphasis will be on the advances reported by Chinese researchers in improving the standard path planning models by including model-based predictive control and multi-step search methodology to increase the threat effectiveness for penetrating an ADS using stealth UAVs.

Introduction

In our previous books on UAS and CUAS, the authors covered a huge range of topics: UAVS, threats, vulnerabilities, countermeasures, radar, IFF, DEW, AI, autonomy, advanced systems technology, stealth design, safe flight activity in the NAS, legal and regulatory considerations, cyber taxonomies, INFOSEC, INFOWAR, SCADA, SWARMS, acoustical defenses, US ADS, ADS-B, GPS spoofing, Chinese New Silk Road Land and Sea Strategic advances, and more. (Nichols R. K., et al., 2019)(Nichols R. K., et al., 2020)

The authors were concerned with the Counter- UAS Problem (see below). (Nichols R. K., et al., 2020) Essentially, the authors were reactive in dealing with hostile UAS penetration of US ADS networks. What the authors did not cover was the path planning for a stealth UAV in static or dynamic civilian or combat environment. This chapter explores some of computer models and methodology to plan strategic UAV penetrations into a host civilian or combat complex environment.

The treatment is cursory as our students do not need to be aviation engineers or Red / Blue team members. They do need to be familiar with the behind the scenes technology. This chapter starts off with the C-UAS problem and attack on the Abqaiq Oil Facilities by Houthi terrorists. It then morphs into questions of how the Houthis 'succeeded where they had failed in the past; what the Chinese technology addition did for them; how this attack could be modelled / enacted with advanced UAV path planning techniques; and what elements are common to the modelling of such dynamic environment for UAS / UAV penetration.

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 (or any) 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 R. K., 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) The Saudi Arabian government has incorporated / purchased many of the US and Israeli ADS technologies into its own ADS.

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) 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 technology 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 Iranian clone uses Chinese path planning stealth penetration technologies.**[1]***

The take-away from this attack is not just the loss of global oil processing capacity and H2S stabilization processing facilities[2] 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) Threats and vulnerabilities of US ADS were covered in (Nichols R. K., et al., 2020) and apply to the ADS used by Saudi Arabia (SA) Over the last two decades, SA has purchased many of their ADS from both US and Israel.

Think of this problem more globally. China, North Korea, and Iran [referred to as CNKI technology cooperation] are aggressively cooperating on drone technologies for use by terrorists against a major oil production region. The technology is cost-effective as well as human capital efficient. Drones substituting for manned aircraft. Drones penetrating the SA ADS.

Figure 9-1 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 us expand the threat. Refer to Figure 9-2. 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.

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 Oilfields -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? Previous works have covered the topics of conventional countermeasures against SUAS / UAS and aggressor counter-countermeasures specific to UAS deployment – SWARMS. (Nichols R. K., et al., 2020)

Figure 9-2 Strait of Hormuz

Source: (Stratfor, 2019)

What else did the Chinese give the Terrorists besides the advanced KH-55 Missiles and Drones?

The answer is they taught the terrorists how to use the drones more effectively by showing them how to computer model and plan the penetration paths for their stealth UAVs in a combat environment.

Chinese Advances in Rapid Path Planning for Stealth UAV in Complex Environment with Bandit Threats

In a recent paper slated for publication in the ***International Journal of Aerospace Engineering***, Drs Zhang, Wu, Dai, and He, presented computer modeling results from their research into the subject of low altitude combat. Their paper addresses "a novel algorithm for stealth UAV to realize the rapid penetration path planning, which aims to devise a penetration strategy based on the improved A-Star algorithm to address problems of path planning and planning (sic) for stealth UAV in the complex dynamic environment. The proposed method introduces the kinematic model of stealth UAV and detection performance of netted radar in the process of low altitude penetration. Combined with the prediction technique and path planning algorithm, the multi-step search strategy is developed for stealth UAV to deal with POP-UP [3]threats and complete the planning (sic)of the path in different scenarios. Furthermore, the attitude angle information is integrated into the improved A-Star algorithm, which reflects the characteristics of the dynamic radar cross-section(RCS) and conforms to the actual flight requirements for the stealth UAV. Finally, the improved A-Star algorithm, learning real-time A-Star algorithm(LRTA-Star), and dynamic A-Star algorithm(D-Star) are respectively adopted to settle the problem of penetration path planning for stealth UAV in three different threat scenarios. Numerical simulations are performed to illustrate that the proposed approach can achieve rapid penetration path planning for stealth UAV indifferent dynamic threat scenarios and verify the validity of the improved A-Star algorithm." (Zhang, 2020)

Novelty

The Zhang paper presents a novel addition to the A-Star algorithm for path planning in a dynamic combat environment with "POP-UP" / *Bandit* threats. The novelty is an upgrade from the standard EW training on radar systems and Air Defense Systems (ADS). (Adamy D. -0., 2015) (Skolnik, 2008) The optimization techniques and computer algorithms (in present day computer programming languages) have been well researched and are not novel. (Reklaitis G. R., 1983) (Horowitz, 1978)

What is novel about the authors' paper is the *real time dynamics and predictive control applied to stealth UAV path planning via computer modelling*. It results in a computationally multi-step search pattern. The non-exclusive but mathematically necessary goals of flyable paths, collision avoidance, computational efficiency and reduced RCS are ably met with the authors' improved A Star algorithm. This gives us an insight into how far ahead the Chinese may be in the field.

Keep in mind that UAVs at low altitude rarely have IFF capability due to SCADA constraints and that Counter UAS (CUAS) technologies can bypass stealth features in combat and civilian UAVs. (Nichols R. K., et al., 2020) (Nichols R. K., et al., 2019) The validity of the algorithm is demonstrated in known mathematical bounded datasets with cases for single, dual, and networked radar surveillance systems. No real flight data is used. To many students in UAS, the above material is like jumping out of plane without a parachute.

UAV Path Planning

Time to take a stroll down cooperative path planning for UAVs in various environments. Then maybe we can recycle back to the Zhang paper with just enough knowledge to get a sense of the novelty of the technology about to be published by the Chinese researchers. The clearest reference on the subject of Path Planning

of UAVs is by Tsourdos, White and Shanmugavel. (Tsourdos, 2011) We will draw heavily from this fundamental textbook. [4] There are other fine textbooks on this subject to enhance the student knowledge: (Angelov, 2012), (Austin, 2010), (Barnhart, 2012), and (Dalamagkidis, 2012)

Path planning is a complex problem, which involves meeting the physical constraints of UAVs, constraints from the operating environment and operational requirements. Paths must be flyable. Flyable paths meet kinematic constraints of the UAV. Satisfaction of this constraint means that the motion of the UAV stays within bounds on maneuver curvature. Paths must exhibit CA for threats, obstacles, and other UAVs. Minimum fuel, energy conservation, and shortest distance come into play for an efficient and better performance path. (Tsourdos, 2011) Path planning algorithms produce one or more safe flyable paths for the UAVs. Path length, limited range, survey area, and flying direction all make a difference. The UAV trajectory must comply with speed and maneuver constraints; deployment of several UAVs in a coordinated manner which involve CA and simultaneous arrival at one or more locations. Lastly the algorithm that optimizes all these conditions must be computationally efficient, work in real-time, re-plan its trajectory if needed and with no significant delay. (Tsourdos, 2011)[5]

Path Planning Formulation

The primary aim of path planning is to provide structured mobility and to facilitate moving or flying multiple UAVs from one location to another. Several locations may mean several paths before reaching the final destination. On any known or partially known map /area there may be several points of interest (POIs).[6] The UAV has a specific attitude, which combined with its location to give the UAV *pose***[7] P(x, y, z, θ, Ψ), where x, y, z, is the UAV location or waypoint and (θ, Ψ) are the horizontal and vertical angles , respectively. (Tsourdos, 2011)**

Consider a UAV moving from one starting pose, Ps to another, finish Pf . Path planning involves producing one or more flight paths r(q) connecting Ps and Pf represented as

$$Ps \xrightarrow{r(q)} Pf \qquad (9.1)$$

Where r(q) is the resulting path, and q is defined as a path parameter. This parameter can be a lengths variable ($0 < q < s$) for a straight-line path or an angle variable ($0 < q > \theta$). The choice of the path variable depends on the path formulation.

Equation (9.1) is re-written for a single UAV as:

$$Ps\,(xs, ys, zs, \theta s, \Psi s) \xrightarrow{r(q)} Pf\,(xf, yf, zf, \theta f, \Psi f) \qquad (9.2)$$

Extending for **N** UAVs, where each pair of poses are connected by paths **ri (q):**

$$Ps\,(xsi, ysi, zsi, \theta si, \Psi si) \xrightarrow{ri(q)} Pf\,(xfi, yfi, zfi, \theta fi, \Psi fi) \qquad (9.3)$$

Where I =1,.....,N.

Equation (9.3) connects a pair of points by a path. This also represents route planning for one or more nodes of a network. The UAV route is usually defined by a set of waypoints joined by straight-line segments. However, these may not be flyable because UAVs cannot turn instantaneously through each waypoint. This is why waypoints require orientation for each segment to match – essentially a common tangent to produce a continuous path. (Tsourdos, 2011)Thus, some segments might be curved or curvy-linear to meet the common tangent condition. SAA sensors for ISTAR missions must be pointed in specific directions for effective

detection and identification. (Nichols, et al., Counter Unmanned Aircraft Systems Technologies and Operations, 2020)

Path Planning Constraints

Various constraints are involved in path planning. There are two general types: UAV-specific and those arising from obstacles in the environment. (Tsourdos, 2011) Violation of these constraints (i.e. communication failure) may lead to the complete loss of the UAV or sensor platform. Safety is a consideration for the mission. Turn radius also dictates which paths are flyable.

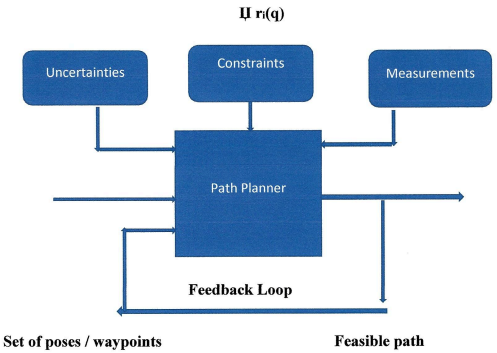


Figure 9.3 Simple Block Diagram Approach to Path Planning for UAVs
Source: Author drawn 07252020

Figure 9.3 Simple Block Diagram Approach to Path Planning for UAVs
Source: Author drawn 07252020

Turn radius also dictates which paths are flyable. Paths must balance safety and flyability. Flyable paths meet kinematic or

motion constraints and dictate maneuverability of the UAVs. (Tsourdos, 2011) Let **Ц** represent constraints. So (9.3) is written to include constraints (9.4). We now have enough information for a simple Black Box representation, Figure 9.1.

The inputs to Figure 9.1 are the poses, with additional constraints, uncertainties, and measurements. The feedback loop senses the measured states of the UAV and feeds back the success in terms of meeting the constraints to the path planner. (Tsourdos, 2011)

$$\textbf{Psi (xsi, ysi, zsi, θsi, Ψsi)} \xrightarrow{\textbf{Ц ri(q)}} \textbf{Pfi (xfi, yfi, zfi, θfi, Ψfi)} \quad \textbf{(9.4)}$$

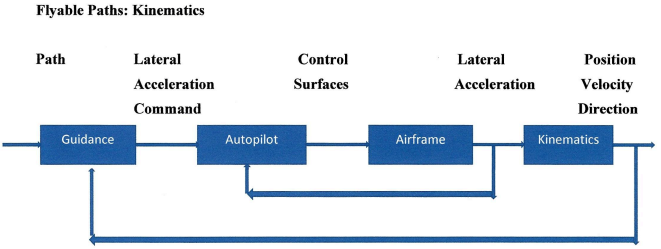


Figure 9.4 Autopilot and Guidance Control Loops
Source: Author drawn, 07252020

Figure 9.4 Autopilot and Guidance Control Loops
Source: Author drawn, 07252020

Paths need to meet the dynamic constraints of the UAV . They are influenced by the motion of the UAV. Essentially we have a SCADA control system. (Nichols R. K., et al., 2019) Refer to Figure (9.2) which shows autopilot and guidance control loops.

The inner feedback loop is the autopilot and the outer feedback

loop is the guidance system. The guidance system provides lateral acceleration commands to keep the UAV on path. The autopilot controls the UAV elevator, ailerons, and rudder to achieve the required lateral acceleration. (Tsourdos, 2011)

UAV dynamics include the aerodynamics, which produces forces and torques on the airframe. (Durham, 2013) Newton's third law of motion dictates that forces and torques produce lateral, longitudinal, and rotational accelerations. The accelerations are usually expressed in UAV body axes and these provide the link to kinematics. (Tsourdos, 2011) Kinematics is produced by integrating the UAV lateral and rotational acceleration vectors to obtain the UAV velocity vector. The attitude angles and current UAV position in the inertial frame give the UAV's translational and rotational velocity. The 2D path planner uses the kinematic model in equation (9.5a-b):

$$\dot{x} = / v / \cos(\theta) \qquad (9.5a)$$

$$\dot{y} = / v / \sin(\theta) \qquad (9.5b)$$

where **v** is the UAV velocity and **(θ)** is the horizontal heading angle. (Tsourdos, 2011)

Whether a given path is flyable is determined by the curvature of the path. The path planning algorithm has to produce a path **r(q)** that meets the dynamic turn rate constraint of the UAV, which is translated into the kinematic curvature constraint in 3D. It is determined by both the curvature and torsion. (Lipschutz, 1969) The curvature at any point on the path must be less than the maximum-curvature constraint of the UAV because it is proportional to the lateral acceleration. (Lipschutz, 1969) A curve segment of zero curvature is just a straight line and a curve segment of a constant curvature is an arc of a circle. At any given speed, **v**, the lateral acceleration **a** is proportional to the curvature **k** such that:

$$/ a / = / v2 / k \infty k \quad (9.6)$$

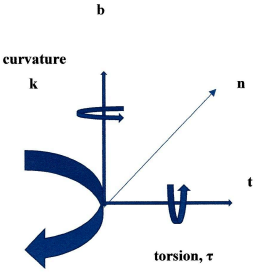


Figure 9.5 Curvature and Torsion
Source: Author drawn

Figure 9.5 Curvature and Torsion
Source: Author drawn

Where **a** is the lateral acceleration vector, **k** is the curvature, **v** is the velocity vector and ∞ is a vector operator. For a constant speed, the acceleration vector **a** is normal to the velocity vector **v**. This ensures that the velocity vector rotates without changing its magnitude. Refer to Figure 9.3where the velocity vector is aligned with the tangent vector **t** and the acceleration vector is aligned with the normal vector **n.** (Tsourdos, 2011)

Maneuver Coordinates

All maneuvers ca that coincide with the path tangent vector. n be defined by reference to a set of coordinates. 2D path planning confines the maneuvers to a plane. If the plane is horizontal, this is equivalent to flying at a constant altitude. In 3D space, flyable paths need to accommodate both curvature and torsion in their design. Curvature defines the turn radius of the path in 2D, which is defined as a rotation about an axis normal to the maneuver. Torsion is

defined as a rotation about an axes. See Figure 9.3 Note that positive curvature and positive torsion are defined as being clockwise along the appropriate axis viewed from the origin. For a UAV, in terms of body axes, curvature is equivalent to yaw rate turn and torsion is equivalent to a roll rate turn. In practice, UAVs will perform the turn by rolling to a fixed bank angle and then using the elevator to produce a maneuver normal to the wings. [8] (Tsourdos, 2011)

Generation of Safe Paths

The second important constraint of path planning is safety. Safety is measured by the ability of a UAV to avoid fixed and moving obstacles, and other AC or UAVs. Safety is represented in terms of a constraint that maintains flyability and collision avoidance. It is represented by **ЏIsafe** and is used to modify path planning equation (9.4). **ЏIk** considers the curvature constraint:

$$\mathbf{Ps\ (xsi, ysi, zsi, \theta si, \Psi si) \xrightarrow{ЏIsafe\ ЏIk\ ri(q)} Pf\ (xfi, yfi, zfi, \theta fi, \Psi fi)} \quad \mathbf{(9.7)}$$

Other constraints could be added to the above equation. For example, communication constraint on UAV separation distance could be represented by **ЏIcomm. (Tsourdos, 2011)**

Collision Avoidance (CA)

Collision avoidance between two flight paths r1(q) and r2 (q) can be represented by:

$$\mathbf{r1(q) \cap r2\ (q) = 0} \quad \mathbf{(9.8)}$$

This equation captures the condition required to be satisfied for CA. A cooperative path planning of multiple UAVs for CA can be formulated as producing flight paths {r1(q), r2(q),....,rn(q)} subject to the following constraints:

$$\text{If } k \le k_{max} \text{ and } \tau \le \tau_{max} \text{ and } r_i(q) \cap r_j(q) = 0 \quad i \neq j$$

Such problems are solved by optimization algorithms which involves heavy computation. In many cases the problem is broken down into phases / stages. (Tsourdos, 2011) Here we have our first intersection with the Chinese improvements on the A star algorithm for path planning. (Zhang, 2020)

A huge amount of work had been done in optimization algorithms to solve UAV and other problems. The best reference on the subject is Reklaitis. (Reklaitis G. R., 1983) Of interest to the reader are three optimization path finding algorithms: A-Star, D-Star, and improved A-Star with predictive control. Focus will be on what makes them different / useful for UAV path planning rather the details of the algorithms which can be found in Zhang. (Zhang, 2020)

A-Star Algorithm

The A-Star algorithm is a heuristic search algorithm, which is widely performed to various agents in the path planning problems to various agents. The main thrust of the A-Star algorithm is as follows. First, select the appropriate heuristic function, estimate the generation value of the extensible search points in the target search area, comprehensively. Compare the different cost values of each point. Consider the operation time and distance cost of the track point search. Last, find an optimal path. (Wikipedia, 2020) A-Star selects the path that minimizes:

$$f(n) = g(n) + h(n) \qquad (9.9)$$

where: **h(n)** is the heuristic function, the estimated distance from next node **n** on the path to the goal node; and **g(n)** is the cost of the path from start node **n** to the goal. **F(n**) is the path cost function.

At each iteration of its main loop, A-Star needs to determine which of its paths to extend. It does so based on cost of the path and an estimate of cost required to extend the path all the way to the goal. (Wikipedia, 2020)

A-Star has some disadvantages: A) only the position information of the stealth UAV can be obtained in the path, and the dynamic RCS characteristics and attitude information of the stealth UAV cannot be obtained; B) unknown path cost estimation cannot be accurately calculated in path planning, the final path cannot guarantee to be globally optimal[9]; and C) performance improvements include search validity, real-time performance in face of unknown threats and the expansion of track modes. (Zhang, 2020)

D-Star Algorithm

D-Star algorithm is a variation of the A-Star algorithm suitable for solving path planning problems in unknown environments. The main idea of the algorithm is to search the reverse path from goal to the origin when a new obstacle is found in the path. The path between the target location and the path node within the range of the new obstacle will not change due to the appearance of the new obstacle, but the path between the UAV and the node within the range of the obstacle will change during flight. The whole path is only partially re-planned. The heuristic expression for the D-Star algorithm is given by:

$$\mathbf{f(X, E) = h(X) + g(X, E)} \qquad \mathbf{(9.10)}$$

where: **h(X)** represents the actual journey cost from goal to state **X** and **g(X,E)** represents the estimated journey cost from the state **X** to the current position of the stealth UAV. (Zhang, 2020)

Chinese Improved LRTA-STAR Algorithm

Zhang describes the *learning real-time* A-*Star algorithm* (LRTA-STAR) as a heuristic search algorithm which satisfies the requirements of real-time planning in a dynamic environment by establishing and updating the evaluation cost from each state to the target point. However, the flight path planned by the single step search is composed of a series of broken lines. The maneuverability of the UAV is limited so that there is some difficulty to achieve accurate flight path tracking control. Search results are prone to traps in local dead loops, leading to failure of path planning. Zhang's team overcame these issues by combining LRTA-STAR with two big improvements: 1) model-based predictive control (MPC) and 2) multi-step optimal search method. (MSSM) Zhang's team extensively compared all the variations and the improved LRTA-STAR algorithm performed exceedingly well in a simulated combat scenario using stealth UAVs! Clearly they are thinking about penetration of allied ADS, something the military should take note of if not already.

MPC

Model-based predictive control is an optimization control method, which includes model prediction, rolling optimization, and feedback correction. MPC is described in detail by Zhang. (Zhang, 2020) MPC optimal control law for a multi-step prediction is given by:

$$J = \sum_{i=1}^{N} q_i [\, y_p(k+i) - y_r(k+i)]^2 + \sum_{j=1}^{W} \delta_j [u(k+j-1)]^2 \qquad (9.11)$$

where: **N** = length of the prediction domain; **W** is the length of the control domain; **qi** is the output prediction error, and **δj is** the weighting coefficient of the control variable. (Zhang, 2020)

Multi-Step Search Method (MSSM)

MSSM is a further refinement on the LTRA-STAR algorithm. It is novel search strategy based on multi-step optimization to achieve re-planning for a stealth UAV in a dynamic environment. In MSSM, the track cost of each predicted track is considered as a cumulative value of **N** predicted track nodes. The objective function of UAV flight planning can be obtained according to the optimal control law of the MPC system. The cost of the predicted flight path in N steps from the kth node is given by: (Zhang, 2020)

$$J(k) = \sum_{j=k}^{k+N} [\, b1T(j/k)\, B1b1(j/k) + \varepsilon j\, Pnet(j/k) \,] + \sum_{j=k}^{k+w} \delta j\, uT(j/k)\, u \quad (9.12)$$

Conclusions

This chapter has touched on a premier concern of ADS systems – path planning for stealth UAVs in a combat or civilian environment. Chinese researchers appear to have a novel approach to penetrating US ADS systems with stealth UAVs.[10] Their "improved LRTA-STAR algorithm presents a new solution for path re-planning control of stealth UAV in complex network radar environments with *Bandit* threats.

The improved A-STAR algorithm is based on a multi-step search strategy designed by model-based predictive control and LTRA-STAR algorithm. The attitude angle information of the stealth UAV is added to the calculations. This demonstrates the variation characteristics of dynamic RCS. [11] Kinematic analysis of the stealth UAV and detection performance analysis of netted radar, the

original paths and the re-planning paths can satisfy the actual flight requirements. (Zhang, 2020)

Discussion Questions

How would you implement the Chinese improved A-STAR algorithm in onboard UAV computers? The calculations are computer / storage intensive. Could part of them be done by ground stations and the intermediate results be communicated up to the UAV in real-time? How about on missiles? Rockets? A really helpful reference on this question is by Dr Tewari**.** (Tewari, 2011)

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. (2015). *EW Against a New Generation of Threats*. Boston: 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*.

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.

Barnhart, R. K. (2012). *Introduction to Unmanned Aircraft Systems*. New York: CRC Press.

Beaudoin, L. e. (2011). Potential Threats of UAS Swarms and the Countermeasures Need. *ECIW*.

Dalamagkidis, K. V. (2012). *On Integrating Unmanned Aircraft into the National Airspace System, 2nd edition*. Denver, CO: Springer.

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

DTRA. (2019, October 18). Private Communication re Aviation Vulnerabilities. (Nichols, Interviewer) Retrieved from https://www.dtra.mil/

Durham, W. (2013). *Aircraft Flight Dynamics and Control*. The Atrtium, Chesterton, UK: Wiley.

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

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.

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/

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, E. (1978). *Fundamentals of Computer Algorithms*. Potomac, MD: Computer Science Press.

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

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

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

Lipschutz, M. (1969). *Schaums Outline for Differential Geometry.* NYC: McGraw-Hill .

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

Marshall, D. M. (2016). *Introduction to Unmanned Aircraft Systems, 2nd Edition.* New York: CRC Press.

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.

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

N/A. (2020, July 25). *Cambridge Dictionary on line.* Retrieved from dictionary.cambridge.org/us/: https://dictionary.cambridge.org/us/

NASA. (2018). *Unmanned Aircraft Systems (UAS) Integration in the National Airspace System (NAS) Project.* Retrieved from NASA: https://www.nasa.gov/feature/autonomous-systems

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. M., & & Hood, J. P. (2020). *Counter Unmanned Aircraft Systems Technologies & Operations.* Manhattan, KS: New Prairie Press #31.

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., Ryan, J., Mumm, H., Carter, C., Lonstein, W., & Hood, &. J. (2020). *Counter Unmanned Aircraft Systems Technologies and Operations.* Manhattan, KS: New Prarie Press #31.

Nichols, R., Ryan, J., Mumm, H., Lonstein, W., Carter, C., & & Hood, J. (2019). *Unmanned Aircraft Systems (UAS) in Cyber Domain: Protecting USA's Advanced Air Assets, 2nd Edition.* Manhattan, KS: New Prairie Press #27 .

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.

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

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*.

Reklaitis, G. R. (1983). *Engineering Optimization: Methods and Practices.* Boston: Wiley.

Reklaitis, G. R. (1983). *Engineering Optimization: Methods and Practices.* Boston: Wiley.

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*.

Skolnik, M. (2008). *Radar Handbook, 3rd Edition.* Boston: McGraw Hill.

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

Tewari, A. (2011). *Advanced Control of Aircraft, Spacecraft and Rockets.* Chichester, UK: Wiley.

Tsourdos, A. &. (2011). *Cooperative Path Planning of Unmanned Aerial Vehicles* . Reston, VA: American Institute of Aeronotics and Astronautics, Vol #235.

Wikipedia. (2020, July 26). *A* Algorithm.* Retrieved from Wikipedia: https://en.wikipedia.org/wiki/A*_search_algorithm

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*.

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

Zhang, Z. W. (2020). Rapid Penetration Path Planning Method for Stealth UAV in Complex Environment with POP-UP Threats. *International Journal of Aerospace Engineering*, TBA.

Endnotes

[1] Chapter solely represents author's conclusion based on his research into Chinese weapons / technology.

[2] H2S is a problem for transportation of oil in tankers. It must be reduced from the raw oil so that the vapor pressure in the containers is stable. Unstable vapor pressure = explosion. Abqaiq facilities are the largest H2S desulfurization facilities in the Middle East (ME).

[3] The author identified the use of the term "POP-UP" as a major descriptive flaw. Almost every age group in society would use this term to describe the irritating browser pre- or post-fetch interrupts on their PC covering a slew of offensive subjects / offers / ransomware / invitations / fraudulent requests, etc. We do not think "POP-UP". We think "Bogie or Bandit." Aircraft threats that are suddenly painted by radar well inside the radar's range that were not seen earlier at a greater range are called BOGIE or BANDITS not "POP-UPS". Bogies are radar or visual contacts whose identity is unknown but not necessarily unfriendly. Bandits are aircraft identified as enemy, in accordance with theater identification criteria. Both Bogie and Bandit terms are based on criteria as

defined elements within ROE to protect friendly ADS from hostile aircraft.

[4] Tsourdos takes the discussion into 2D, 3D, Dubins paths, clothoid paths, Pythagorean hodographs, guidance geometry, torsion variations, and Frenet-Serret frames on 3D surfaces. These mathematical devices although interesting are way beyond the scope of this chapter.

[5] The computer modelling algorithms described in this chapter are elegant, efficient, and complex requiring advanced knowledge of optimization techniques, coding, differential geometry, and Pythagorean hodographs. Only the results or final equations that can be digested will be discussed.

[6] AKA waypoints. Same meaning for boat navigation

[7] Pose = 1) Present or constitute a problem , danger, or difficulty or 2) to move into a particular position, in order to be photographed, painted, recognized, etc. (N/A, 2020)

[8] This is known as a bank-to-turn maneuver.

[9] It may also be computationally inefficient.

[10] It is not mere speculation that such advanced path planning modelling may have been tested in the Abqaiq attacks. The UAVs were successful in reaching their target with only loss of ~3 drones.

[11] The Radar Cross Section (RCS) and radar detection probability methods are covered in many references. (Adamy D. , 2001) (Adamy D. L., 2004) (Adamy D. , 2015) (Alford, 2000) (Monahan, 2004) (Skolnik, 2008) Derivations were not included in this chapter.

PART IV

SECTION 4 UNMANNED VEHICLES WEAPONS FOR C4ISR & POPULATION TRACKING & CONTROL

10. Chapter 10 UV, Social Networks & Covid-19 Defense [Shay]

Student Learning Objectives

The student will obtain an understanding of how the federal regulation of UAS operations by the FAA, are affected by current Fourth Amendment, privacy laws and their interpretation at national, state, and local levels. Earn an understanding of how privacy laws have been applied to UAS and the common technologies they carry in their payloads. Develop an understanding of layered system of FAA regulation, matched with state and local level UAS legislation.

Key Concepts

1. Understanding the creation and evolution of the UAS legislative and regulatory operating environment, both federally and locally.
2. Understand the relationship between the CoViD-19 pandemic and UAS systems, their diverse technical payload and freight carrying abilities.
3. The ability for UAS to enable a "Surveillance State", facilitating fear and the potential 'over-regulation' which could hinder and undermine continued UAS industry growth in America.
4. Application and interpretation of the Fourth Amendment, privacy laws, and why they matter to UAS operators and industry.
5. FAA Regulations v. State Laws: Which is better for the continued growth and progression of the UAS industry and public privacy rights as a whole.

A Recent Rise in UAS Operations, Privacy Concerns and A Pandemic

The recent novel coronavirus (CoViD-19) pandemic has been a black swan event which has brought many modifications to our local, national, and global societies and norms. (Taleb, 2007) Many of these required changes, such as those related to the desire for increased usage and relaxed regulation of unmanned aerial systems (UAS) will likely have the intended effect of increasing UAS usage but may the unintended consequence of affecting the interpretation and application of constitutional law.

The UAS industry with the rapidly evolving technologies it employs, is by definition a disruptive technology. According to Margaret Rouse on WhatIs.com, "A disruptive technology is one that displaces an established technology and shakes up the industry or a ground-breaking product that creates a completely new industry." (Rouse, 2016) This disruption of legacy industry will continue and gain momentum, as UASs increasingly make their way into the average American experience.

These flying robots are natural candidates to perform pandemic related tasks categorized into the "three Ds": dull, dirty, or dangerous. (Diab, 2014) Until recently, the Federal Aviation Administration's (FAA) regulatory framework governing UAS and their industry was evolving at a slow, methodical pace. With the onset of the pandemic, UAS regulation has loosened to allow more industry partners to help the government combat the disease. Due to the ever-growing list of payloads and tasks UAS can and do perform, their new uses have made some citizens nervous and rightfully concerned about their privacy. As with all innovation and change, the UAS disruptions will have pros and cons. UAS sensors and payloads have the potential to capture, record, and upload huge amounts of data to their corporate owners and sponsors in near real time. Whether you are a willing part to this collection or not, there are privacy concerns regarding the collected data and for what it

can and will potentially be used. The Fourth Amendment protects citizens from unreasonable searches and seizures of individuals and their property. (Smentkowski, 2020) Whether or not the data collected and used by UAS, that pertains to individuals and their activities in both public and private locations, is protected by our Fourth Amendment rights or not is a brewing debate and one that could delay this disruptive technology's contributions to our society and economy.

As UAS use continues to grow without specific legislation or regulation protecting privacy, a legal conflict will likely ensue. This conflict and its outcome will undoubtedly affect the interpretation and application of constitutional law. We will look at the changes in the FAA's regulatory environment applicable to UAS, the court cases most likely to be referred to as precedence when UAS operation affects privacy concerns, any current cases in the federal system with potential to become or change the legal precedence for UAS' impact on Fourth Amendment rights[1], and the pros/cons of UAS v. 'Public Privacy' being regulated at the national level by the FAA or by a more Federalist approach at the local and state levels.

Background to the FAA's Regulatory Environment

To examine an environment and the effects a new technology has on that environment, we first need to understand how the environment was created and existed prior to the new technology. It is important to understand why the FAA and not the legislative bodies, have the authority to regulate private and commercial UAS operations within the national airspace (NAS). Congress grants this regulatory authority to ensure experts with aerospace experience are making the decisions concerning the safety and accessibility of the NAS. When Congress mandated the FAA establish rules for the regulation of UASs, they started with drafting new rules for private and commercial operators to establish CFR Title 14, Part 107. Commercial operators who wanted to carry freight via UAS would

also be regulated by meeting the applicable requirements in CFR Title 14, Part 135, which all air carriers must comply with.

To appreciate the different roles of the FAA and state legislations, as they pertain to UAS, and their effects on public privacy, it helps to review an online press release dated 20 July 2018, from the FAA. The title of the web page is, "Press Release – FAA Statement–Federal vs. Local Drone Authority." (FAA, 2018) The primary purpose of the press release is to remind readers what gives the FAA its authority over the entire NAS, and allows it to preempt state and local governments from legislating UAS operations; EXCEPT for areas traditionally governed by state or local legislation i.e. land use, zoning, privacy, trespass[2], and law enforcement usages. (FAA, 2015)

There are two congressional laws which encompass most of the federal legislation pertaining to UAS; the FAA Extension, Safety, and Security Act (FESSA) of 2016, and the FAA Reauthorization Act of 2018 (H.R. 302). There are others, such as the National Defense Authorization Act of 2017, which makes it legal for the Department of Defense to shoot down UAS over certain areas, but these only have small or single sections pertaining to UAS. (Rupprecht J.) The FESSA provided one key article of particular importance to this chapter; the article which streamlined the FAA process for approval of interagency teams to use UAS in emergency situations. (U.S. Senate, 2016) We've included a summary of the Part 107 and 135 changes made by the FAA to address the CoViD-19 pandemic in Appendix C. In short, the FESSA was exactly what the FAA used when it issued the emergency changes at the beginning of the pandemic to rules established under the direction of H.R. 302. (FAA, 2020)

As stated, most of the relevant legislation Congress has passed pertaining to UAS was included in H.R. 302. For reference, we've included a summary in Appendix A. The primary UAS result of

H.R. 302 was the FAA's establishment the regulations in the Code of Federal Regulations (CFR) Title 14, Part 107 requirements. The operating environment created by H.R. 302 can be summarized by the following: operators of UAS must obtain a certification from the FAA, must be operated below 400', must be operated within visual sight of pilot, a pilot can only operate one UAS at a time, cannot be operated over people, and cannot be operated at nighttime. For reference, a summary of the complete set of CFR 14, Part 107 rules pilots or UAS operators must follow is located in Appendix B. Since the establishment of the Part 107 rules, any operators who wish to deviate outside these rules is required to request a waiver through the FAA.

To review the legal operating environment created by the H.R. 302, and its impacts on privacy, a few sections of the law, and the deliverables required by those sections, are of particular importance to this study. The first of these is Section 357, titled "UNMANNED AIRCRAFT SYSTEMS PRIVACY POLICY UAS." The summary of this section is quite brief but clear, "UAS operations shall be carried out in a manner that respects and protects personal privacy consistent with the United States Constitution and federal, state, and local law.[3]" Although this statement in the law appears to be quite vague, it ensures the state and local authorities will have a say in how UAS operations and their effects on privacy will be litigated.

The next applicable area of H.R. 302, Section 358, and titled "UAS Privacy Review" mandates a deliverable from the Comptroller General of the United States National Telecommunication and Information Administration. The deliverable is a report to congress from the Comptroller General because this is the office of government that has been working on a review of federal, state, and local statutes, meant to address UAS impacts on personal privacy. The Comptroller General's office was originally tasked with this review by President Obama in his Presidential memorandum "Promoting Economic Competitiveness While Safeguarding Privacy,

Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems," dated February 15, 2015. (Obama, 2015) This report was originally due to Congress 180 days after the signing of the law, around April 2019, and has not been produced or delivered according to the authors' research.

The final section of H.R. 302 pertaining to this study is Section 378, titled "Sense of Congress." The purpose of this section is to require anyone who operates UAS for hire, except the media, to have a written privacy policy which must be made available to customers and the public. This policy is required to disclose the collection, storage, use(s), destruction, and sharing of any data collected during the UAS operations. (Zoldi, 2020)

It should be pointed out concerns over the changes made to UAS regulation by the FAA have not created a wild west free for all of UAS activity in the U.S. The changes made to the FAA's regulations were largely administrative. (FAA, 2020) There is an increasing amount of UAS operating companies working to get into the CoViD-19 fight. Here are examples of newly approved applications for waivers to operate UAS during the pandemic:

- March, Wing begins making home deliveries of dry goods and medicines to homes in Virginia during CoViD-19 induced lock-down, through FAA approved trial (Summers, 2020)
- April 27, UPS and Matternet get approval to support a quarantined retirement community with UAS deliveries from a local CVS pharmacy (Bonifacic, 2020)
- May 27, the FAA granted Zipline an emergency BVLOS waiver to fly medical supplies in North Carolina. The flights will cover 20-30 miles and carry up to 4 lbs of medical personal protective gear and supplies (de León, 2020)
- July 14, UPS and Matternet approved to deliver time and temperature critical medicines and PPE to medical facilities in N.C.(McNabb, Matternet and UPS Expand Hospital Delivery

Network, 2020)
- July 28, Cotton Bowl is first outdoor stadium to use UASs spraying disinfectant in an effort to combat CoViD-19 and support sporting events. (Davis, 2020)

How Previous Case Law Concerning UASs or the Technology They Carry, Has Been Applied Toward Privacy and Fourth Amendment

To begin the examination of cases involving UASs, privacy concerns and the Fourth Amendment; we will start with a relatively recent case, Brossart v. North Dakota (2015)[4]. The following is a summary of the case and its related features to our study. The case involved local law enforcement requesting a UAS from the U.S. Customs and Border Patrol to take photographic evidence when local authorities were confronting Brossart over allegations of cattle theft. This is the first known incidence in the U.S. where evidence, collected by a UAS, *without a warrant*, was used against an American citizen. Brossart looked to dismiss the charges due to his belief his Fourth Amendment rights were violated by the UAS invading his privacy.

His defense cited support from a SCOTUS decision in Kyllo v. U.S. (2001)[5]. In this case SCOTUS ruled to throw out evidence obtained by infrared technology without a warrant. The North Dakota Supreme Court ruled the evidence from the UAS was admissible due to the precedence set by SCOTUS in the ruling of California v. Ciaraolo (1986)[6]. In this case SCOTUS ruled an individual's privacy and Fourth Amendment rights are not violated when their actions can be observed from an aircraft in navigable airspace, in this case, from 1000 feet above ground level (AGL). With these decisions by the North Dakota Supreme Court, Brossart was the first American citizen to serve federal prison time, due to evidence obtained with a UAS. (Bomboy, 2014)

To further examine the issue of UASs and privacy, it is sometimes necessary to form a scenario using a very particular set of assumptions. This was precisely the case made by David Sella-Villa in his work, *Drones and Data: A Limited Impact on Privacy*. We will look at just how a UAS would affect privacy within the set of assumptions he describes in his paper, and what happens when you alter the assumptions. Let us start with a UAS being operated with a simple visual light spectrum camera. The visible light spectrum simply put is light or images visible to the naked eye.[7] Further we are only looking at scenarios where the UAS are being operated and piloted legally. Finally, it is important to know the author's definition of privacy, which is "privacy simply means freedom from unwanted visual observations in and about the home."[8] (Sella-Villa, Drones and Data: A Limited Impact on Privacy, 2020)

Another key condition to be noted concerning this paper and the author's view point is the statement and reference that UAS flights beyond visual line of sight (BVLOS), "have been reserved exclusively for military and search-and-rescue operators."[9] Although this may have been true at the time of his writing and publishing, the UAS industry has been moving towards BVLOS flights as being absolutely necessary for UAS delivery and other commercial uses. (Seeking Alpha, 2019) Within these viewpoints and assumptions, the author examines and makes a convincing argument that UASs outfitted only with visual light spectrum cameras do not significantly challenge the jurisprudence[10] of privacy law in the U.S. However, the author does concur that UASs are significantly able to exploit traditional assumptions about privacy and trespass as defined in our legal system. (Sella-Villa, Drones and Data: A Limited Impact on Privacy, 2020)

The most significant contribution of Mr. Sella-Villa's paper to this chapter's study is his break-down of why UASs outfitted with visual light spectrum data collection devices alone, will not challenge our

Fourth Amendment rights, as the laws are currently written. Much of his legal reasoning for this has to do with the precedence of "Third Party Doctrine". The basis of this concept has been established through several cases heard and decided by the SCOTUS, and "maintains that one cannot assert a privacy interest over something that has been knowingly shared with a third party."[11] The two primary ideas behind this premise according to the author's listed assumptions, are; the UAS is operated legally, without trespass and the UAS' image capture software stores images remotely. This is almost always true because of the how UASs share what they are 'seeing' in near real time with their operators. (Sella-Villa, Drones and Data: A Limited Impact on Privacy, 2020)

Additional examples of how UAS and their technologies potentially impact privacy concerns can be found in products of the Congressional Research Service, which prepares and drafts reports for Congress[12]. One particular we will examine is titled, *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses*, by Richard M. Thompson II, a Legislative Attorney. His report specifically looks at and addresses the use of UAS by law enforcement to conduct surveillance both with a warrant and without one. Key points highlighted in this report are how a UAS is essentially a data collection device, and that without its high technology payloads, should not be considered a threat to Fourth Amendment rights or privacy laws. The author suggests that many of the known high-tech payload capabilities of UAS (keep in mind this article was written in 2013) have been addressed sufficiently in federal or state laws. In the conclusion however, the author concedes that where the capabilities of a UAS and its payload is headed, could be a place that will stretch our current privacy and Fourth Amendment protections to their limits. (Thompson II, Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses, 2013)

A second report from the Congressional Research Service, also

written by Thompson, but slightly later in 2015, is titled *Domestic Drones and Privacy: A Primer*. This report, its cited sources, and the author's legal perspective provide a comprehensive understanding of the complexities surrounding UAS and our current legal framework's ability to contain the privacy invasion concerns and unlawful search threat posed by the potential of UAS payloads. (Thompson II, Domestic Drones and Privacy: A Primer, 2015)

Technologies of the Digital Age and the Fourth Amendment

Further study of the existing legal and regulatory landscape and the dangers of its lack of specific privacy protections, can be found in *The Sky Police: Drones and the Fourth Amendment*, by Jessica Dwyer-Moss. Her work is a fairly comprehensive examination of the wide array of technologies UASs can bring to domestic authorities' surveillance methods. Applicable legal cases, pertaining to the individual technologies and their impact on the Fourth Amendment are also reviewed. This work uses many of the case studies we have discussed previously to show how dated these references are compared to the twenty first century technologies UASs will present to test them. An important case she brings to the discussion is Carpenter v. United States[13]. This case was not decided by the time of her publishing, but she correctly included it due to its topic being cell phone location records being used without a warrant, in the conviction of a robbery suspect. Shortly after she published her article, SCOTUS decided the case. In their decision it was determined that cell phone location data is constant and should be considered from the legal standpoint like GPS data, as protected by the Fourth Amendment, requiring law enforcement to obtain a warrant for its sharing and use as evidence. This is seen as a win for privacy advocates and a blow to the Third-Party Doctrine's coverage of modern electronic data. (Dwyer-Moss, The Sky Police: Drones and the Fourth Amendment, 2018)

Another case highlighted by this work is Riley v. California[14]. In

this case SCOTUS had to decide if law enforcement could search an individual's cell phone upon arrest. The court in its decision made particular note that the main reason an officer is allowed to search an individual under arrest is to preserve evidence and ensure safety of the officer and person under arrest. SCOTUS concluded digital data could not harm an officer or help the individual escape, a warrant was required in order to search a cell phone. (Dwyer-Moss, The Sky Police: Drones and the Fourth Amendment, 2018) This ruling could be immensely important to UAS operators and companies, since the primary thing UASs will "deliver" in the near future is data.

Dwyer-Moss also examines the rulings in cases where aerial observation was a key component, although Brossart v. North Dakota was not among them. Dwyer-Moss is an Assistant General Counsel at the Department of Defense whose extensive areas of practice include but are not limited to, Privacy Act, Privacy and Civil Liberties, and Intelligence Oversight. (Dwyer-Moss, Jessica Dwyer-Moss' Profile, 2020) Her knowledge, opinions, and expertise in subjects discussed in this chapter has been immensely helpful in establishing the current environment and upon where it can be improved.

An important legal construct to understand when we look at how UASs and the data they can collect effect privacy and the Fourth Amendment is known as the Miller Doctrine or Third-Party Doctrine. This extremely important concept in Fourth Amendment law came from two decisions, Smith v. Maryland[15] and United States v. Miller[16], by SCOTUS in the 1970s. These two decisions both referenced SCOTUS's decision in Katz v. United States[17]. In the Katz decision SCOTUS ruled that Fourth Amendment protections not only applied to an individual's tangible things but also to an individual's reasonable expectation of privacy. United State v. Miller's decision helped to frame and contain this expectation by establishing that no reasonable expectation of

privacy can be expected when one uses the services of a third party, in this case the phone company, to contact (dial numbers) another party. The conversation between yourself and the party you contact is protected and would require a warrant for authorities to access[18], but the number you dialed, the time you dialed it, and the connection made, were ruled to be business records of the third party, and therefore could be subpoenaed[19]. In Smith v. Maryland, a similar decision was handed down stating that records such as deposit slips, and checks used by an individual to perform business with the bank were not protected by the "reasonable expectation of privacy"[20] outlined in Katz because the customer was voluntarily sharing and disclosing their business with a third party[21]. All these decisions taken together have come to be known as the Third-Party Doctrine. This doctrine and its application to twenty-first century technology is highly applicable to the subject matter of this chapter. (Thompson II, The Fourth Amendment Third-Party Doctrine, 2014)

Examinations of Technologies on UASs due to CoViD-19

An examination of all the individual technologies UASs are capable of carrying and collecting data with, is beyond the scope of this chapter. In an effort to discuss these technologies in a relevant perspective, we will discuss one cutting edge technology and how it is being used in the CoViD-19 pandemic. This technology was selected to be the example of how new technologies can raise privacy and Fourth Amendment concerns. The technology is a new form of bio-identification. A recent study of this new technology demonstrates just how capable UASs have become at being private data collection devices. The recent research study proved how UASs can pick-up and monitor the cardiorespiratory signals from multiple individuals while flying at 200 feet AGL. (Al-Naji, 2017) This type of progress and advancement in a potential payload's abilities are the kinds of advancements, once unleashed on society 'for its own good', are very difficult to discontinue or legislate after the fact. Although, as we will discuss in a later section, efforts to

legislate this type of UAS data collections have been proposed and argued in state capitals.

Another work to study modern technology and its impact on the Fourth Amendment, is a short but important contributor to this chapter. The article is *Drones and the Fourth Amendment* by Robert E. Smith and published in the May 2017 edition of Privacy Journal. In his work, Smith concentrates on the implications of the government's use of UAS equipped with surveillance technologies. His first point is how there is an established precedence for the government to use visual camera-based surveillance both with and without warrants. These instances without a warrant require certain circumstances to exist such as "possible destruction of evidence, escape of a suspect, danger to the police or public." However, any video surveillance that includes audio recordings must have a warrant. This is due to established requirements in the federal electronic surveillance laws. Smith boils down the two most important cases, in his opinion, for UAS surveillance by the government. These are Kyllo v. U. S., due to the use of thermal imaging equipment; and Jones v. U.S. and its use of GPS tracking data. The final point to stress from this article is the one Smith makes by including words from the late Associate Justice Anton Scalia, who wrote the majority opinion in both cases. In the majority opinion of Jones v. U.S., Justice Scalia wrote;

"This court has to date not deviated from the understanding that mere visual observation does not constitute a search…It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question. We may have to grapple with these 'vexing problems' in some future case where a classic [physical trespass] is not involved."

Associate Justice Anton Scalia, (2012)

In another fairly prophetic portion of the major opinion, Justice Scalia also noted, "the transmission of electronic signals without

trespass" falls under Fourth Amendment restrictions. (United States v. Jones, 2012) (Smith R. E., 2017) To date, from the author's research, no further decision by the Supreme Court has addressed the potential of electronic signals to be included in or excluded from Fourth Amendment protections.

Federalism or Federal Regulation of UASs

To better understand the role of Federalism in UAS and privacy legislation and regulation, we will look at both the pro-Federalism view, and the con-Federalism (or continued FAA regulation) view. Available academic materials were heavily sided toward the pro Federalism argument of UASs and their abilities being regulated at a local level. The con arguments cited are predominately articles from economic advocacy groups.

Pro Arguments

To begin the look at the "Pro" side of the argument, an essay by Margot E. Kaminski titled Drone Federalism: Civilian Drones and the Things they Carry, was reviewed. Her essay is rooted in the belief that there are two basic areas of UAS privacy legislation, UAS use by law enforcement, and UAS use by civilians. She notes the FAA's regulations have specifically allowed law enforcement to use UAS technology since the Congress's original UAS legislation[22]. A common theme throughout this essay is the regulation and control of UASs and their payloads is best legislated by local authorities because of their "experience regulating other forms of civilian-on-civilian surveillance." Perhaps the most notable argument for local authorities to regulate the privacy concerns around UASs, is one where she points out that an overarching and preemptive bill by Congress or omnibus privacy regulation by the FAA would, to be effective, be too restrictive in nature and run the real risk of infringing on UAS operators First Amendment rights. The essay also points out the FAA Modernization and Reform Act of 2012 (112 Congress, 2012) does not mandate the FAA take up the issue of privacy, and suggests the reason for this is likely the tradition

of states and local governments enacting privacy controls at their levels. Her conclusion has a focused warning against Congress getting in too big of a hurry to control the budding UAS threat, and to allow the state and local authorities address the issue in their own jurisdictions. (Kaminski, 2013)

The next work doesn't so much argue for the states to regulate UASs as it assumes their control by local authorities is what is best for the growth potential of the UAS industry as a whole. In their report, Which States Are Prepared For the Drone Industry, Brent Skorup and Connor Haaland from George Mason University study which states have prepared themselves to take advantage of the economic benefits the UAS industry can bring. The basis of their work is the assumption that states can best be ready to reap these benefits by creating "drone highways-aerial corridors directly above public roads." The authors research which states have the appropriate legislative conditions to enact UAS highways. They do this documenting and grading all 50 states on their preparedness in 5 factors for UASs and enacting UAS highways. The factors are: an airspace lease law on the books, an avigation easement law, a law vesting air rights with landowners, some sort of aviation advisory committee at the state level, and a look at the number of UAS jobs (per 100,000 residents) in each state. Of note, North Dakota was ranked #1, Arkansas #2, Vermont #3, Kansas #32, and S. Carolina #50. The 'air' highways described by Skorup & Haaland are one of the concepts proposed that would make the UAS industry more palatable to property owners concerned about their privacy and is a novel way for states to enact similar legislation to maintain an economically even playing field. Whether this legal construct for UASs catches on and is enacted or not remains to be seen. (B. Skorup & Haaland, 2020)

The final piece of pro-Federalism research comes from a guest article published by Dronelife.com, but written by Jonathan Hayden, Esq. It is titled Why the Drone Community Should Not Embrace

Exclusive FAA Control of Drone Regulations. In this article, Mr. Hayden begins by setting the scene twenty years into the future. He assumes that many of the FAA's UAS regulatory arm members and experts are former employees from the larger of the companies within the UAS industry. This is not an uncommon or unlikely occurrence since other federal regulatory bodies are currently made up of such professionals. The problem Mr. Hayden foresees with this is *if* the FAA has complete regulatory control, this can create an environment where the large corporations, who are primarily concerned about profit, will have too large of a voice in the regulatory process. An idea which has been demonstrated in other industries on multiple occasions. This could even create a reality where landowners are prevented from flying UASs over their own property because they may interfere or endanger commercial UAS activity in some scenarios. The best possible answer to this is for the states and local governments to have control over their jurisdictions. (Hayden, 2020)

Con Arguments

The first argument against a federalism approach to UASs, privacy and the Fourth Amendment is a revisiting of *The Sky Police: Drones and the Fourth Amendment*, by Jessica Dwyer-Moss. As a backdrop to the overall concerns from UASs on privacy in her paper, Ms. Dwyer-Moss opens her work with the following quote, "In the far distance a helicopter skimmed down between the roofs, hovered for an instant like a bluebottle, and darted away again with a curving flight. It was the Police Patrol, snooping into people's windows." (Orwell, 1949) The majority of her paper examines a collection of case law which can and will be used as precedence to decide UAS and high technology legal disputes in the near future. The problem, as the Dwyer-Moss sees it, is that precedence can be overturned by a new subjective definition of societies "reasonable expectation of privacy" and regulations can be changed by an agency submitting a proposed change and allowing it to be committed on before changing it. The only sure way for Fourth Amendment protections to be guaranteed is for Congress to take up the matter and legislate

visual and electronic surveillance norms. She sums up her argument by stating that "A national approach is ideal, but in the absence of federal legislation, some states have begun to regulate drones for themselves." (Dwyer-Moss, The Sky Police: Drones and the Fourth Amendment, 2018)

An additional argument against the state and local governments controlling UASs is presented in *States Rush to Regulate Drones Ahead of Federal Guidelines*, by Sarah Breitenbach. This article uses what the states have already tried to do in their legislation to make the argument that Congressional law and Federal regulation will be the best way to protect privacy without stifling the natural innovation of this disruptive technology. In 2015 California's Governor vetoed a law that would have made it illegal for any commercial or private UAS to fly less than 350 feet AGL over private property without consent. Had this legislation been enacted, UAS delivery in California would have been severely set back. An interesting point in this article is when the author notes the ACLU has not requested tighter regulation of UASs due to their belief that most privacy concerns posed by UASs are covered by laws already on the books. In a further comment, the ACLU attorney, Chad Marlow suggested state laws limiting UAS activity can actually harm society by preventing the filming of illegal activity. (Breitenbach, 2015)

A Look at UAS Federalism in Action

In order to understand what state legislative responses have been to disruptive UAS and the technologies they carry; we will review state legislation whose primary purpose was to address UAS or their technologies specifically. A comprehensive review of all the state legislation pertaining to our topic is beyond the scope of this textbook. To ensure a more accurate accounting of state UAS laws, two web sites were used to create the collection of laws represented in this chapter. The first was the site of the National

State Legislative Council. (National Conference of State Legislatures, 2020) This site was extremely thorough with its list of UAS impacting legislation and resolutions, up to and through 2019. This sight included laws that addressed newer technology privacy laws in its list, knowing that UAS could or would be outfitted with increasingly sophisticated payloads. The second site was a site dedicated to monitoring state and local governments, called Governing.com, and their adaptation to current events and national cultural trends. One article on this site in particular looked at how state and local governments were using UAS technology as an answer to the CoViD-19 pandemic. (Smith C. , 2020) This article and its included database have been kept current through the writing of this chapter.

State Laws Pertaining to Privacy and UASs Before CoViD-19

In the effort to understand the different approaches state legislatures took to regulating UAS and their potential to impact privacy, the author first went to the website for the National Conference of State Legislatures[23] (NCSL). This site lists and tracks by each year (from 2013-2019), all state legislatures who introduce UAS law, and each of them that end up enacting UAS laws. A review of all state level UAS laws *introduced* that pertain to privacy is beyond the scope of this Chapter. Particular attention will be paid to those laws that address privacy concerns in all 50 states. The following is a list of state laws concerning UAS and their impact on privacy or the Fourth Amendment, and their summaries. (National Conference of State Legislatures, 2020)

Table 1. State Laws and Resolutions pertaining to UASs, their administration and Wildlife (National Conference of State Legislatures, 2020)

Year	DEFINE WHAT A DRONE IS	CREATE A STATE REGISTRY	CREATE AN ADVISORY BOARD OR PRIMARY OFFICE OF RESPONSIBILITY FOR UAS	RECOGNIZE THE IMPORTANCE OF DRONE TECHNOLOGY AND POTENTIAL ECONOMIC BENEFIT	ADDRESSES DRONES IN RELATION TO HUNTING AND/OR FISHING
2013 Laws	FL ID IL MT OR	OR	IL NC OR TX VA		IL
2014 Resolutions			AK IN TX	AL CA GA ID MI ND NV	
2014 Laws	NC OH		IN IA NC OH UT		NC TN
2015 Laws	NV OR	NV	IL MD NC		MI NH OR WV
2016 Laws	OR	CA	AK GA IL KS MI ND		IN WI
2017 Resolutions			AK ND UT		
2017 Laws	GA IN LA NC SD WY		CO WY		MN
2018 Laws	KY SD	WV	SC VA		WV
2019 Laws		OR	NV NJ NC OH	AK WA	

Table Footnote 1-Virginia was the first state to pass a piece of UAS legislation, with the passing of HB2012. This defined what a UAS legally is.

The Table 1 above contains a list of all the state UAS laws and resolutions which pertain to the administration of UASs, with a final column showing the states with laws concerning the use, or prohibition of use, of hunting and fishing with UASs. The inclusion of the laws pertaining to UAS affecting the privacy of hunters/fishers or the rules pertaining to using UAS while hunting and fishing demonstrates a unique look at the priorities of state legislatures as the introduction of UAS technology is growing. The table listed below is a look at which states addressed UAS and their

impacts on personal privacy, either through their physical presence or the data they collect.

Table 2. State Laws and Resolutions pertaining to UAS, their impacts on law enforcement, personal privacy, and wildlife (National Conference of State Legislatures, 2020)

Year	CONCERNING USE BY LAW ENFORCEMENT AND WARRANT REQUIREMENTS	PUTS A DATA COLLECTION, RETENTION AND DESTRUCTION POLICY IN PLACE	MAKES IT ILLEGAL TO HACK INTO OR ELECTRONICALLY DISRUPT PUBLIC DRONES	ADDRESSES LANDOWNER PROTECTION	DIRECTLY ADDRESSES PRIVACY ISSUES AND/OR VOYEURISM CRIMES	ADDRESSES DRONES IN RELATION TO HUNTING AND/OR FISHING
2013 Laws	FL ID IL MT NC OR TN TX VA!	IL	OR	OR	TX	IL
2014 Resolutions						
2014 Laws	AK IL IN IA NC UT WI	AK IL UT		LA NC TN UT WI	IN LA NC UT WI	NC TN
2015 Laws	MA NV ND UT VA			CA FL	AR CA FL	MI NH OR WV
2016 Laws	IN OR VT			CA MI	KS CA MI	IN WI
2017 Resolutions						
2017 Laws	OR UT	UT		IN KY NJ OR SD UT VA WY	IN NJ SD UT VA	MN
2018 Laws	KY			DE LA WV WI	DE LA PA WV	WV
2019 Laws	VA			IN	DE IN TN	

Due to the ever-changing landscape of laws and resolutions at the

state level, a second source listing these laws was used. Automated Unmanned Vehicle Systems International (AUVSI) maintains a site of state and local laws that affect UASs, autonomous ground vehicles and unmanned maritime vehicles. (AUVSI Advocacy, 2020) The information on the AUVSI website was reviewed and found to be more comprehensive, as in there were UAS and robotic bills found on this site, but all bills found on the NCSL were verified on the AUVSI site.

Federal and State Laws Pertaining to Privacy and UAS After CoViD-19

Since the CoViD-19 pandemic's dominance of societies attention, the methods and instruments used by society to deal with and attempt to contain the disease have not only been addressed by each citizen, but our federal legislative and regulatory bodies as well. The FAA was quick to realize the constraints their regulations were placing on the UAS industry in the name of safety, were needlessly preventing the potential of UASs to be a key tool in the fight against the virus. With this realization, the FAA was quick[24] to put out extensions on any knowledge requirements with the SFAR. The biggest changes made by the FAA to help get UASs into the fight against CoViD-19 has been an effort to quickly return approved waiver requests for BVLOS flight, night flight, and other requests by UAS operators and pilots.

There have been 58 State Law concerning UASs proposed so far this year with only one of them being directly contributed to the CoViD-19 pandemic. (National Conference of State Legislatures, 2020) The number of UAS laws to actually be enacted by states so far this year is only 6. Below is a chart to show the status and topics of state UAS laws pertaining to privacy. For consistency of method, the author made note of how many states continue to address UASs being used in hunting or fishing.

Table 3. Status of 2020 State UAS Legislation (Governing.com, 2020)

Table Footnote 1-New York was the first state to draft UAS & CoViD-19 specific related legislation[25]

Status of 2020 State Drone Legislation	CONCERNING USE BY LAW ENFORCEMENT AND WARRANT REQUIREMENTS	PUTS A DATA COLLECTION, RETENTION AND DESTRUCTION POLICY IN PLACE	MAKES IT ILLEGAL TO HACK INTO OR ELECTRONICALLY DISRUPT PUBLIC DRONES	ADDRESSES LANDOWNER PROTECTION	DIRECTLY ADDRESSES PRIVACY ISSUES AND/OR VOYEURISM CRIMES	ADDRESSES DRONES IN RELATION TO HUNTING AND/OR FISHING
Enacted into Law	ID	CT		SD ID	SD ID	SD
Passed 2nd Chamber						
Passed 1st Chamber	OK			OK ME	OK ME	
Out of Committee	MA MN	MA MN		AL MA	AL MA	
Introduced or Pre-Filed	VT TN NJ IL NY			NJ ID OH	NJ ID NY[1] OH	WV

Conclusions

UASs are becoming more prevalent in American society and the industry is expected to grow exponentially once BVLOS commercial flights become a reality. In July 2020, it was reported the use of the Low Altitude Authorization and Notification Capability (LAANC) has significantly increased in so far in 2020. In the first 6 months of 2020, a third of the 320,000 LAANC authorizations (it's been operating since Oct 2017) were submitted by UAS operators and granted by the FAA. (McNabb, LAANC Use Accelerates: Kittyhawk Reports All-Time Record Levels of Activity, 2020) Further evidence of increased UAS activity during the pandemic, the numbers of FAA registered UASs and certified pilots continues to grow. On 10 March 2020 we checked the numbers on the FAA's "UAS By the Numbers"

website. We checked the site again on 28 July 2020. Only 138 days have passed.

FAA.GOV	Drones by the #s 10 Mar 20	Drones by the #s 28 Jul 20	Δ
Drones Registered	1,563,263	1,668,243	104,980
Commercial Drones	441,709	479,902	38,193
Recreational Drones	1,117,900	1,184,839	66,939
Remote Pilots Certified	171,744	186,292	14,548

Table 4. Registered UAS & Certified Pilot growth during the 2nd quarter of 2020 Invalid source specified.Invalid source specified.

With healthy growth of the UAS industry even during the CoViD-19 pandemic, the importance of understanding how UASs will affect the Fourth Amendment and the privacy rights attached to it are even more important. Since the beginning of the pandemic there have been multiple nations around the world using UASs in their fight against the CoViD-19 virus. (Chen, 2020) Some appear to be using the pandemic to push forward their own desires to increase their surveillance state. (Maynes, 2020) Americans see these situations and naturally fear UASs and their capabilities will facilitate a similar environment here. (Tuccille, 2020) During the chapter, we have reviewed an immense amount of material to study concerns about UAS and their effects on our privacy laws. Many of these references have shared deep concerns UASs *will* impact our privacy and Fourth Amendment protections. Dissenting views were more difficult to come by but made strong focused arguments our current laws are sufficient for the current level of technology used by UAS. (Sella-Villa, Drones and Data: A Limited Impact on Privacy, 2020)

As pointed out previously, the changes to UAS laws so far during the pandemic have largely been administrative. Without the blanket approval of BVLOS flights, night flights, or commercial freight licenses, there hasn't been an overwhelming number of UAS taking

to the sky and therefore there has been no need for knee-jerk reactions by the Congress or the state legislatures.

The slow and fairly methodical spread and management of UAS delivery introduction appears to be exactly what is necessary for the current environment. The FAA's focus on safety and free efficient economic mobility in the U.S. NAS, while leaving the issues of law enforcement use, zoning, and privacy to be governed by that state and local authorities (FAA, 2018) appears to be the best mix of Federal oversight and Federalist control for the UAS industry, *at the moment*. This patchwork approach has been proven for other transportation focused industries such as the automobile industry and maritime industry. We shall see of this remains true for UAS.

Student Questions

1. What has been the impact, if any at all, of the CoViD-19 pandemic related regulatory changes to increase UAS use during the U.S.'s pandemic response?
2. Do these changes create an environment where UAS and their payloads can further infringe upon or hamper individuals Fourth Amendment rights?
3. Can you name benchmarked and precedence establishing court cases concerning UAS and the technologies used in their payloads?
4. What situations can you see where privacy and Fourth Amendment rights can be endangered or negated by UAS and their payloads?
5. When it pertains to privacy and UAS, do you think a national approach to regulation, or a Federalist approach is better for the UAS industry? For public privacy protections? For advancing and protecting both?
6. Were your answers to the previous question different? Why?

References

(NASIC), N. A. (2019, July 19). Emerging IADS Threats: Talking Points. *DoD Periodical*.

112 Congress. (2012, February 14). The FAA Modernization and Reform Act of 2012. *H.R. 658*. Washington D.C., United States.

49 U.S. Code §40103. Sovereignty and use of airspace. (1994, July 5). Retrieved July 2020, from law.cornell.edu: https://www.law.cornell.edu/uscode/text/49/40103

Al-Naji, A. P. (2017). Remote monitoring of cardiorespiratory signals from a hovering unmanned aerial vehicle. *Al-Naji, A., Perera, A. G., & Chahl, J. (2017). Remote monitoring of cardiorespiratory siBiomedical Engineering Online*, 16(1). doi: https://doi.org/10.1186/s12938-017-0395-y

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

Association for Unmanned Vehicle Systems International. (2018, September 26). *Summary of UAS Provisions in H.R. 302*. Retrieved April 2020, from auvsilink.org: http://auvsilink.org/AUVSIDocs/AUVSI%20Summary%20of%20HR%20302.pdf

AUVSI Advocacy. (2020, July). *2020 State Legislation Map*. Retrieved July 2020, from cqrcengage.com: https://cqrcengage.com/auvsi/statelegmap

1. Skorup & Haaland, C. (2020, March 1). *Which States Are Prepared for the Drone Industry? A 50-State Report Card. Mercatus Center.* Retrieved from https://www.mercatus.org/: https://www.mercatus.org/system/files/skorup-drone-report-card-mercatus-summary-v1_1.pdf

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/

Bomboy, S. (2014, February 7). A *legal victory for drones warrants a Fourth Amendment discussion.* Retrieved from news.yahoo.com: https://news.yahoo.com/legal-victory-drones-warrants-fourth-amendment-discussion-105607148.html

Bonifacic, I. (2020, April 27). *UPS will use drones to deliver prescriptions to retirees in Florida.* Retrieved May 2020, from engadget.com: https://www.engadget.com/ups-will-use-drones-to-deliver-prescriptions-to-retirees-in-flordia-171337603.html

Breitenbach, S. (2015, September 10). *States Rush to Regulate Drones Ahead of Federal Guidelines.* Retrieved July 2020, from pewtrusts.org: https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2015/09/10/states-rush-to-regulate-drones-ahead-of-federal-guidelines

Busch, K. a. (2016, February 09). No Denial: How NATO Can Deter Creeping Russian Threat. *www.cer.org.uk/insights* .

Chen, C. (2020, April 9). *Drone-maker DJI rubbishes reports of mass layoffs, says it is busy meeting demand amid pandemic.* Retrieved April 2020, from scmp.com: https://www.scmp.com/tech/gear/article/3079211/drone-maker-dji-rubbishes-reports-mass-layoffs-says-it-busy-meeting

Cuddington, J. (2015). Intelligence Operations in Denied Area. *At Home and Abroad: Thinking Through Conflicts and Conundrums* .

Cuddington, Jeff. (2016, January). Opinion: Need of the Hour: New Intelligence .

Davis, H. (2020, July 28). *Texas stadiums helping fight coronavirus with disinfectant-spraying drones.* Retrieved August 2020, from foxnews.com: https://www.foxnews.com/sports/coronavirus-texas-stadiums-disinfectant-spraying-drones

de León, R. (2020, May 27). *Zipline, Novant Health launch the*

first long-distance emergency drone operation in U.S. to deliver PPE and medical supplies. Retrieved July 2020, from cnbc.com: https://www.cnbc.com/2020/05/27/zipline-novant-health-launch-us-drone-service-to-fight-pandemic.html

Defense, O. o. (2006). Annual Report to Congress: Military Power of the Peoples Republic of China . *US DoD* , pp. 21, 25. .

Diab, A. (2014, November 13). *Drones perform the dull, dirty, or dangerous work*. Retrieved from tech.co/news/drones-dull-dirty-dangerous-2014-11: https://tech.co/news/drones-dull-dirty-dangerous-2014-11#:~:text=Drones%20perform%20tasks%20generally%20categorized%20into%20the%20%22three,Often%2C%20the%20mission%20c

Dictionary.com. (2020). *Jurisprudence*. Retrieved August 2020, from Dictionary.com: https://www.dictionary.com/browse/jurisprudence

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

Dwyer-Moss, J. (2018). The Sky Police: Drones and the Fourth Amendment. *Albany Law Review*, Vol81_3/1047. Retrieved from Dwyer-Moss, J. (2018). The Sky Police: Drones and the Fourth Amendment. Albany Law Review. https://www.albanylawreview.org/Articles/Vol81_3/1047%20Dwyer-Moss%20PRODUCTION.pdf.

Dwyer-Moss, J. (2020). *Jessica Dwyer-Moss' Profile*. Retrieved July 2020, from LinkedIn.com: https://www.linkedin.com/in/jessicadwyermoss/

FAA. (2015, December 17). *State and Local Regulation of Unmanned Aircraft Systems (UAS) Fact Sheet*. Retrieved July 2020, from FAA.gov: https://www.faa.gov/uas/resources/policy_library/media/UAS_Fact_Sheet_Final.pdf

FAA. (2018, July 20). *Press Release – FAA Statement–Federal vs. Local Drone Authority*. Retrieved July 2020, from FAA.gov:

https://www.faa.gov/news/press_releases/
news_story.cfm?newsId=22938

FAA. (2018, July 20). *Press Release – FAA Statement–Federal vs. Local Drone Authority*. Retrieved June 2020, from faa.gov: https://www.faa.gov/news/press_releases/
news_story.cfm?newsId=22938

FAA. (2020, July 8). *Coronavirus guidance & resources from FAA*. Retrieved from www.FAA.gov: https://www.faa.gov/coronavirus/guidance_resources/

FAA. (2020, April 16). *Regulatory updates due to coronavirus*. Retrieved from www.faa.gov/coronavirus/regulatory_updates/: https://www.faa.gov/coronavirus/regulatory_updates/

Freier, N. (2012). The Emerging Anti-Access/ Area Denial Challenge. *Center for Strategic and International Studies* .

Governing.com. (2020, July 23). *Drone Legislation Map*. Retrieved July 2020, from Governing.com: https://www.governing.com/next/Legislative-Watch-The-Rise-of-Drones-During-the-Pandemic.html

Hayden, J. (2020, May 19). *Why the Drone Community Should Not Embrace Exclusive FAA Control of Drone Regulations*. Retrieved May 2020, from DroneLife.com: https://dronelife.com/2020/05/19/faa-and-drone-regulation-should-the-faa-have-excusive-control/

Kaminski, M. E. (2013, April 26). *Drone Federalism: Civilian Drones and the Things They Carry*. Retrieved July 2020, from SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2257080

Maynes, C. (2020, May 06). *Behind Russia's Coronavirus Fight, a Surveillance State Blooms*. Retrieved May 2020, from voanews.com: https://www.voanews.com/europe/behind-russias-coronavirus-fight-surveillance-state-blooms

McNabb, M. (2020, July 15). *LAANC Use Accelerates: Kittyhawk Reports All-Time Record Levels of Activity*. Retrieved July 2020, from dronelife.com: https://dronelife.com/2020/07/15/laanc-use/

McNabb, M. (2020, July 14). *Matternet and UPS Expand Hospital Delivery Network*. Retrieved 2020 July, from dronelife.com:

https://dronelife.com/2020/07/14/matternet-and-ups-expand-hospital-delivery-network/

National Conference of State Legislatures. (2020, April 1). *Current Unmanned Aircraft State Law Landscape*. Retrieved June 2020, from ncsl.org: https://www.ncsl.org/research/transportation/current-unmanned-aircraft-state-law-landscape.aspx

Obama, B. (2015, February 15). *Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems.* Retrieved April 2020, from hsdl.org: https://www.hsdl.org/?view&did=762711

Orwell, G. (1949). *Nineteen Eighty Four: A Novel.* United Kingdom: Secker & Warburg.

Posen, B. (2003). Command of the Commons: The Military Foundation of US Hedgemony. *International Security, Vol 28, No1.* , pp. 5-46 .

Rouse, C. (2016, December). *What is disruptive technology? – Definition from WhatIs.com.* Retrieved from WhatIs.com: https://whatis.techtarget.com/definition/disruptive-technology#:~:text=A%20disruptive%20technology%20is%20one%20that%20displaces%20an,Clayton%20M.%20Chris

Rupprecht, J. (2020, June 4). *Ultimate Guide to Drone Laws [2020] Written by a Lawyer.* Retrieved from jrupprechtlaw.com/drone-laws/: https://jrupprechtlaw.com/drone-laws/

Rupprecht, J. (n.d.). *Drone Legislation Directory.* Retrieved June 2020, from jrupprechtlaw.com: https://jrupprechtlaw.com/drone-legislation/

Seeking Alpha. (2019, January 22). *Robotics: Unmanned Traffic Management (UTM) Systems Outlook.* Retrieved April 2020, from seekingalpha.com: https://seekingalpha.com/article/4234878-robotics-unmanned-traffic-management-utm-systems-outlook

Sella-Villa, D. (2020, July 24). *David Sella-Villa's Profile page.* Retrieved July 2020, from LinkedIn: https://www.linkedin.com/in/dsellavilla/

Sella-Villa, D. (2020, January 30). Drones and Data: A Limited Impact on Privacy. *University of Richmond Law Review, Forthcoming*.

Smentkowski, B. P. (2020, July 12). *Fourth Amendment*. Retrieved from www.britannica.com/topic/Fourth-Amendment: https://www.britannica.com/topic/Fourth-Amendment#:~:text=Fourth%20Amendment%2C%20amendment%20%281791%29%20to%20the%20Constitution%20of,the%20text%20of%20the%20Fourth%20Amendment%2C%20see%20b

Smith, C. (2020, April 3). *Legislative Watch: The Rise of Drones During the Pandemic*. Retrieved April 2020, from governing.com: https://www.governing.com/next/Legislative-Watch-The-Rise-of-Drones-During-the-Pandemic.html

Smith, R. E. (2017, May). Drones and the Fourth Amendment. *Privacy Journal*, 5-7.

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

Summers, N. (2020, May 26). *Drone deliveries are making their case in a crisis*. Retrieved June 2020, from engadget.com: https://www.engadget.com/drone-wing-zipline-matternet-everdrone-coronavirus-133021691.html

Taleb, N. N. (2007). *The Black Swan: The Impact of the Highly Improbable*. Random House.

Thompson II, R. M. (2013). *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses.* United States Congress. Washington D.c: Congressional Research Service.

Thompson II, R. M. (2014). *The Fourth Amendment Third-Party Doctrine.* United States Congress. Washington D.C.: Congressional Research Service.

Thompson II, R. M. (2015). *Domestic Drones and Privacy: A Primer.* United States Congress. Washington D.C.: Congressional Research Service.

Tuccille, J. (2020, April 10). *The Surveillance State Thrives During the Pandemic*. Retrieved July 2020, from reason.com: https://reason.com/2020/04/10/the-surveillance-state-thrives-during-the-pandemic/

U.S. Senate. (2016). *FAA Extension: Safety, Security, Stability*. Retrieved July 2020, from commerce.senate.gov: https://www.commerce.senate.gov/services/files/f0ed7c52-f6aa-4bb7-86a4-562a5e468253

United States v. Jones (U.S. 400 2012).

US Department of Defense. (2013, May). Air Sea Battle: Service Collaboration to Address Anti Access Area Denial Challenges. *DoD Periodical*.

Weise, E. (2015, September 10). *California governor vetoes drone bill*. (Gannett Satellite Information Network, LLC) Retrieved Aug 2020, from usatoday.com: https://www.usatoday.com/story/tech/2015/09/10/california-drones-veto-governor-jerry-brown-news-photographers/71987132/

Zoldi, D. M. (2020, July 10). *Crawl, Walk, Run, Fly! – Urban Traffic Milestones*. (L. Autonomous Media, Producer) Retrieved July 2020, from insideunmannedsystems.com: https://insideunmannedsystems.com/crawl-walk-run-fly-urban-traffic-milestones/

11. Chapter 11 UV & Disinformation / Misinformation Channels [Ryan]

Preamble

Much of this book is devoted to technology and its application within specific domains. This chapter will explore the use of unmanned vehicles as conduits of information and the varying purposes to which those conduits can be put.

Student learning objectives

After reading this chapter, students should be able to do the following:

1. Describe the components of communications
2. Define misinformation and disinformation
3. Describe the types of problems that can result from deceptive information in automated systems.

The Ruses of War

The concepts of misinformation and disinformation come from the practices of adversarial competition. In fact, they are only useful in adversarial competition. In collaborative endeavors, misinformation and disinformation can be not only problematic but downright dangerous. Think about a team of medical professionals working together to perform a surgery, or a team of operators working with remote unmanned systems to execute a mission. Any problems with the clarity and common understanding of information could be disastrous. When working with another party

towards a common goal, it is paramount that all parties understand the goal, the steps, and the strategies clearly. Any mistakes in information, whether originating from the sender or by faults in the transmission or misinterpretation by the receiver, causes friction in relationships. That friction slows down the effectiveness and speed of collaboration, because clarification must be sought, sometimes multiple times. A savvy competitor uses such friction to gain an advantage. An aggressive competitor creates and promulgates such friction to undermine and damage abilities to interpret, analyze, and strategize.

In competition, it is sometimes useful to increase the friction rather than decrease it. As the Earl of Chesterfield observed in 1749, "without some dissimulation, no business can be carried on at all." (Breuer, 2001, p. viii) In warfare, the practice falls under a category known variously as stratagem, deception, diversion, ruse, or camouflage (Whaley, 2007). Disinformation can be considered as "the most important single broad category of ruses … fed into another's information system in order to deceive him" (Whaley, 2007, p. 8). The practice of disinformation has spanned all of history (Breuer, 2001) (Whaley, 2007) and has been observed in the animal kingdom as well (King, 2019). As noted by Breuer (2001), "force and fraud have been the two cardinal principles of warfare since Sun Tzu, the Chinese warlord who conquered huge expanses of Asia, recorded his military theories in 550 BCE: 'undermine the enemy, bewilder and confuse him, strike at his morale, then his army will fall to you.'" (Breuer, p. 1) As such, it is prudent to understand both effective communication and how that process can be subverted or perverted.

Understanding Effective Communication

In order to understand the subversion of communication, it is necessary to understand what communication is and what distinguishes effective communication. There have been many, many, many tomes written on effective communication, but for the purposes of this discussion, we will focus on the complexities

of communicating from person to person through the lenses of effective listening techniques and a model of communicative elements.

The Elements of Communications

There are several different elements of communication that are important to understand. The most common way of referring to these elements is as 'signal' and 'noise'. However, that type of nomenclature obscures the subtleties associated with deception. For the purposes of this discussion, the 'signal' is described in four categories while 'noise' is treated through two categories.

First, there is information that is both relevant and truthful. An example of this could be a fire alarm that correctly alerts a home owner to a fire in the home while he is home. It would be less relevant if the homeowner were away and unable to respond to the matter.

Next, there is information that is truthful but irrelevant. For example, if a person interrupted a business meeting to inform everyone present that two people in the grocery store were seen arguing, that would be truthful but highly irrelevant to the business meeting. It is a distraction.

Following that, there is information that is relevant but false or misleading. An example of this could be a lie about a situation or manipulated media that presents a situation differently than what really happened.

Finally, there is information that is irrelevant and false or misleading. An example of this might be casual gossip that spreads an untrue rumor.

Technical problems in the communications channel, such as static or blurred focus, are distinguishable from the previous categories and deserve a separate discussion. While technical problems are neither true nor false, they do impede the effectiveness of communications. Further, they may be caused by either

circumstances (weather, faulty equipment, or user error) or by malicious activity (jamming, sabotages, or computer exploit).

Note that there are 4 components that are undesirable. We can simplify by referring to them as misinformation and disinformation, thusly:

- Misinformation is the general term for information that is one of the following types:
    - o Truthful but irrelevant information
    - o Irrelevant and false or misleading
    - o Technical problems in the communications channel, such as static or blurred focus, are distinguishable from the previous categories and deserve a separate discussion.
- Disinformation is the general term for information that is relevant but false or misleading.

The challenge to the consumer of information is, therefore, threefold:

- Figure out what is truthful information;
- Judge the relevancy of the information; and
- Minimize the occurrence of technical problems.

Figuring out either truthfulness or relevance of communications is not always as easy as it should be. There are charlatans who publish fraudulent data, there are idea thieves who publish plagiarized material, and there are simpletons who publish what they think is good but which suffers from inherent flaws in logic or methodology. Some publishers exert little control over the quality of material. As a result, there is a span of quality in the published literature that ranges from extremely reliable to extremely questionable.[i]

The increasing automation of information collection, interpretation, and fusion makes the challenge even greater:

As dependence on information increases due to the automation

of more and more elements in the surrounding environment, the ability of the warfighter to judge the reliability and accuracy of information content becomes more important. There are two aspects to this challenge:

- Judging relative truth: being able to comprehend the inherent inaccuracies in data that exist due to model uncertainty, source inaccuracies, and so on; and
- Judging continued truth: being able to determine whether the information being considered has been tampered with, replaced, or otherwise interfered with.

The significant technical challenges in both of these aspects range from human interface issues to confidentiality measures. In responding to these challenges, complex information display techniques, such as virtual reality applications, will clearly have some level of payoff. As capabilities for injecting falsehoods into otherwise truthful data continue to be developed, the challenge of determining continued truthfulness will be exponentially greater, particularly in light of the automated fusion capabilities that are being relied on to assist humans in handling the huge amounts of available data in a timely manner.
(Panel on Information in Warfare, 1997, pp. 81-82)

A Simple Model of Communications

For information to be communicated from one entity to another, there is a surprisingly complex set of requirements. Think about communications between a person and a pet, or between two dogs meeting for the first time in the park, or between two people who speak different languages. The goal of communications is to transfer information from one entity to another. Let's look at what this entails.

First, the entity originating the message must have some way

of encapsulating the information into the message. This can be done with facial expressions, body language, words, music, and even pheromones.

Next, the originator must have some way of transferring the message to the recipient. This can be done by various ways, depending on how the information is encapsulated. One simple way of transferring the message would be to simply place oneself in the visual range of the recipient and make sure that the recipient is looking and paying attention. Another way would be to speak within auditory range of the recipient. Crucially, the actual transmission a message requires some level of cooperation by the recipient. In other words, the actions of the originator are necessary but not sufficient.

The cooperation of the originator and the recipient are also not sufficient. For communication to occur, the information must be in a form that is understandable by both parties. The pet must understand what the person means by a specific hand gesture or a specific command. Two people talking must have a common language interpretation. Simply speaking the same language is not enough: the dialects and common usage patterns matter as well.

To illustrate this point, consider this anecdote of a person from Australia visiting some American colleagues. Obviously, they shared English as a common language and communication was seemingly problem-free. The Americans, as part of their hospitality, took the Australian to a baseball game. As is customary in the United States, the song "Take Me Out to the Ballgame" was sung with great gusto by the fans in the stadium. The Australian was taking this all-in stride until the song got to the part about "Let me root, root, root for the home team…", at which point in time a shocked look took over his face. The Americans, noticing this, asked him if he was feeling okay. He then explained how the word "root" was used in Australia, which is as an offensive and vulgar reference to sexual intercourse (O'Shea, 2016). So when the Australian heard an entire stadium of people singing happily about rooting for the home team, he was somewhat taken aback.

The simple model of communications is, therefore, this: an originator forms and encapsulates information into a message medium, which is received and interpreted by a recipient. The effectiveness of the communication is dependent upon the shared knowledge of the originator and the recipient. It is also dependent on several elements that the originator and the recipient may have little to no control over: interference in the environment, in the signal formation, in the signal reception, or in the context. The originator might sneeze while talking, a car backfire might drown out a few words, or the context of the conversation may lead the recipient to misinterpret the intended meaning. In order to reduce the probability of misinterpretation or misunderstanding, active strategies can be adopted, including repeating messages through multiple channels or saying the same thing in many different ways. Crucially, these active measures to reduce misunderstandings are generally dependent upon cooperation between the originator and the recipient.

Effective Listening

There is an entire philosophy about how to reduce misunderstandings in human communication that illustrates this process. The philosophy is called Active Listening (Rogers & Farson, 1957) and it's actually interesting to consider through the lens of "what can go wrong" in communications. Since the entire point of disinformation and misinformation is to cause problems in communication, it's worth taking a moment to reflect on how life coaches teach active listening as a way to make things go right.

To practice active listening, six skills are emphasized. These skills are used to enable a "listener to thoroughly absorb, understand, respond, and retain what is being said." (Center for Creative Leadership, 2019) Each of the skills identifies some element of communication that can improve the effectiveness of

communication but also identify targets for a disinformation campaign. These six skills are:

- *Paying attention*
- *Withholding judgment*
- *Reflecting*
- *Clarifying*
- *Summarizing*
- *Sharing* (Center for Creative Leadership, 2019)

Paying attention is exactly what it sounds like: actually listening to what a speaker is saying. But it is also paying attention to what the speaker is conveying through other aspects: tone of voice, volume, pauses, emphasis, word choices, body language, and other elements of the conversation.

Withholding judgment is meant to imply keeping an open mind but a more sophisticated interpretation of this skill is developing an understanding of what the person speaking is actually trying to communicate, taking into account that person's culture, language skill, opinions, and purpose. By integrating the spoken message into an appreciation of where the person is coming from, a listener develops a better platform for productive conversation.

Reflecting is the process of repeating what you think you have heard in other words, with the purpose being to confirm that you have received the correct message. If your paraphrase of what you think you have heard is rejected, then you know that there has been some breakdown in the communication effort.

Clarifying the message is done through asking questions, either to ensure you have interpreted the context of the conversation correctly or to request amplifying information. By asking questions, you give the speaker a chance to expand a topic to contextualize it better or to explain something that may be slightly ambiguous. Using reflection and clarification iteratively can be a powerful method for getting the speaker to be more descriptive and precise.

Similarly, summarizing the message briefly back to the speaker

can test your comprehension of the conversation, particularly the sensitive elements. Once you have established that your understanding is correct, then you have the ability to share some of your own thoughts and insights.

The purpose of describing the processes associated with active listening is to underscore how very complex the act of communication is. Communication consists not just of the information contained in the transmitted message; it also includes all the noise and extraneous information in the communication channel, including the brains of the communicators.

Deception As A Strategy

When one has perfect knowledge, one can choose the timing of actions and go fast or slow as appropriate to the situation and to the goals of action. Perfect knowledge of any situation is the product of communication: collecting, analyzing, and interpreting messages that are both deliberately and inadvertently sent by an adversary. In the real world, achieving perfect knowledge is both desired and impossible: there is too much information, variation and change, and deception.

Deception is used to deny perfect knowledge, to seed confusion into intelligence, and to mislead adversaries, which ultimately slows them down, from an effectiveness perspective. Effective deception can result from hiding information, changing information, and seeding information. Some examples of the use of deception include the following:

- In the early 1960s, the Walt Disney Productions company used a series of companies to buy the land around Orlando that became the site for Disney World. These companies were created specifically for the purpose of shielding the true identity of the purchaser in order to keep land prices from rising, which surely would have happened if people had known the truth about who was buying the land and for what purpose. In fact, when the news broke, "land prices skyrocketed in Orlando, where in some cases the land went up to $80,000 an

acre" (Ganninger, 2020).

- In 1944, as the planning for the Allied invasion of Normandy was increasing in intensity, an actor playing the part of Field Marshall Montgomery was taken to alternative locations in order to deceive the Germans as to where the invasion would take place. This was only one of the many deceptions associated with Operation Overlord, but an effective one as it distracted the Axis powers with information that "Montgomery" had been observed in Gibraltar and North Africa, leading them to speculate that the invasion would be in the Mediterranean region. (Breuer, 2001, pp. 198-202) (Whaley, 2007, p. 376) (Howard, 1995, p. 125)
- During the Cold War, agents of the Soviet Union used the tactic of injecting false news reports into media. One example of this type of activity was included in a 1981 US Department of State advisory:
  "In 1980, Pierre-Charles Pathe, a French Journalist, was convicted for acting as a Soviet agent of influence since 1959. His articles – all subtly pushing the Soviet line on a wide range of international issues – were published in a number of important newspapers and journals, sometimes under the pseudonym of Charles Morand. The journalist also published a private newsletter which was regularly sent to many newspapers, members of parliament, and a number of foreign embassies. The Soviets used Pathe over a number of years to try to influence the attitudes of the prominent subscribers to his newsletter and to exploit his broad personal contacts." (U.S. Department of State, 1981)

Deception is a technique that can be reasonably low cost as well as effective. Deception includes many ruses, such as camouflage, diversions, and disinformation (Whaley, 2007, p. 7). Barton Whaley, a scholar of deception and military successes over the century, noted in his seminal book *Stratagem: Deception and Surprise in War* (2007):

The most important single broad category of ruses includes all false information fed into another's information system in order to deceive him. The standard technical term is "disinformation". It is conventionally meant to cover only the verbal or written forms of information, leaving "camouflage" and "diversion" to cover the nonverbal or visual forms. (pp. 8-9)

He made this assessment of the importance of disinformation from his painstaking analysis of the effects of surprise in warfare over history. A key analytical finding from his scholarship:

Of the 61 cases of strategic military surprise that occurred between 1914 and 1968, no more than 4 can be exclusively or even mainly attributed to the initiator's passive security. More or less specific warning signals almost inevitably filter through the security screen and reach the intended victim. Moreover, these warning usually increase in frequency and specificity as the attacker's preparations unfold, drawing more and more indiscrete persons into the planning and making ever more visible the necessary adjustments in mobilizations, deployment, logistics, and perhaps diplomacy. … There is only one type of activity still available that will multiply [the commander's] chances of gaining surprise. That is stratagem. (Whaley, 2007, pp. 1-2)

In this quotation, the word stratagem in its classic meaning, which is as a reference to strategic deception.

The world that he studied is not the world of today. The growth and integration of information technologies is a dramatic change that has affected all aspects of life. Further, the types and representations of information has increased exponentially, to the point where it makes less sense to separate non-verbal and visual information from written or spoken information. The growth of augmented and virtual reality (AR and VR) applications, the widespread adoption of artificial intelligence implementations, and the integration of video, photography, data, and sound has changed the environment of deception activities. As such, the discussion in this chapter includes manipulation of non-verbal and visual information in the definition of deception.

Implications for Unmanned Systems

Unmanned systems rely on information technology. As noted in Chapter 1 of this book:

The separation of human labor, cognition, and equipment into disparate pieces means that a concomitant need for collaborative technologies becomes important. The most obvious collaborative technologies are communications – exchanging data, commands, and responses. Other types of collaborative technologies that need to be considered are those that prevent adverse interactions between system components, environmental sensing and reaction technologies, and control guidance technologies. All of these enable the remote operation of an unmanned system.

In other words, communication between the various components are a critical part of unmanned system operations. It is therefore necessary for operators to plan for identifying and mitigating deception. A solid information security regime provides a platform to build upon. Having the people, processes, and technologies in place that protect the integrity of data in storage as well as in transactions is a critical first step.

That first step is, obviously, only a first step. It provides a way of adjudicating information already in the system and that being shared with trusted edge systems. The next steps need to address the deception challenges that come from external data of all types: sensor collected data, aggregated data from a data market, and deliberately introduced deceptive data. Problems to consider include the following:

- Sensors that correctly work as engineered but which are triggered to misread a sensed situation because the target environment has been manipulated. For example, an unmanned car could be tricked into "reading" a road marking because the marking had been augmented with material designed to trick the car's sensor.
- Aggregated data from a data market that is used to create highly detailed virtual reality depictions of a target

environment, in which the data has been seeded with deliberately misleading information, such as multiple altitude power lines in a place where none exist. UAS operations would use that deceptive information to avoid flying in the vicinity of the powerlines, which could reduce the effectiveness of their mission operations.

- Deliberately introduced deceptive data could come from an insider or from a modified infrastructure component. For example, an AI application that quickly processes data inputs to a system could follow a set of rules that leads it to an incorrect decision. That incorrect decision then becomes deceptive data: relevant but misleading or untruthful.

Any approach to addressing the problem of deceptive data will be unique to the operations and mission of the unmanned systems, so a one-size-fits-all solution is not possible. As with every engineering problem, the solution lies in understanding what the threats are, what the potential impacts might be, and what countermeasures can effectively be used.

Sensing and Interpreting Challenges

Because there is no one-size-fits-all solution to the challenge of deceptive data, it is helpful to review some examples of historical events.

"Hidden" Information Embeds

In 2018, researchers experimented with overlaying what they called "adversarial examples" on actual stop signs to see if autonomous vehicle detection systems could be fooled. The overlays used did not change a human's ability to identify the sign as a stop sign: the overlays were smaller than many of the graffiti stickers commonly seen on stop signs in cities. The researchers were able to make the

sensors miss the stop sign. Further, they were able to make the sensor detect things that were not present:

… we create perturbed physical objects that are either ignored or mislabeled by object detection models. We implement a *Disappearance Attack*, in which we cause a Stop sign to "disappear" according to the detector—either by covering the sign with an adversarial Stop sign poster, or by adding adversarial stickers onto the sign. In a video recorded in a controlled lab environment, the state-of-the-art YOLO v2 detector failed to recognize these adversarial Stop signs in over 85% of the video frames. In an outdoor experiment, YOLO was fooled by the poster and sticker attacks in 72.5% and 63.5% of the video frames respectively. We also use Faster R-CNN, a different object detection model, to demonstrate the *transferability* of our adversarial perturbations. The created poster perturbation is able to fool Faster R-CNN in 85.9% of the video frames in a controlled lab environment, and 40.2% of the video frames in an outdoor environment. Finally, we present preliminary results with a new *Creation Attack*, wherein innocuous physical stickers fool a model into detecting nonexistent objects. (Eykholt, et al., 2018)

One can easily understand the potential impact of an unmanned system missing or inventing information: the problems could cascade to the entire system as well as cause harm to external elements, such as people or property.

In another set of experiments, researchers developed a set of eyeglass frames that foiled a facial recognition system. The choice of glasses frames was to minimize the perturbation components while using something that was easy to modify and widely available:

One advantage of facial accessories is that they can be easily implemented. In particular, we use a commodity inkjet printer (Epson XP-830) to print the front plane of the eyeglass frames on glossy paper, which we then affix to actual eyeglass frames when physically realizing attacks. Moreover, facial accessories, such as eyeglasses, help make attacks plausibly deniable, as it is natural for people to wear them. (Sharif, Bhagavatula, Bauer, & Reiter, 2016)

The results were impressive. In all but one experiment, the device worked perfectly. In the one in which it didn't, the device worked 91% of the time. They were able to successfully show that their "eyeglass frames enabled subjects to both dodge recognition and to impersonate others." (Sharif, Bhagavatula, Bauer, & Reiter, 2016)

These two examples represent a rich and growing field of research. As the rush towards full automation for unmanned systems continues, this type of work is both useful for improving the sensing systems and for identifying the types of threats that need to be considered during operations.

Distinguishing Signals in Noisy Environments

In 2013, a group of students conducted an experiment on a 213-foot ship to see if they could successfully change the course of the yacht without the crew noticing. From the top deck of the yacht, they:

broadcasted a faint ensemble of civil GPS signals from their spoofing device a blue box about the size of a briefcase toward the ship's two GPS antennas. The team's counterfeit signals slowly overpowered the authentic GPS signals until they ultimately obtained control of the ship's navigation system.

Unlike GPS signal blocking or jamming, spoofing triggers no alarms on the ship's navigation equipment. To the ship's GPS devices, the team's false signals were indistinguishable from authentic signals, allowing the spoofing attack to happen covertly.

Once control of the ship's navigation system was gained, the team's strategy was to coerce the ship onto a new course using subtle maneuvers that positioned the yacht a few degrees off its original course. Once a location discrepancy was reported by the ship's navigation system, the crew initiated a course correction. In reality, each course correction was setting the ship slightly off its course line. Inside the yacht's command room, an electronic chart showed its progress along a fixed line, but in its wake there was a pronounced curve showing that the ship had turned.

"The ship actually turned and we could all feel it, but the chart display and the crew saw only a straight line," Humphreys said.

After several such maneuvers, the yacht had been tricked into a parallel track hundreds of meters from its intended one the team had successfully spoofed the ship. (Animation by Erik Zumalt, 2013)

This type of attack is not just in the lab. Around the world, there have been increasing reports of navigation problems of varying sorts, all related to the electronic navigation aids in use to make navigation possible through storms, night, and disputed waters. The misuse of the technology has led to some very interesting situations:

Automatic Identification Systems (AIS) are causing problems for mariners transiting waters where there are high concentrations of fishing vessels, particularly in the East China Sea. … Local fisherman discovered that by putting AIS transponders on their fishing nets, large ships would change course for the nets, thinking they were vessels. … If we are to see more unmanned ships in the future, this needs to be rectified. What would an unmanned ship approaching a literal "sea" of AIS targets do without a professional mariner in charge to properly assess the situation? Ships would be changing course to avoid fishing nets, only to be "faced" with a whole new set of AIS targets on the new course. Shipowners may find their unmanned vessels turning circles in order to avoid what the automated equipment deems to be dangerous, but may only be crab pots or fishing buoys. (Kovary, 2018)

Conclusions

These two examples underscore the challenge of sensing and interpreting, particularly in noisy environments where competing interests collide.

References

Animation by Erik Zumalt. (2013, July 30). *Spoofing a Superyacht at Sea.* Retrieved September 3, 2020, from UT Austin News: https://news.utexas.edu/2013/07/30/spoofing-a-superyacht-at-sea/

Breuer, W. B. (2001). *Deceptions of World War II*. New York: John Wiley & Sons, Inc.

Center for Creative Leadership. (2019, August 21). *Use Active Listening to Coach Others*. Retrieved August 25, 2020, from Center for Creative Leadership: https://www.ccl.org/articles/leading-effectively-articles/coaching-others-use-active-listening-skills/

Eykholt, K., Evtimov, I., Fernandes, E., Li, B., Rahmati, A., Tramer, F., . . . Song, D. (2018, October 5). *Physical Adversarial Examples for Object Detectors*. Retrieved September 3, 2020, from ArXiv.org: https://arxiv.org/pdf/1807.07769.pdf

Ganninger, D. (2020, May 2). *How Walt Disney Secretly Bought the Land for Walt Disney World*. Retrieved September 2, 2020, from Medium: https://medium.com/knowledge-stew/how-walt-disney-secretly-bought-the-land-for-walt-disney-world-21d24de723e9

Howard, M. (1995). *Strategic Deception in the Second World War*. London: W.W. Norton & Company.

King, B. J. (2019, September). Deception in the Animal Kingdom: Homo Sapiens is not the only species that lies. *Scientific American*.

Kovary, L. (2018, December 27). *AIS Problems Revealed in East China Sea*. Retrieved September 3, 2020, from gCaptain: https://gcaptain.com/ais-problems-revealed-in-east-china-sea/

O'Shea, R. P. (2016, February 19). *Words Americans should avoid saying to Australasians*. Retrieved September 1, 2020, from Robert P. O'Shea: https://sites.google.com/site/oshearobertp/publications/words-americans-should-avoid-saying-to-australasians

Panel on Information in Warfare. (1997). Information in Warfare. In C. o. Forces, *Technology for the United States Navy and Marine Corps, 2000-2035* (Vol. 3, p. 131). Washington DC: National Academy Press.

Rogers, C. R., & Farson, R. E. (1957). *Active Listening*. Chicago: University of Chicago.

Sharif, M., Bhagavatula, S., Bauer, L., & Reiter, M. K. (2016, October 24). *Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition*. Retrieved September 3, 2020, from SBhagava

papers: https://www.cs.cmu.edu/~sbhagava/papers/face-rec-ccs16.pdf

U.S. Department of State. (1981, October). *Soviet "Active Measures": Forgery, Disinformation, Political Operations.* Retrieved September 2, 2020, from CIA Library Reading Room: https://www.cia.gov/library/readingroom/docs/CIA-RDP84B00049R001303150031-0.pdf

Whaley, B. (2007). *Strategem: Deception and Surprise in War* (Reprint of the 1969 edition ed.). Boston: Artech House.

[i] For an excellent overview of how to approach understanding the believability of published information, see The University of Groningen's "Information literacy – Media Studies: Evaluation criteria: relevance and reliability", found online at https://libguides.rug.nl/c.php?g=560673&p=3857909

PART V

SECTION 5 UV GEOPOLITICAL, MARITIME & LEGAL ADVANCES

12. Chapter 12 Chinese UAS Proliferation along New Silk Road Sea / Land Routes [Carter]

Student Learning Objectives

Upon completion of this chapter, students should be able to:

1. Explain the sectors of the Belt and Road Initiative that impact unmanned technology
2. Understand the importance and impact of the relationship between China and the Middle East
3. Explain the Blue Ocean Information Network
4. Identify factors of the Digital Silk Road that impact them directly

Progression of Belt and Road Initiative (BRI) Partnerships

The Belt and Road Initiative (BRI) was launch as part of the Constitution of the People's Republic of China in 2013. Partnerships among China and other countries continue increase by engaging through economic and diplomatic means. The target completion date for BRI is 2049, the anniversary of the founding of People's Republic of China. For lower income countries, the enticement of low-interest loans and support to build infrastructure is part of the attraction to a relationship with China. Current events of Brexit and a spilt United States political infrastructure have played into China's goal of becoming a global superpower. As the U.K. and the

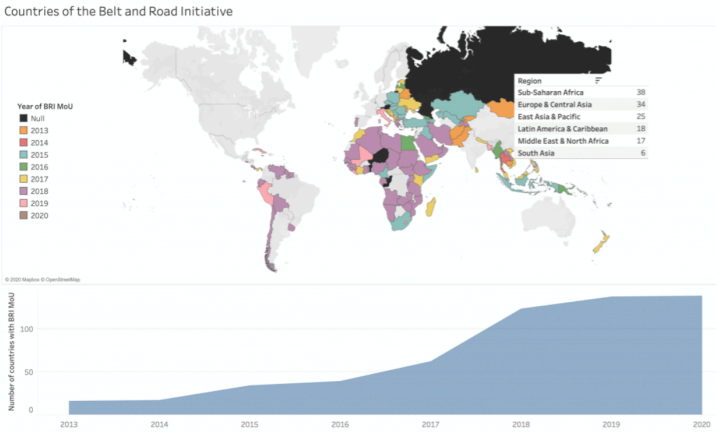
U.S. appear to be in consistent conflict with itself and other nations, China's façade to help countries through loans, technology, infrastructure without personal gain grows. Partnerships with the European Union, Middle East, Africa, Russia, Latin America and Asia fall into the different BRI initiative categories of Economic, Maritime, or Digital. The relationships formed by China have put the country as the world's largest shipping nation. China is second in the world for economy and ranks and third in the world's military powers (Tybring-Gjedde, 2020).

As of March 2020, 138 countries and 30 international organizations are part of BRI, covering the following regions: (Figure 12.1)

- 38 countries are in Sub-Saharan Africa.
- 34 BRI countries are in Europe & Central Asia (including 18 countries of the European Union (EU) that are part of the BRI).
- 25 BRI countries are in East Asia & pacific.
- 17 BRI countries in Middle East & North Africa.
- 18 BRI countries are in Latin America & Caribbean.
- 6 countries are in South East Asia.

A *complete country listing, region, and income status can be found in Appendix A.*

(International Institute for Green Finance II Central University for Finance and Economics, 2020)



Map of the Belt and Road Initiative (BRI) by year: As of March 2020, 131 to 138 countries had joined the Belt and Road Initiative (BRI) by signing an MoU.

Figure 12.1 Countries of Belt and Road Initiative as of March 2020

Source: (International Institute for Green Finance II Central University for Finance and Economics, 2020)

The BRI has the remained strong with the following five goals:

- policy coordination
- facilities connectivity
- unimpeded trade
- financial integration
- people-to-people bonds

The BRI "people to people bonds" has created a network of think tanks, media agreements, and establishment in communities and universities (Hamilton & Ohlberg, 2020). The spread of propaganda using these bonds, delivers a powerful message of international

trust within a global community, making the BRI appear attractive and peaceful. With the addition of Italy and Switzerland in 2020, reinforces BRI commitment and credibility. Along with BRI, China has evolved to modernize their military defense and establish themselves as an international arms dealer.

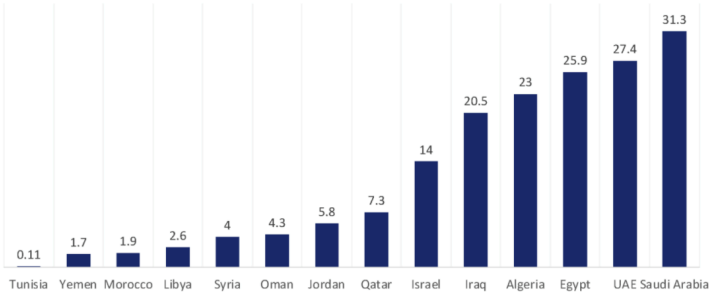


Figure 12.2 China's Inward Investment

Source: (Harding, 2020)

Middle East

The BRI is critical for China in the Middle East; the gulf region is a global player for trade and finance. The Middle East's partnership will give China advantages in trade, military operations, and infrastructure. Drones in this region have grown from surveillance to Unmanned Combat Air Vehicles (UCAVs). The U.S. has strict polices against the export of these deadly attack weapons. In a ten-year period, China has sold 163 UCAVs verses the sale of 15 Reaper drones during the same time period (Roblin, 2020). The largest producer of UCAVs, China Aerospace Science and Technology Corporation (CASC), has plans to open a factory in Saudi

Arabia. Egypt and Saudi Arabia are given priority by China for UCAVs, which are 75% cheaper than MQ-9 Reaper (Alden, Fiala, Krol, & Whittle, 2020).

Chengdu Aircraft Industry Group has taken advantage of China's freedom to sell to anyone, not restricted by export policies. Wing Loong I and Wing Loong II are popular UAV models sold to the United Arab Emirates and Saudi Arabia. The Wing Loong series of UAV are similar to the GA-ASI Predator. Saudi Arabia has acquired an estimated 300 UAV's from China (Stevenson, 2019). China is in close competition with Turkey for supplying UAV's to the Middle East. December 2019, Rainbow (CH-5) drones were exported to Pakistan, Egypt, UAE, and Saudi Arabia. (Figure 12.3)

In the Middle East, China invests in the energy, infrastructure, nuclear power, agriculture and finance to strengthen the ties to the Middle East (Chaziza, 2020). China would bring to Iran telecommunications (5G), banking, ports and railways to the region. China's partnership with Iran could pose detrimental to the U.S. Military. China and Iran would agree to joint military operations, training, weapons development and intelligence sharing. This would give China a military advantage over the U.S. and Iran global ally.

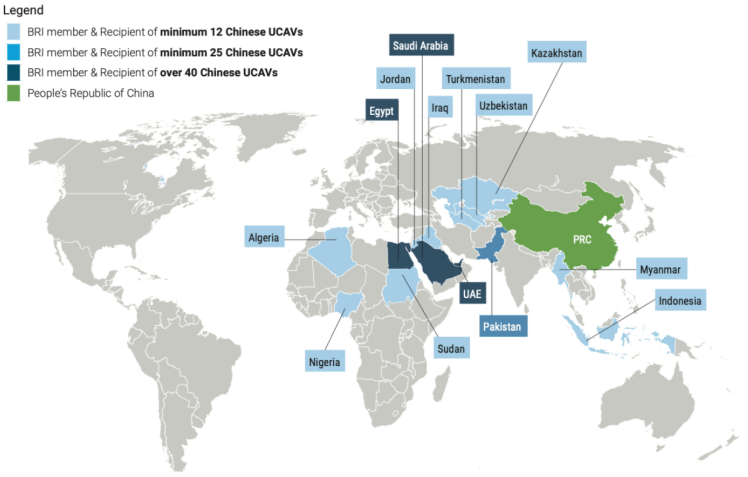


Figure 12.3 Sale of Chinese UCAVs Along BRI

Source: (Alden, Fiala, Krol, & Whittle, 2020)

European Union

The build out of China – EU partnerships began in 2013 with the recruitment of the former Swedish ambassador to an advisor position with Huawei. Eventually, other members of the EU were recruited to be advisors for Huawei. With the growth of the Huawei relationships enabled China to build trust and obtained signatures of support for the BRI from EU member states. The governing body of the EU does not have a formal agreement with China regarding BRI. However, about half EU member states signed on to the BRI (Hamilton & Ohlberg, 2020). China has not sealed commitments for BRI from the top European economies (France, U.K. and Germany). Other EU member states have begun participating in the BRI through financial, corporate, and educational sectors. In July 2020, Serbia received their first order of Six Chinese-built CH-92A combat drones. This marks the beginning of China supplying drones to Europe, another step-in building ties in the region.

Figure 12.4 CH – 92A Unmanned Combat Air Vehicle (UCAV)
Source: (Roblin, 2020)

As part of the Made in China 2025 plan, Aviation and Aerospace Equipment is considered a priority sector. In some reports referred to as the "Air Silk Road".

Maritime Silk Road

Tracing back to 12th century BC, the East China Sea Routes connect mainland China to Northeast Asia. The Liaodong Peninsula located in this region of Asia holds critical military value, dating back the Sino-Japanese War (Japan Center for Asian Historical Records, 2020). The peninsula's trade route value, natural resources, and military positioning makes it a cornerstone for this route of Maritime Silk Road (MSR). The South China Sea route is critical for MSR, opening China to the continent of Africa, following the maritime routes through the Persian Gulf, Indian Ocean, and Red Sea. China has 32,000 kilometers of coastline and more than 3 million square kilometers of maritime land, making the country

a real maritime power, according to the China Engineering Academician of the Chinese Academy of Sciences.

UAE is a leader in supporting China with the Maritime Silk Road (MSR). The creation of Khalifa Port's CSP Abu Dhabi Terminal, by UAE and China shipping giants has attracted twenty additional Chinese companies to the area (Calabrese, 2020). This is the first phase of MSR for Abu Dubai. Turkey is the only country in the region not favorable to MSR.

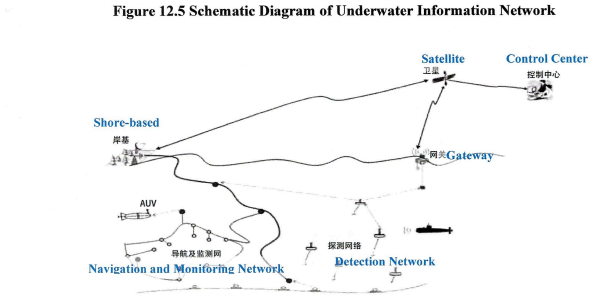
Blue Ocean Information Network

In addition to the support of countries along the MSR, China is building an underground network for military communication and expanding sensors to create a "World Ocean" (Asia Maritime Transparency Initiative, 2020). The *Blue Ocean Information Network*, is part of MSR, will accomplish the following for China:

- Information perception (internationally)
- Target recognition
- Active sonar
- High-resolution marine satellites

The Blue Ocean Information Network is based on Skynet and Submarine Net according to the PLA. China will have the ability to detect mineral, biological resources. With the information network China will have advanced unmanned cyber methods to control and protect the BRI. The Blue Ocean Information network combined with the increase of partnerships / locations along BRI will accelerate China as a maritime superpower.

Figure 12.5 Schematic Diagram of Underwater Information Network

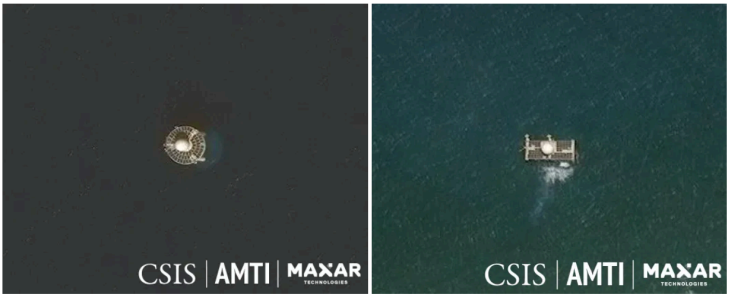


(Ministry of Industry and Information Technology, 2019)

(Ministry of Industry and Information Technology, 2019)

Floating Integrated Information Platforms (FIIP) (also called Ocean E-Stations are the most visible piece of the Blue Ocean Information Network. The network is currently deployed between the Hainan Island and Paracel Islands, and the Bombay Reef. It is believed a previously identified one of the was deployed to Bombay Reef in the Paracel Island sometime in 2018. Communications capabilities of the FIPP include a Ku-band satellite antenna, an L-band satellite antenna, radio antenna, and cellular communications antenna. Sensing systems include an Automatic Dependent Surveillance Broadcast (ADS-B) antenna and an Automatic Identification System (AIS) antenna as well as a small air- and surface-search radar (Asia Maritime Transparency Initiative, 2020).

Figure 12.6 Ocean E-Stations



Left FIIP Between the Hainan Island and Paracel Islands (February 7, 2019)

Right FIIP Bombay Reef (April 28, 2020)

Source: (Asia Maritime Transparency Initiative, 2020)

Other components such as ocean buoys, fixed and relocatable underwater sensors to include sonar and hydrophones, unmanned aerial vehicles (UAVs), unmanned underwater vehicles (UUVs), and unmanned surface vehicles (USVs) could be part of the Blue Ocean Information Network (Asia Maritime Transparency Initiative, 2020). Revisiting the first edition of this textbook, *Unmanned Aircraft Systems (UAS) in the Cyber Domain: Protecting USA's Advanced Air Assets*, Chapter 16 *Chinese Drones in Spratly Islands and Chinese Threats to USA forces in the Pacific*, the case for cyber weapon spoofing of legacy GPS signals affecting the US Navy and commercial vessels in Pacific Ocean are relevant to the Ocean E-Station that was placed in 2018 Bombay Reef in the Paracel Island. The FIIP communications functionality includes AIS, which could be allow for spoofing of AIS sending a fake collision alert by Closet Point of Approach (CPA) spoofing and negating the true alert transmitting to the vessel.

China's goal to complete the development of the "Belt and Road" sea network cooperation to meet the military and civilian management by 2025. China's researchers state there is an urgent

need for information acquisition in the jurisdictional sea area (Ministry of Industry and Information Technology, 2019). China Telcom will use the maritime information nodes, network and submarine network to construct ideas and continue to strengthen the Blue Ocean Information Network.

Digital Silk Road

Digital Silk Road (DSR) initiative was introduced by China in 2015. DSR has more of a government push using Chinese commercial company channels. The idea to grow DSR through several vectors such as social media, telecom, fintech, etc. Ideally, China wants the homegrown companies to fit in with their specific industry, to become a trusted member and contributor to their specific sector. This would give China the ability to intertwine DSR within the different tech vectors. China uses to their advantage of taking lead in specific technology to gain members for DSR, for example next generation (5G). They have used mobile technologies and fiber optic infrastructure to entice countries to the DSR with internet/telecom advantages (Greene & Triolo, 2020). China also promotes their payment system technology, digital wallets, two-way QR codes, paying via social media.

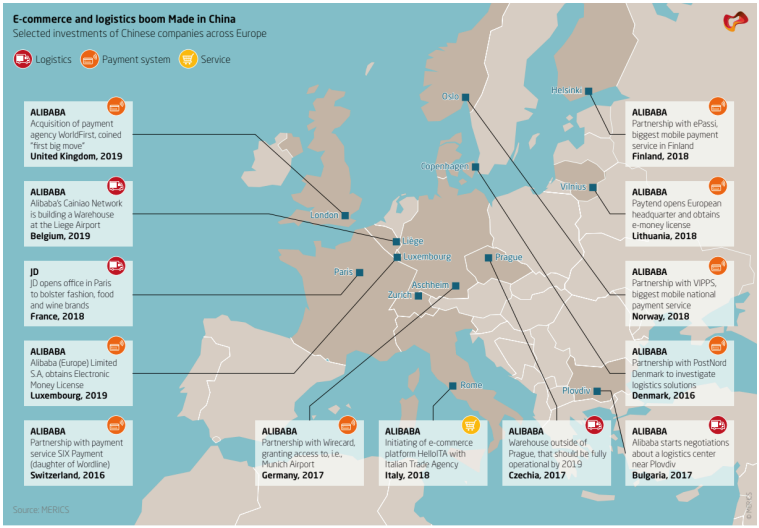


Figure 12.7 China E-Commerce Europe

Source: (Shi-Kupfer & Ohlberg, 2019)

The fiber-optic members of the Digital Silk Road (DSR), Frankfurt to Mumbai via Azerbaijan added a new member November 2020. Turkmenistan agreed to link with Azerbaijan through cables in the Caspian Sea. It is suspected Iran is part of the DSR with cables running down the Persian Gulf.

The drone industry plays a critical part of DSR. SZ DJI Technology is a leader in the global consumer drone marketplace, therefore a large part of the technology vector. DJI has been accused of sharing user information and having week cybersecurity practices. Banned by the U.S. Military, DJI is attempting to create a DoD version of their product. If DJI is successful reaching DoD level of security, it could allow DJI access to a broader marketplace.

Conclusions

China's Brick and Road Initiative has covered several sectors. In

the context of unmanned, China has a significant role in the Middle East, Asia, and Africa military drone marketplace. They are beginning to capture the attention buyers from the Europe Union. China's strong relationships across all vectors in the Middle East has led to a maritime advantage for trade and military operations. Extensive ties between China and Iran has created an unlikely partnership for the U.S. and allies. China has expanded technology under water that will lead to control of several regions if maritime partnerships continue to grow. The Digital Silk Road is an immediate cause for concern for Europe and the U.S., as consumers and industry become dependent on products produced by Chinese companies. The BRI continues to grow at an accelerated rate as trusted partnerships across all industries continue crossover into other opportunities.

Discussion Questions

1. Discuss the key areas of expansion of Belt and Road Initiative that impact the military drone marketplace.
2. Which Silk Road initiative is a greater threat, Maritime or Digital?
3. What Silk Road initiative has greater impact to the United States?

References

International Institute for Green Finance II Central University for Finance and Economics. (2020, March). *Countries of the Belt and Road Initiative (BRI)*. Retrieved from Green Belt and Road Initiative Center: https://green-bri.org/countries-of-the-belt-and-road-initiative-bri?cookie-state-change=1596286450104

Alden, C., Fiala, L., Krol, E., & Whittle, R. (2020, May 28). *Wings Along the BRI: Exporting Chinese UCAVs and Security*? Retrieved

from Medium: https://medium.com/@lseideas/wings-along-the-bri-exporting-chinese-ucavs-and-security-a4bf7a3324df

Asia Maritime Transparency Initiative. (2020, June 16). *Exploring China's Unmanned Ocean Network*. Retrieved from Asia Maritime Transparency Initiative: https://amti.csis.org/exploring-chinas-unmanned-ocean-network/

Calabrese, J. (2020, May 19). *China's Maritime Silk Road and the Middle East: Tacking Against the Wind*. Retrieved from Middle East Institute: https://www.mei.edu/publications/chinas-maritime-silk-road-and-middle-east-tacking-against-wind

Chaziza, M. (2020, March 25). *Belt and Road Initiative, BRI, Business, China, Economic Growth, Economy, Middle East*. Retrieved from The Asia Dialogue: https://theasiadialogue.com/2020/03/25/chinas-partnership-diplomacy-and-the-successful-implementation-of-the-bri/

Dahlquist E., H. S. (2017). System Perspective. . In H. S. Dahlquist E., *In: Dahlquist E., Hellstrand S. (eds) Natural Resources Available Today and in the Future*. Springer, Cham. Retrieved from https://doi.org/10.1007/978-3-319-54263-8_1

Electronics Science & Technology Committee of MIIT. (2019, July 27). *Electronics Science & Technology Committee of MIIT*. Retrieved from Ministry of Industry and Information Technology: http://www.miitestc.org.cn/uploadfile/2019/0727/20190727050055199.pdf

Greene, R., & Triolo, P. (2020, May 8). *Will China Control the Global Internet with the Digital Silk Road*. Retrieved from Carnegie Endowment for International Peace: https://carnegieendowment.org/2020/05/08/will-china-control-global-internet-via-its-digital-silk-road-pub-81857

Hamilton, C., & Ohlberg, M. (2020). *Hidden Hand Exposing How the Chinese Communist Party is Reshaping the World*. Richmond: Hardie Grant Books.

Harding, R. (2020, September 20). *China's Belt and Road Initiative and the Impact on the Middle East and North Africa* . Retrieved from International Banker: https://internationalbanker.com/finance/

chinas-belt-and-road-initiative-and-its-impact-on-the-middle-east-and-north-africa/

Japan Center for Asian Historical Records. (2020, July 28). *Japan Center for Asian Historic Records*. Retrieved from National Archives of Japan: https://www.jacar.go.jp/english/nichiro/map.htm

Ministry of Industry and Information Technology. (2019, July 27). *Electronics Science & Technology Committee of MIIT*. Retrieved from Ministry of Industry and Information Technology: http://www.miitestc.org.cn/uploadfile/2019/0727/20190727050055199.pdf

Pan, C. (2020, March 27). *UK university study identifies Chinese drone maker XAG as best fit for disinfection operations to fight coronavirus spread.* Retrieved from South China Morning Post : https://www.scmp.com/tech/gear/article/3077296/uk-university-study-identifies-chinese-drone-maker-xag-best-fit

Roblin, S. (2020, July 9). *Missile-Armed Chinese Drones Arrive In Europe As Serbia Seeks Airpower Edge*. Retrieved from Forbes: https://www.forbes.com/sites/sebastienroblin/2020/07/09/missile-armed-chinese-drones-arrive-in-europe-for-serbian-military/#4af9aff679d2

Shi-Kupfer, K., & Ohlberg, M. (2019). *China's Digital Rise : Challenges for Europe.* Berlin: Mercator Institute for China Studies.

Stevenson, B. (2019, November 17). *Dubai Airshow*. Retrieved from AIN Online: https://www.ainonline.com/aviation-news/defense/2019-11-17/uavs-continue-grow-strength-middle-east

Tybring-Gjedde, C. (2020). *China's Belt and Road Initiative: A Strategic and Economic Assessment.* Brussels: Nato Economics and Security Commitee.

Xuanzun, L. (2020, June 6). *PLA special mission aircraft approaches Taiwan after the island's missile test*. Retrieved from Global Times: https://www.globaltimes.cn/content/1191424.shtml

13. Chapter 13 Automaton, AI, Law, Ethics, Crossing the Machine – Human Barrier [Lonstein]

"The development of full artificial intelligence could spell the end of the human race….It would take off on its own, and re-design itself at an ever-increasing rate. Humans, who are limited by slow biological evolution, couldn't compete, and would be superseded." Stephen Hawking (Cellan-Jones, 2014)

Student Learning Objectives

Professor Stephen Hawking gave the cautionary warning above almost six years ago. While no human can predict what the future will hold with specific accuracy, we can examine new technology, blend it with the social sciences and history to develop generalized ideas of the societal risks and rewards of new technology. Students should use their imagination, experience, and learning to enhance their understanding of how best to implement technology, predict intended and unintended consequences, and engage in their risk-benefit analysis. This process is an essential precursor for the introduction of Artificial Intelligence into everyday life. This analysis will challenge the student to think critically, not merely accept statements of "experts" or manufacturers of even celebrity or other endorses of a particular technology at face value. Someone once said: "Any intelligent fool can make things bigger and more complex… It takes a touch of genius – and a lot of courage to move in the opposite direction." – Attributed to Albert Einstein, E.F Schumacher, and Woody Guthrie in various publications, for our purposes, the source of the quote is less important than the message. Students should be bold and

brave, speak truth based on their experience, and education and not shy away from being unpopular or different. Conformity, for the sake of conformity, does not honor students' effort in acquiring knowledge. It makes them more lemming and less human. Students should strive to be the best human one can be.

Once Completed Students Should

- Understand that they all possess unique thinking and analysis tools based upon their imagination, learning, experience, and uniqueness. Those attributes are critical to better not only themselves but to better mankind both by embracing new technology or rejecting it based upon risk.

- Consider the risk of ubiquitously using automation and AI throughout many aspects of everyday life. Students must be aware of potential risks from connected technology, such as social media where information is simple to acquire and digest in seconds carry risk of abuse, manipulation or even degradation of human thought processes?

- Be aware that there are no simple answers to the widespread implementation of AI and Automation and beyond the changes to how we, as humans do things but also consider how we might be changed as a result of this process. From mental and physical health to its impact upon future generations, the environment, public safety, and many other aspects of the human existence.

Humans, Humanity and Humanoids

According the Merriam-Webster Dictionary a “Human” is defined as “a bipedal primate mammal (Homo sapiens), a person” (Merriam-Webster, 2020); “Humanity” is defined as “the quality or state of being human.” (Merriam-Webster, 2020); And “Humanoids” are defined as “a humanoid being: a nonhuman creature or being with characteristics (such as the ability to walk upright) resembling those of a human.” (Merriam-Webster, 2020). Finally, Merriam-Webster Defines Artificial Intelligence as: “1. a branch of computer science dealing with the simulation of intelligent behavior in computers and 2: the capability of a machine to imitate intelligent human behavior.” (Merriam-Webster, 2020) [See Figure 13.1]

The question which will confront all of us in the very near future is what will differentiate the human and humanity, one organic the other more ethereal in terms of their ability to make subjective judgments, from the Humanoid which is not organic, nor is it capable of subjective thought, only objective decision making based upon its programming.

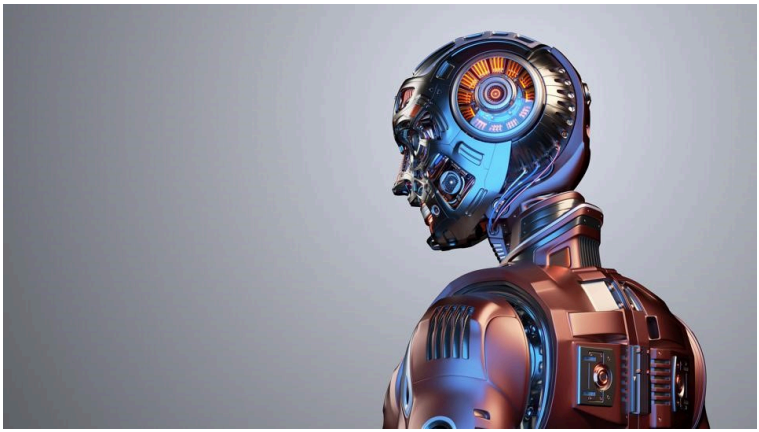


Figure 13.1 The Humanoid

Source: Courtesy Forbes & Adobe Stock)

Are We Losing Our Minds?

Today there is no shortage of conflicting viewpoints on the law, ethics, and morality relating to autonomous technology and Artificial Intelligence. Moving beyond what is their current nascent state, these technologies will undoubtedly continue to become staples of everyday life. To focus our discussion on technology familiar to most if not all of us, we will examine the issues of AI and Autonomous operation in social media. In 2017 Liz Stillwaggon Swan wrote an article in the IEEE publication "Technology and Society" entitled "Are Social Media Making Us Stupid?" Swan asks whether addiction to social media amongst our youth results in a rapid loss in writing skills proficiency. Swan writes:

"Social media platforms force users to think and write in bit-like form, with acronyms substituting for sentences and emoticons substituting for the expression of feelings. We are learning–some of us more quickly than others–to adapt to a computer-dictated form of communication. Sherry Turkle (M.I.T.) has noted that a fluency with texting and tweeting is commonly correlated with a dearth of skills in face-to-face interactions. We're noting, in addition, what social media addiction is doing to written communication: specifically, it's eroding the traditional divide between speaking and writing." (Stillwaggon Swan, 2017)

Our focus will be on the rapidly decreasing face-to-face interactions associated with increased social media usage. Social media is a simple technology, but Swan writes it also has "broken time and space barriers" by allowing users to communicate with followers and vice-versa 24/7 around the globe instantly.[1] How do AI and autonomous technology result in the need for consideration of laws and ethics relating to their implementation in social media?

According to Courtney Seiter, the Neurotransmitter Dopamine, ("the Pleasure Chemical") and the Hormone Oxytocin (the "Cuddle Chemical") play a significant role in the addictive use and near-

blind acceptance of content on social media. According to Seiter, there is a strong relationship between these two behaviors affecting biological compounds and the online and increasingly offline actions of its users. Seiter writes that the roles of Dopamine and Oxytocin play significant roles in the psychology of social media.

Dopamine

Dopamine is stimulated by unpredictability, by small bits of information, and by reward cues—pretty much the exact conditions of social media. The pull of dopamine is so strong that studies have shown tweeting is harder for people to resist than cigarettes and alcohol.

Oxytocin

Then there's oxytocin, sometimes referred to as "the cuddle chemical" because it's released when you kiss or hug. Or … tweet. In 10 minutes of social media time, oxytocin levels can rise as much as 13%—a hormonal spike equivalent to some people on their wedding day. And all the goodwill that comes with oxytocin—lowered stress levels, feelings of love, trust, empathy, generosity—comes with social media, too. As a result, social media users have shown to be more trusting than the average Internet user. The typical Facebook user is 43% more likely than other Internet users to feel that most people can be trusted. So, between dopamine and oxytocin, social networking not only comes with a lot of great feelings, it's also really hard to stop wanting more of it." (Seiter, 2016)

Slot Machines in Your Hand & Head

Creators of social media platforms like Facebook, Twitter, amongst many others, did not need to look far to learn how to drive maximum adoption and daily dependence upon social media. I always enjoy the bells and whistles and lights when walking into a casino. Yet, after playing a bit, the usual sensation experienced is regret, foolishness, and quite frankly dirtiness. Much like a smartphone, noises, visuals, and other sensory stimulation 24 hours a day can lead to dependence and mistakes. B.F Skinner, the famed Harvard psychologist, once said "A pigeon can become a

pathological gambler, just as a person can," (Skinner, 1977) [See Figure 13.2]

Figure 13.2 Gambling Pigeons

Source: (Courtesy Bettmann Archive / Getty)

So, what do pigeons and gambling have to do with social media? "Just as substance addicts require increasingly strong hits to get high, compulsive gamblers pursue ever riskier ventures. Likewise, both drug addicts and problem gamblers endure symptoms of withdrawal when separated from the chemical or thrill they desire. And a few studies suggest that some people are especially vulnerable to both drug addiction and compulsive gambling because their reward circuitry is inherently underactive—which may partially explain why they seek big thrills in the first place." (Scientific American, 2013)

The Psychology of Social Media

In 2004 Dr. John Suler wrote the groundbreaking paper entitled the "Online Disinhibition Effect. In the paper Dr. Suler examined the psychology behind our behavior on line and how it varies from the brick and mortar world. Dr. Suler wrote in 2004:

"Everyday users – on the Internet–as well as clinicians and researchers have noted how people say and do things in cyberspace that they wouldn't ordinarily say and do in the face-to-face world. They loosen up, feel less restrained, and express themselves more openly. So pervasive is the phenomenon that a term has surfaced for it: the online disinhibition effect." (Suler, 2004)

What the psychological components of the Online Disinhibition Effect and how do they drive our online behavior? [See Table 13.1]

**ONLINE BEHAVIOR –IS IT DIFFERENT?
SIMPLE, VIRTUAL, ANONYMOUS**

•You Don't Know Me (Dissociative anonymity) -As you move around the internet, most o
you are. When people have the opportunity to separate their actions from their real worl
don't have to own their behavior by acknowledging it within the full context of who they "

•You Can't See Me (Invisibility) -Even with everyone's identity visible, the opportunity to
effect. You don't have to worry about how you look or sound when you say (type) somethi
look or sound when you say something.

•See You Later (Asynchronicity) -People don't interact with each other in real time. Othe
to reply to something you say. Asynchronous communication is like "running away" after

•It's Just a Game (Dissociative imagination) –People feel their online personae exist in a
demands and responsibilities of the real world. Once they turn off the computer and retu
leave their online identity behind. Why should they be held responsible for what happens
reality?

•It's All In My Head (Solipsistic Introjection) -Absent cues combined with text communi
Sometimes they feel that their mind has merged with the mind of the online companion.
experienced as a voice within one's head, as if that person magically has been inserted or
may not know what the other person's voice actually sounds like, so in our head we assig
or unconsciously, we may even assign a visual image to what we think that person looks li
companion now becomes a character within our intrapsychic world, a character that is sh
him or herself via text communication, but also by our expectations, wishes, and needs. B
people we know, we fill in the image of that character with memories of those other acqu

•**We're Equals (Minimizing authority)** -While online a person's status in the face-to-face
have as much impact as it does in the face-to-face world. If people can't see you or your s
president of a major corporation sitting in your expensive office, or some "ordinary" perso
computer.

Table 13.1 Online Disinhibition Effect

Source: (Courtesy John Suler)

When Facebook was conjured up one of its founders, Sean Parker, its President at the time said:

"The thought process that went into building these applications, Facebook being the first of them… was all about: 'How do we consume as much of your time and conscious attention as possible?'" "And that means that we need to sort of give you a little dopamine hit every once in a while, because someone liked or commented on a photo or a post or whatever. And that's going to get you to contribute more content, and that's going to get you … more likes and comments." "It's a social-validation feedback loop … exactly the kind of thing that a hacker like myself would come up with because you're exploiting a vulnerability in human psychology. "The inventors, creators – it's me, it's Mark [Zuckerberg], it's Kevin Systrom on Instagram, it's all of these people – understood this consciously. And we did it anyway." (Allen, 2017)

Now that we have enough understanding of how social media was designed to psychologically effects humans, the question becomes how it can be used or misused. By leveraging the known psychological intended effects social media can be used to cross the virtual / actual barrier to cause humans to take or not take actions or behave in a particular way. This can fulfill the objective of the social media platforms or actors as a tool of disinformation, confusion, political unrest, or even armed conflict.

Noted internet and virtual reality Jaron Lanier recently wrote about these and many other concerns in his 2018 book, "Ten

Arguments for Deleting your Social Media Accounts Right Now." In an April 2018 interview with the Intelligencer he spelled out his concerns about the damage social media may be doing across society.

Weaponizing AI and Automation Using Social Media as the Delivery Method

Lanier in a prescient and articulable fashion express his very real concern with the potential of social media and its digital automation to have profoundly dangerous affects upon the world:

"One of the things that I've been concerned about is this illusion where you think that you're in this super-democratic open thing, but actually it's exactly the opposite; it's actually creating a super concentration of wealth and power and disempowering you. This has been particularly cruel politically.

Every time there's some movement, like the Black Lives Matter movement, or maybe now the March for Our Lives movement, or #MeToo, or very classically the Arab Spring, you have this initial period where people feel like they're on this magic-carpet ride and that social media is letting them broadcast their opinions for very low cost, and that they're able to reach people and organize faster than ever before. And they're thinking, Wow, Facebook and Twitter are these wonderful tools of democracy. But then the algorithms have to maximize value from all the data that's coming in. So, they test use that data. And it just turns out as a matter of course, that the same data that is a positive, constructive process for the people who generated it – Black Lives Matter, or the Arab Spring– can be used to irritate other groups. And unfortunately, there's this asymmetry in human emotions where the negative emotions of fear and hatred and paranoia and resentment come up faster, more cheaply, and they're harder to dispel than the positive emotions. So, what happens is, every time there's some positive motion in these networks, the negative reaction is actually more powerful. So, when you have a Black Lives Matter, the result of that is the empowerment of the worst racists and neo-Nazis in a way that hasn't been seen in generations. When you have an Arab Spring,

the result ultimately is the network empowerment of ISIS and other extremists – bloodthirsty, horrible things, the likes of which haven't been seen in the Arab world or in Islam for years, if ever." (Lanier, 2018)

A mere two years later we have seen protests and riots across the United States and globe started in late May when a citizen in Minneapolis, George Floyd was seen dying during a police restraint where an officer kneeled on his neck for over eight minutes. Spontaneous and understandable protests and cries for justice ensured and social media became a tool employed to coordinate some of these demonstrations. Unfortunately, almost immediately social media's emotional and Dopamine intensive qualities were manipulated to turn peaceful protests into riots, violence, property damage and even death across America. [See Figure 13.3]

Figure 13.3 Protest Tweet

Source: (Twitter Post @sugaaab_retweeted by @rave_mom_breezy)

Large sections of the population have recently become more reliant upon social media, especially during the global Coviid-19 Pandemic, which has turned to social media and away from broadcast media in droves. According to the Business Insider, a

"Harris Poll conducted between late March and early May, between 46% and 51% of US adults were using social media more since the outbreak began. In the most recent May 1–3 survey, 51% of total respondents – 60% of those ages 18 to 34, 64% of those ages 35 to 49, and 34% of those ages 65 and up – reported increased usage on certain social media platforms." (Samet, 2020)

Couple a significant uptrend in the global usage of social media with a populace that has increasingly become addictively and compulsively tethered to social media, and the result is an army of potential human assets which, to a certain degree, can be transformed to near humanoids.

The ability to deploy a humanoid army, nearly instantly, anywhere in the world, is a potent delivery system. The ordinance must be programmed into the delivery vehicle. Bots, fake accounts, fake news, disinformation, real-fake videos, and memes are all tools of social media information warfare. They have increasingly leveraged as a weapon of information warfare globally.

Recently Jeff Elder of Business Insider reported:

Media and citizen journalists are posting video, images, and accounts of scattered and chaotic protest events in response to the killing of George Floyd by a Minneapolis police officer, and the posts are being re-shared broadly. The result is an often-overwhelming stream of media from multiple sites and sources, and experts say audiences must be aware that the situation is being manipulated.

"People need to be aware that these events on the ground are being spun for political reasons," says Angie Drobnic Holan, editor-in-chief of PolitiFact, the Pulitzer Prize-winning fact-checking news service of the Poynter Institute journalism think tank. Much of that spin likely comes from forces outside of America, the experts warn.

"Were there foreign-backed disinformation accounts targeting Americans this weekend? Absolutely. I am positive that was happening," says Molly McKew, a writer and lecturer on Russian influence who advises the non-profit political group Stand Up America." (Elder, 2020)

Information warfare is nothing new as a tool of conflict. Between

the 1920's and 1940's Germany under Hitler's Minister of Propaganda Dr. Joseph Goebbels. According to Dr. Yaniv Livyatan, "Goebbels needed a staff of 1,000 to generate propaganda. Today all it takes is the click of a button." (Livyatan, 2019) [See Figure 13.4]

Figure 13.4 Dr. Joseph Goebbels

Source: (Courtesy AP)

Dr. Levyatan belies that social media, its ubiquitous nature, ease of automation and ability to instantly "push" notifications to subscribers instead of them searching for content makes it a propaganda game changer. He continues:

So, it's vital to understand who your audience is and what moves it. At the same time, the world is becoming a place where you can accumulate more and more knowledge of that kind. You can target your messages accurately. Scientifically. Think what Goebbels could have done with Facebook.

"Facebook is excellent for psychological warfare because they're constantly collecting information about us. An analysis of that information is very illuminating with respect to our personalities, our aspirations, our opinions. We saw that vividly in the story of Cambridge Analytica [which acquired data from profiles of some 50 million Facebook users] in the 2016 U.S. election. Our behavior in the social networks, which we perceived as something innocent

and mundane, has become an instrument through which we can be influenced via manipulative techniques. The information we volunteer, such as Likes, make it possible for those who want to, to understand how to communicate with us in a precise way.

Goebbels had a ministry of 1,000 personnel whose primary task was not to compose messages but to go into the field and examine how the messages work on people. Today you can do that by pressing a small button. If the Nazis had come to power today, they would have ruled the world.

Indeed, we see which rulers are rising to power today and what their messages look and sound like. We can take it that there's a connection." (Livyatan, 2019)

Conclusions

While many consider the implementation of Artificial Intelligence and Autonomous Technology concepts most closely associated with Drones, Driverless Vehicles, Autonomous Surface and sub-surface and sea technology, students must keep a keen eye on their personal technology as well. According to Rescuetime.com the average American checks their cell phone 58 times each day so if you wanted to get a message in front of a target's eyes, the phone and Social media apps are the way to do it. (McKay, 2019) When combined with addictive behavior and a growing reliance on short form messaging and content, critical thinking is under attack and those who seek to do harm are well aware of this troubling reality.

Questions for students to consider

1. How would you respond to the mass dissemination of false information on social media video designed to mislead the public that a terror attack was occurring in New York City using film from the 9/11 attacks in 2001?

2. Should social media technology be controlled or be subject to oversight and regulation from the federal government due to the risk it can easily be used to destabilize or even overthrow the nation?

3. Should Social Media companies be allowed to employ algorithms and use encryption technology without allowing access to the information to the federal government or military in a time of national crisis?

4. How would you slow the progress of the pernicious addictive allure of social media upon today's youth or do you believe that is something best left to the social media companies themselves?

5. Have you ever asked another who informed you that they saw that a particularly disturbing event occurred where they saw the information and their reply was Facebook, Twitter, or another social media platform?

REFERENCES

@sugaaab_. (2020, May 27). Tweet. Minneapolis, Minnesota, United States.

Allen, M. (2017, November 9). *Sean Parker unloads on Facebook: "God only knows what it's doing to our children's brains"*. Retrieved from Axios.com: https://www.axios.com/sean-parker-unloads-on-facebook-god-only-knows-what-its-doing-to-our-childrens-brains-1513306792-f855e7b4-4e99-4d60-8d51-2775559c2671.html

Cellan-Jones, R. (2014, December 2). *Stephen Hawking warns*

artificial intelligence could end mankind. Retrieved from bbc.com: https://www.bbc.com/news/technology-30290540

Cherry, K. (2020, May 25). *The Skinner Box or Operant Conditioning Chamber*. Retrieved from Verywellmind.com: https://www.verywellmind.com/what-is-a-skinner-box-2795875

Elder, J. (2020, June 2). *Foreign actors and extremist groups are using disinformation on Twitter and other social networks to further inflame the protests across America, experts say*. Retrieved from Business Insider: https://www.businessinsider.com/twitter-facebook-disinformation-george-floyd-unrest-politifact-2020-6

Lanier, J. (2018, April). 'One Has This Feeling of Having Contributed to Something That's Gone Very Wrong". (N. Kulwin, Interviewer)

Livyatan, D. Y. (2019, January 6). *Just Think What Goebbels Could Have Done With Facebook*. Retrieved from Haaretz.com: https://www.haaretz.com/world-news/.premium.MAGAZINE-just-think-what-goebbels-could-have-done-with-facebook-1.7308812

Marr, B. (2020, February 17). *Artificial Human Beings: The Amazing Examples Of Robotic Humanoids And Digital Humans*. Retrieved from Forebes.com: https://www.forbes.com/sites/bernardmarr/2020/02/17/artificial-human-beings-the-amazing-examples-of-robotic-humanoids-and-digital-humans/#6103bce65165

McKay, J. (2019, March 21). *Screen time stats 2019: Here's how much you use your phone during the workday*. Retrieved from Rescue Time: Blog: https://blog.rescuetime.com/screen-time-stats-2018/

Merriam-Webster. (2020, August 15). *artificial intelligence noun*. Retrieved from Merriam-Webster.com: https://www.merriam-webster.com/dictionary/artificial%20intelligence

Merriam-Webster. (2020, August 5). *Definition of human (Entry 2 of 2)*. Retrieved from Merriam-Webster.com: https://www.merriam-webster.com/dictionary/human#h2

Merriam-Webster. (2020, August 11). *humanity noun*. Retrieved from Merriam-Webster.com: https://www.merriam-webster.com/dictionary/humanity

Merriam-Webster. (2020, August 12). *humanoid adjective*. Retrieved from Merriam-Webster.com: https://www.merriam-webster.com/dictionary/humanoids

Samet, A. (2020, June 9). *2020 US SOCIAL MEDIA USAGE: How the Coronavirus is Changing Consumer Behavior*. Retrieved from Business Insider: https://www.businessinsider.com/2020-us-social-media-usage-report

Scientific American. (2013). How the Brain Gets Addicted to Gambling. *Scientific American*, 309, 5, 28-30.

Seiter, C. (2016, August 10). *The Psychology of Social Media: Why We Like, Comment, and Share Online*. Retrieved from Buffer: https://buffer.com/resources/psychology-of-social-media/

Skinner, B. F. (1977). *Skinner- Operant Conditioning*. Retrieved from YouTube: https://www.youtube.com/watch?v=LSv992Ts6as&feature=youtu.be&t=244

Stillwaggon Swan, L. (2017, June 29). *Are Social Media Making Us Stupid?* Retrieved from technologyandsociety.org: https://technologyandsociety.org/are-social-media-making-us-stupid/

Suler, J. (2004). The Online Disinhibition Effect. *CyberPsychology & Behavior*, 321-326.

[1] Nations such as North Korea, Iran and a few others have been referred to as hermit nations because to the extent technologically possible, they restrict the use of social media.

14. Chapter 14 Maritime Cybersecurity [Nichols]

Student Objectives

Students will revisit the South China Sea and Chinese Threats to USN and Commercial vessels in the area.

Students will grasp the size and cybersecurity issues for the Maritime Transportation Sector (MTS)

Students will understand the nuances of Cyber-Physical systems, Operational technology, and the Internet of Things (IoT).

Introduction

I would like to dedicate this bonus chapter to Dr Gary C Kessler and Steven D. Shepard on their 2020 release of a fascinating book on ***Maritime Cybersecurity: A Guide for Leaders and Managers*. (Kessler, 2020)**. I respect and agree with everything their many years of experience have witnessed and put into writing on the subject except strategies for maritime cyberdefense in which the authors mistake the priorities of Vulnerabilities over real Threats. The author has liberally cited this excellent work. *We can do something about Threats – applying appropriate countermeasures to reduce risk.* Vulnerabilities are a constant and represent an existing weakness in the information system that will always be present, will generally increase even after a computer security audit, or patch(es), and may or may not be a conduit for a real Threat to attack an information system. The security goal is to identify Vulnerabilities and to reduce Threats.

Our views are different. The author is a captain of a cruising yacht with 40 plus years as previous owner / master of five different medium – size sail and power boats. Every effort was made to maximize / duplicate the security of electronics, navigation systems, powertrain, fire suppression, pumping, SOLAS, anchoring, weather, piloting, RADAR, AIS, SONAR, seamanship, and passenger

safety on my marine craft. My charges were USCGA approved / inspected every two years. It took nearly 20 years to become a decent captain. The author made every mistake that was on some novice list of "don'ts" on the water. But that is called experience. My career has been in cybersecurity and INFOSEC. Multiple systems on my craft were computer aided including AIS, RADAR plots, navigation, USCG soundings / charts, ATN, buoys, weight distribution / loading, emergency systems, power, bilge, satellite phone, EPIRB, entertainment, three VHS radios, previously LORAN-C, and remote communications. Threats to these coordinating computer – information systems were serious and might have denied me port entry if they were not adequately protected. [1]

The author's point is that qualitative information system *Risk is ~ f(Threats / Countermeasures).* This is true because Vulnerabilities and Impact are essentially constants that drop out of the strategic consideration for planning for cyberdefense. Increase the Threat vector and we directly increase the risk. Increase applied Countermeasures and Risk is reduced. These can be calculated as qualitative levels of risk or translated into worst, best and normal case scenarios for comparison of incremental changes to either dependent variable.

This chapter will not debate the (Kessler, 2020) notions of Risk Vs Vulnerabilities Vs Threats. There are some valid points, charts, procedures presented in his final chapters. (Kessler, 2020) Instead, Chapter 14 will revisit the authors research on the spoofing of navigation systems on vessels in the South China Seas. This will be followed by a section on the MTS and potential cybersecurity vectors and end with a section focused on the holy grail of IoT as related to the maritime sector.

The Case for Cyber Weapon Spoofing of Legacy GPS Signals Affecting US Navy and Commercial Vessels in Pacific

In (Nichols R. K., et al., 2019), the *author presented a detailed case for GPS spoofing by Chinese assets of US Navy and Commercial*

Vessels in South China Seas. It is summarized here as a starting point for a condensed discussion on maritime security.[2]

U.S Navy Vessel Collisions in the Pacific

In 2017 there was a chain of incidents/collisions involving four U.S. Navy warships and one U.S. Navy submarine. On 17 June, the destroyer USS Fitzgerald collided with the ACX, a 30,000-ton container ship resulting in seven dead. Records show that the ACX turned sharply starboard (right) at the time of collision. *The captain of the Philippine-flagged container ship accused the Navy destroyer of failing to heed warning signs before the crash.* Those warning signs came from the commercial vessels Automated Collision Systems (AIS) on the bridge. On 9 May, the guided-missile cruiser USS Lake Champlain collided with a South Korean fishing boat off the Korean Peninsula. There were no injuries (Department of the US Navy, Office of Chief of Naval Operations, 2017). On 31 January, the guided-missile cruiser USS Antietam ran aground dumping more than 1000 gallons of oil into Tokyo Bay. On 18 August, the ballistic-missile submarine USS Louisiana collided with the Navy Offshore Support Vessel in the Strait of Juan de Fuca. There were no injuries. "On 20 August, the guided-missile destroyer USS John S McCain collided with the 600-foot oil and chemical tanker Alnic MC at 0624 JST resulting in ten dead (Navy Information Office , 2017)". (Weise, 2017)

Navy Response

In all five incidents, the U.S. Navy blames their field leadership for not responding in an appropriate manner. This response means that the Skipper / XO / COB and at least five (5) watch sailors on each Naval vessel (roughly 40 – 50 personnel including bridge staff plus 130 lookouts on the USS McCain because of ordered watch conditions) have been judged incompetent (Navy Information Office , 2017). Their careers are over, and some will face courts martial and possible brig time. This response also implies that all five Navy vessels' radar, emergency positioning alert systems, AIS, sonar, and long-range collision avoidance equipment must have been functioning perfectly, without a catastrophic failure or interference

of any kind. This conclusion assumes that none of the ships were in difficult maneuverable waters or serious traffic. The Navy blames funding, readiness, and training. However, their response may not fully account for the commercial vessel accident data, actions required, o GPS positional data received (Olson, August 30, 2017). (Nichols, et al., Unmanned Aircraft Systems (UAS) in Cyber Domain: Protecting USA's Advanced Air Assets, 2nd Edition, 2019)

The Navy Official Reaction regarding the possibility of Cyber-Weapon or Cyber-Attack

The Navy has downplayed the possibility of a Cyber Weapon or Cyber Attack. Prior Chief of Naval Operations (CNO) Admiral John Richardson said in a tweet on Monday 23 August, referring to the USS McCain and USS Fitzgerald collisions, "there was no indication of the possibility of cyber intrusion or sabotage was involved or that the Navy ships were hacked, but the review will consider all possibilities." (Weise, 2017) The Navy investigators after inspecting the physical damage to the USS McCain and USS Fitzgerald agree with the CNO's conclusions (Olson, August 30,2017).

"Navy experts in the technology and researchers at University of Texas at Austin say there are certainly scenarios they can imagine in which GPS hacks could have been used to foil ships' navigations systems but emphasize there's no evidence such attacks took place in the case of the Navy collisions." (Weise, 2017) "The technology to jam or misdirect navigational software is readily available, though the Navy uses a much more robust encrypted version of GPS that would be very difficult to disrupt." (Weise, 2017)

The only way to spoof such a system is a *record and replay* attack, "where a recording is made of the encrypted location data being sent from GPS satellites to the naval ship. Replaying the recording at a slightly later time could fool a ship into thinking it is someplace else. This is a very sophisticated and difficult hack that requires multiple recordings of the navigation data stream from multiple angles, and then sending the recorded signal from two or more locations." (Weise, 2017) "To ensure that nearby ships do not also

get the false data, it would have to be transmitted from close to the Navy ship being targeted, perhaps using multiple drones." (Weise, 2017)

However, according to " Professor David Lust, former president of the Royal Institute for Navigation in the United Kingdom, "it takes two to Tango…. I" think you just have to attack the weakest of the pair, which is the commercial vessel." Commandeering the GPS of the cargo ship to get it to veer off course could cause collision, and it is a much easier hack." (Humphreys, 2009)

The Case for a Cyber Weapon

There appears to be valid evidence to support the theory that at least two of the U.S. Navy Warships, USS John McCain, and the USS Fitzgerald AND/OR the commercial vessels involved were the on the wrong end of a Cyber-Weapon and were receiving incorrect GPS generated positional information. In agreement with Dr. Lust's conclusions, the Cyber Weapon may have been deployed by an adversary's [China PLAN] UAS off a small nearby vessel. The author believes that the subject Cyber-Weapon is an advanced modular entity that can spoof the GPS signals received by all vessels in its range. J.S. Warner & R.G. Johnson established in 2013 that the cyber-security of many common automated navigational systems today lacks basic cyber-attack protection; vessels using incorrect data will make wrong decisions in terms of navigation and emergency responses, leading to potential collisions and deaths (Warner & Johnson, 2013).

Surfacing Questions

Spoofing is generation of false transmissions masquerading as P(Y) [the encrypted] Precise Signal that makes up the military vessel positioning basis, or unencrypted C/A [Civilian Acquisition] code from GPS satellites. In a virtual world tracking invalid data streams or non-integrity-based data is difficult, especially on three dimensional vessels moving in time. However, there may be more than one method to spoof a signal no matter how well it is encrypted. The cargo ships involved could have received

unencrypted GPS ranging; a much less complex method than is required for military vessels.

Both ships do not need to be disabled or spoofed. All ships (military, commercial, recreational, specialized service) in international waters require detailed positional information. GPS systems accurately supply a 3-D position, velocity, and time fix in all types of weather, 24 hours a day.

GPS satellite signals are ranging devices that deliver two signals made up of a civilian carrier, C/A code, NAV message, P-Code, and a military carrier. (Nichols, et al., Unmanned Aircraft Systems (UAS) in Cyber Domain: Protecting USA's Advanced Air Assets, 2nd Edition, 2019)

Because of cost, most systems on commercial vessels have legacy GPS systems. In the author's view, even if the GPS signals of the military vessels were not hacked the unencrypted C/A – L1 Civilian signal may have been. *It is also provable that this spoof is technically feasible* on the legacy systems. Experiments by Warner and Johnston out of Los Alamos, and surveys by Schmidt, et al out of Queensland University clearly support the GPS/GNSS Cyberattack threat vector. (Warner, 2013) In 2013, Humphreys and his students successfully spoofed an $80MM Yacht's GPS system. (Humphreys, 2009)

What the physical damage indicates for the USS McCain and USS Fitzgerald is that both naval vessels appear to have collided on the starboard side. This leads to the theory that the Civilian vessels involved in crossing or approaching the US Naval vessels were relying on faulty information for their position. Further, the cyber weapon may have been delivered by small UAS from a nearby fishing or recreational vessel. It would be a perfect delivery vehicle: stealth, quiet, low radar signature, requiring only 1- 25 watts signal spoofing power. Since the true GPS signal strength reaching the surface of the Earth is about -160dBw (1x 10**-16 Watts), a 1-Watt GPS jamming

spoof signal can override C/A code acquisition for more than 620 miles (Line of Sight (LOS) to horizon.) (Warner, 2013)

The starboard side collisions suggest that one of the vessels may have turned port or that the commercial ship tried to avoid a fake collision target received by turning starboard at the wrong time. The USS Fitzgerald report confirms this observation. These are huge vessels. Turning, stopping, or reversing course on a dime are not possible – especially by a large freighter. Decisions must be made well in advance of potential collision alerts. This is also why delivery of a cyber-weapon by UAS is so attractive. It would be a small bird *in the glasses* while attention was directed to the huge targets closing in on each other. In the chaos, the adversary wins.

How could GPS chaos be achieved against US Vessels?

The author believes, that for the spoofing GPS signal theory [targeting a commercial vessel by cyber weapon to give it a false position and potentially cause collision to itself or another vessel], to be possible. It would require an enemy Unmanned Aircraft System (UAS) to be launched from either a sea-based vessel or land-based intelligence station in the Spratly Islands. The methodology contemplated consists of three cyber-attack activities:

1) Breaking the existing AIS GPS commercial vessel receiver signal locks,

2) Locking the AIS GPS tracking device onto the GPS Simulator counterfeit signal,

3) Maintaining access by continued broadcasting of the fake GPS signal.

The problem is interesting because there are two three-dimensional maritime targets moving in time based on inaccurate or false ranging (GPS position) signals. The clocks used in GPS satellite systems are extremely accurate and present synchronization difficulties with the target naval / commercial vessel receivers. If it is possible to simulate and spoof the GPS signals to the commercial vessel using AIS collision avoidance systems (Cyber-weapon

CONOP), then it is also possible that the US Navy may not have given proper attention to the non – personnel issues in their accident investigations.

Further, the possible delivery of such a Cyber-Weapon by close range UAS means that adversaries may have increased their knowledge management and understanding of U.S. Navy defensive systems. Using asymmetric warfare tactics and attacking the commercial traffic, which deploys legacy and cheaper GPS receivers, forces dependence on faulty information. Unfortunately, it is an effective tactic that bypasses much of the military modernization of GPS signals and satellites. This same possibility could affect military and commercial aircraft also, especially at airports where traffic speeds are reduced, and aircraft are closer to each other. (Nichols, et al., Unmanned Aircraft Systems (UAS) in Cyber Domain: Protecting USA's Advanced Air Assets, 2nd Edition, 2019)[3]

Chinese Nightmare

Think of Chinese use of swarming drones on the seas, in the air, floating nuclear power plants, underwater mining, robot freighters and anti-submarine UUVs. In the author's view, they are leapfrogging US technology and antiquating defenses (Lehman, 2017).

It should be clear that the Chinese (PLAN) are heavily invested in military operations using unmanned aircraft and naval vessels in the Spratly Islands. This researcher has been tracking Chinese UAS and Intelligence assets /facilities / naval vessels since 2014. Figure 14.1 shows a glimpse of the deployment in the Spratly Area of Operations (AO). The black pin is the Spratly Islands group. Blue pins represent US Navy capital ships involved in either collisions or groundings in the AO. Red pins represent center of known Chinese UAS Intelligence elliptical paths. Green pins represent Chinese Intelligence facilities or seaborn assets. An exploded map view

would show many more Chinese assets in the AO (Nichols R. &., 4 May 2018).

Given the capabilities that Chinese (and US) UAS systems can deploy in almost any conditions and any location, it seems reasonable to this researcher, that the Chinese military might test their cyber weapons from their UAS in the Spratly AO coverage to harass US vessels and potentially disrupt US Navy capital ships navigation systems. [This would be a natural priority for the Wanshan Marine Test Facility.] As a lesser alternative, the Chinese might take the 911 approach [i.e. turning planes into missiles loaded full of fuel and ramming them straight into fixed buildings] by disrupting (signal spoofing) the GPS /AIS unencrypted signals of huge commercial vessels and forcing them to act as Greek trireme vessels, colliding into the US Naval vessels in restricted maneuverable waters. [4]

Figure 14.1 Chinese UAS Chinese Intelligence Assets Deployment in Spratlys

Source: (Nichols R. &., 4 May 2018)

Marine Transportation System / Sector (MTS) Scope

To their credit, Kessler and Shepard have a wonderful description of the MTS. (Kessler, 2020) Its size /scope and value to the economy as well as the enormity and complexity of its cyber structure cannot be overestimated. *The MTS represents a very large cyberthreat surface, given every system with it represents a potential attack vector*. (Kessler, 2020)

The MTS comprises ships, shipping lines, ports, passenger terminals, manufacturers, cargo facilities, intermodal partners, and all users of these facilities globally. Every element represents a potential vulnerability to cyber attack – a potential weak point to cyberthreats – and a vector for infection of other elements in the MTS. (Kessler, 2020) By 2023 there are expected to be more than 70,000 merchant vessels on the water operating in / out of approximately 4,800 ports in 200 countries. Merchant ships don't make money if they sit idle, they are in constant motion. (Kessler, 2020) All modes of transportation interact with each other as cargo and passengers move be to disposal, tween ships, inland waterways, railroad cars, trucks, and airplanes. Intermodal connections are additional vectors for cybersecurity threats.

(Kessler, 2020) describe the MTS as a system of systems comprising of six interconnected systems: ships, ports, people, shipping lanes, inland waters, and intermodal transfers.

MTS Systems / Sector

The Ships subsystem includes all aspects of in the lifecycle of a vessel, from manufacturing, to maintenance, to operations, communications, networks, security, and navigation systems.

The Ports subsystem includes construction, maintenance, logistics, vessel traffic management, and daily port operations.

The People subsystem includes the entire supply chain, trading partners, vendors, and customers.

The Shipping Lanes subsystem comprises the operation and management of companies that own ships, passengers and cargo, reservation and scheduling, finances, operations, and communications.

The Inland Waters subsystem includes the inland waterway systems, Aids to navigation (ATN), Notice to Mariners (NTM) and dredging and maintenance.

The intermodal Transfer subsystem describes the MTS interfaces with other transportation modalities, including barge, railroads, trucking and to lesser extent aviation. (Kessler, 2020)

MTS Scope

The MTS is a significant economic driver for the nation. It contributes about $5 trillion annually to the GDP, supports 30 MM jobs, representing 20% of the workforce. It includes 25,000 miles of navigable channels, 95,000 miles of shoreline, 361 commercial ports, 50,000 federal and millions of private aids to navigation (ATNs) / (ATONs), 20,000 bridges over water, greater than 3700 marine terminals, 200 ferry operations, 238 locks at 192 locations. The MTS user community includes hundreds of thousands of small fishing , sightseeing, liveaboard, dive boats, and 12 million recreational boats. MTS waterways are shared by military, public safety, LEO vessels; work boats, dredge boats, buoy tenders; commercial fishing vessels; personal power boats and sailing vessels; and drilling platforms , wind turbines, moorings, and fixed location offshore facilities. (Kessler, 2020)

It should be clear that the MTS environment comprises countless moving parts, each playing a critical role in maritime transportation safety and operations. Each represents a potential attack vector *through their associated computer networks.*

MTS Cyber Attack Vectors / Targets

Most maritime cyber-attacks are via operational computer

networks. In general, they are not designed for robust security nor are they modern.[5] (Kessler, 2020) identifies eight critical cyberattack vectors in the MTS: vessel operation, shipping line operations, port operations, cargo and transit, manufacturing, vessel traffic control (VTC), remote control and autonomous operations and partners.

Vessel operations: Ships are floating networks. They include operational networks controlling ships systems, security and cargo management, bridge controls for navigation, weapons control, and lad / ship to ship / satellite communications.

Shipping line operations: cargo and passenger shipping lines have complex outward facing networks and internal networks. They use the public internet for public relations, e-commerce, reservations, partner portals, reservations, cargo tracking and sales / marketing information. Internal networks handle all the vessel operations above plus payroll, taxes, logistics, legal compliance, route management and partner relations.

Port operations: networks handle all the shipping line functions, vessel tracking, USCG operations, vessel traffic management (VTM),immigration, drug enforcement, cargo security, and links to intermodal carriers.

Cargo and shipping: cargo-related operations include SCADA systems to move cargo, onloading / offloading, port cranes, security at several stages, inspections, and autonomous systems.

Manufacturing: All the functions of the port are seen through the eyes of its supporting manufacturers and vendors. Critical to the security is supply chain management, intellectual property protection, and ID theft resolution.

VTC: Managing the flow of vessels, especially in a busy port or narrow body of water requires reliable communications; positioning, navigation, and timing (PNT) systems. Automatic Identification Systems (AIS), NTM, are critical to safe operations. Each of these systems provides a fertile line of cyber-attack in geographic areas than can tolerate a low margin of error. VTC does

not control the recreational or commercial fishing vessels. (Kessler, 2020)

Remote control and autonomy: Unmanned and autonomous vehicles and vessels, are emerging as

shortage of qualified personnel becomes more acute. Remote control ships, tugs, docking facilities, drones, trucks, and cranes are sprouting up like weeds. Each can be manipulated independent of the owner /operator. The author did a simulation of taking over an oil company's storage facilities and SCADA systems to pour 12 MM gallons of oil into the Chesapeake Bay. The environmental damage was in the billions and loss of services, crab industry, effects on the recreational boating industry took a decade to recover. (Nichols R. K., Nov 28-30 2006)

Partners: Vulnerable computer network systems can be exploited as a jumping point on to a more fertile target. Attackers do not want your computers or your networks; they want your information. That is the very definition of partner in the context of cybersecurity. A partner is any entity that affects, the chain of custody of your data. Last point, the IT structure in many organizations are shared ownership. In terms of security, this is akin to sharing a hypo needle for cocaine. Organizations use the cloud as a host. Reservations, ticketing, are managed by an e-commerce host. It is linked to a financial system. This is nuts of course. So many ID frauds and compromised credit cards in huge numbers ought to tell us this. Corporate networks general use VPNs to provide access to their internal network via a public internet.

Civilian ships have multiple onboard networks to handle ballast, propulsion, power, status monitoring and provides a pathway to communicate with their land-based counterparts. GPS, AIS, VHF, and VTS communicate over public radio channels. (Kessler, 2020)

The MTS represents a huge cyber threat surface, given that every system within it represents a potential attack vector. (Kessler, 2020)

Cyber-Physical Systems, Operational Technology, and the Internet of Things (IoT)

Cyber-physical systems(CPS) is the global term encompasses people, computers, and physical devices into an operational system. CPS takes advantage of sophisticated sensors, instruments, networks, embedded computers, SCADA brains, and combines them into smart infrastructures and industrial applications. CPS applications run the whole gamut from the smart grid; medical monitoring; autonomous vehicles, vessels, aircraft; process control systems; robotics systems; and automatic aviation and maritime navigation systems. (Kessler, 2020).

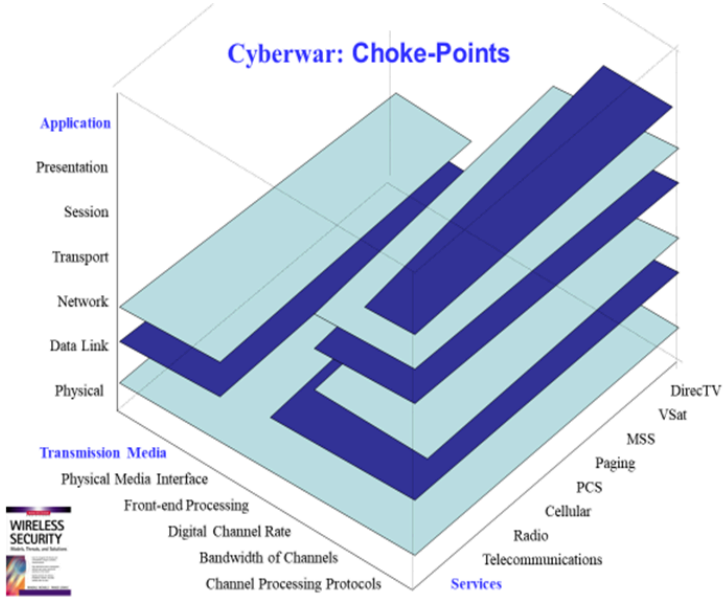


Figure 14.2 Cyberwar: Chokepoints

Source: (Nichols R.K, 2002)

There are lots of views / models of CPS systems. Figure 14.2 shows a differentiation of computer “choke points” (vulnerable to cyberattacks in cyberwar scenario) based on network parameters,

transmission media, applications, and services. Figure 14.3 shows the interaction between physical and cyber systems and how they leverage each other.

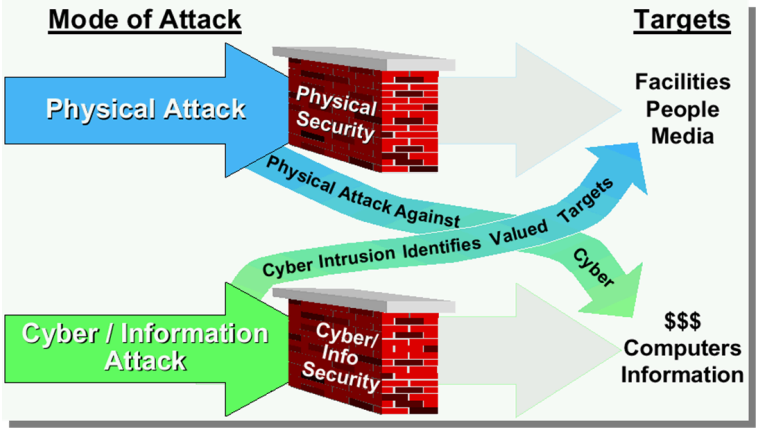


Figure 14.3 Shared Cyber Threats in CPS System

Source: (Nichols R. K., Nov 28-30 2006)

Figure 14.4 shows the complex interdependencies between Infrastructure and the SCADA controls that dictate the inter-flows in a CPS system.

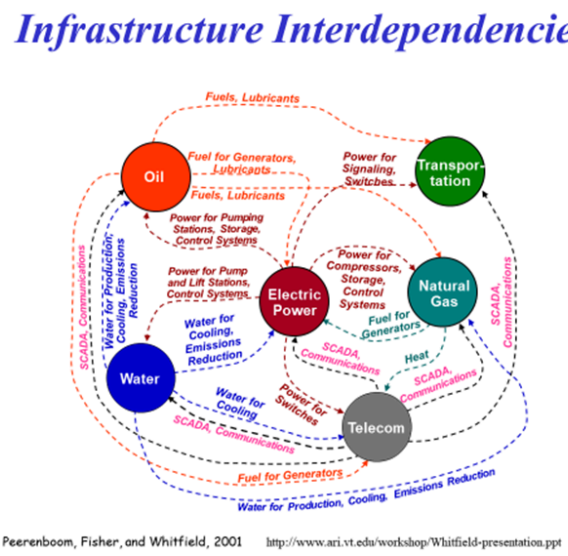


Figure 14.4 shows SCADA and Infrastructure interdependencies in a CPS System

Source: (Peerenboom, 2001)

Operational Technology (OT) comprises the technologies and methods that enable the cyber and physical worlds to interact. In OT systems, computers directly provide real-time monitoring, and control of physical devices such as valves, pumps, dams, power grids, robots and transportation systems. Industrial Control Systems (ICS) make up the largest OT devices. SCADA is the control brains of these systems and represents the preferential vector for cyberattacks. (Randall K. Nichols, 2000) (Nichols R. K., Nov 28-30 2006) (Kessler, 2020)

Internet of Things (IoT)

The Holy Grail of CPS is the Internet of Things (IoT)! IoT combines data analytics, artificial intelligence (AI), wide available broadband networks (WABN), advanced sensor technology, miniaturized processors, embedded ASICS,[6] and advanced software to allow independent devices to share all kinds of information and engage

in network-wide decision making. This transforms traditional physically limited devices into smart equivalents. (Kessler, 2020) IoT devices number in the multi-billions. IoT applications are found in every business and infrastructure and home. They are single reason that privacy is a thing of the past. {I have taught my students the theory behind hacking the house smart electrical meter (installed in about 80% of homes without their permission or realization how much privacy and control of their lives was lost). The meter-hack can tell the Bad Actor how many times you flush your toilet, use the microwave, the frequencies behind your security systems, or turn lights off /on or even charge your phone. All without the user knowledge or permission. IoT!}

Computers within CPS and IoT networks are prone to the same threats and vulnerabilities with any other architecture BUT the span of control has a much larger purview. Unsecured IoT devices are a very real threat to the global internet and attached devices. They are the favorite target for criminals. Websites like censys.io and shodan.io allow people to search the internet for IoT devices where one can find passwords to hacked IoT devices. Many of them crack security monitoring / credit monitoring services.

Maritime CPS Applications and Cybersecurity

The trend is to increase automation systems on vessels. The trends is also miniaturization and to some extent replace people. The USN is doing this at David Taylor Research Center in Annapolis , MD. There goal is to automate vessels and reduce the crew size. The author has been on some of these experimental ships.

There is no doubt that automation has safety and economic benefits and achieve precise solutions to navigation scenarios. But more systems also means increasing interdependencies and more risky cyber vulnerabilities. New ICS and IoT technologies have enabled innovations inside the ship envelope and outside. From bridge to the engine room, system designers have endeavored to

build more integrated shipboard control systems (ISCS) and make the supply chain operations and fuel systems more efficient.

New IoT technologies have enabled innovative systems outside of the ship:

- ü Intelligent mooring systems with embedded sensors in mooring lines. From the bridge, these monitor tension, time, temperature, and predict early failure or wear. (Kessler, 2020)
- ü Supplement Interactive Electronic Maintenance Manuals (IETM) and optimize outcomes.
- ü Act as building blocks for a Cooperative Cognitive Maritime Cyber Physical System (CCMCPS) to provide high-speed, low-cost communications between ships, ports, buoys,offshore platforms, and shore stations. This includes automation of the cranes and transport vehicles. Ports are the bottleneck for movement of cargo. CCMCPS optimizes communication between vessels, ports, maritime terminals and cargo handling systems. (Kessler, 2020)

Autonomous maritime systems are starting to incorporate drones, UAVs to provide surveillance, situational awareness in a port area, for both manned and unmanned ships. UAVs supplement ship inspections by their ability to safely enter locations too dangerous for people. They are used for a detailed analysis of hull or cargo bay in real-time. They supplement autonomous tugs and mooring systems by transporting heaving lines from the dock or tug or ship. (Kessler, 2020)

Conclusions

IoT, ICS and autonomous maritime systems are technologies bringing the maritime industry into the future. While the individual devices are small the systems they interact with are large, complex, and complete with cybersecurity issues because fundamentally, they are merely computer hardware, software, SCADA, and communications technologies.

Student Questions

1. Make a taxonomy of the top cybersecurity attacks on the MTS and needed cyber defenses to reduce risk in the chosen targets.
2. Where do you see the IoT landscape in terms of cyber attack payloads on MTS.
3. There is no silver bullet to protect the MTS "elephant." So develop an initial plan to protect the "part of the elephant" subsystem in the MTS that offers the biggest return on investment (lowers risk of cyber attacks).

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. (2015). *EW Against a New Generation of Threats*. Boston: 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*.

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.

Balduzzi, M. W. (2014). A *Security Evaluation of AIS.* Retrieved from Trend Micro: https://www.acsac.org/2014/program-final/oc_multifile/3/62.pdf

Barnhart, R. K. (2012). *Introduction to Unmanned Aircraft Systems.* New York: CRC Press.

Beaudoin, L. e. (2011). Potential Threats of UAS Swarms and the Countermeasures Need. *ECIW.*

Dalamagkidis, K. V. (2012). *On Integrating Unmanned Aircraft into the National Airspace System, 2nd edition.* Denver, CO: Springer.

Department of the US Navy, Office of Chief of Naval Operations. (2017, November 29). *Report on the USS Lake Champlain Collision.* Retrieved from www.documentcloud.org/documents/: https://www.documentcloud.org/documents/4316708-171129-USS-Lake-Champlain-Collision-Report.html

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

DTRA. (2019, October 18). Private Communication re Aviation Vulnerabilities. (Nichols, Interviewer) Retrieved from https://www.dtra.mil/

Durham, W. (2013). *Aircraft Flight Dynamics and Control.* The Atrium, Chesterton, UK: Wiley.

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

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.

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/

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, E. (1978). *Fundamentals of Computer Algorithms*. Potomac, MD: Computer Science Press.

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

Humphreys, T. e. (2009, January 1). *Assessing the Spoofing Threat: Development of a Portable Civilian GPS Spoofer*. Retrieved from Cornell University: https://gps.mae.cornell.edu/humphreys_etal_iongnss2008.pdf, Cornell University

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

Kessler, G. &. (2020). *Maritime Cybersecurity: A Guide for Leaders and Managers.* Daytona Beach, FL: Kessler & Shepard (Self-published) ISBN: 979-867-6215354.

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

Lehman, C. (2017, August 29). *China Increasing Drone Operations in Disputed Seas, Freebeacon.* Retrieved from Freebeacon: http://freebeacon.com/author/charles-lehman

Lipschutz, M. (1969). *Schaum's Outline for Differential Geometry.* NYC: McGraw-Hill .

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

Marshall, D. M. (2016). *Introduction to Unmanned Aircraft Systems, 2nd Edition.* New York: CRC Press.

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.

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

N/A. (2020, July 25). *Cambridge Dictionary online.* Retrieved from dictionary.cambridge.org/us/: https://dictionary.cambridge.org/us/

NASA. (2018). *Unmanned Aircraft Systems (UAS) Integration in the National Airspace System (NAS) Project.* Retrieved from NASA: https://www.nasa.gov/feature/autonomous-systems

Navy Information Office . (2017, November 1). *Navy Releases Collision Report for USS Fitzgerald and USS John S McCain Collisions.* Retrieved from Story Number: NNS171101-07: Story Number: NNS171101-07Release Date: 11/1/2017 9:01:00 AM

Nichols, R. &. (4 May 2018). *RSCAD Presentation of Research to KSUP Faculty on Deployment of Chinese Cyber-weapons and GPS spoofing of Naval Vessels.* Salina, KS: KSU.

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. (Nov 28-30 2006). *Presentation on Cyber Terrorism, Critical Infrastructure and SCADA .* Shirlington, VA: Defense Threat Reduction Agency Conference.

Nichols, R. K., Mumm, H. C., Lonstein, W. D., Ryan, J. J., Carter, C. M., & & Hood, J. P. (2020). *Counter Unmanned Aircraft Systems Technologies & Operations.* Manhattan, KS: New Prairie Press #31.

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. L. (2002). *Wireless Security : Threats, Models, Solutions.* Washington, DC: McGraw Hill.

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., Ryan, J., Mumm, H., Carter, C., Lonstein, W., & Hood, &. J. (2020). *Counter Unmanned Aircraft Systems Technologies and Operations.* Manhattan, KS: New Prairie Press #31.

Nichols, R., Ryan, J., Mumm, H., Lonstein, W., Carter, C., & & Hood, J. (2019). *Unmanned Aircraft Systems (UAS) in Cyber Domain:*

Protecting USA's Advanced Air Assets, 2nd Edition. Manhattan, KS: New Prairie Press #27 .

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.

Olson, W. (August 30,2017). *Adm No Evidence of Hacking in McCain Fitzgerald Collisions pdf.* Washington: Stars and Stripes.

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

Peerenboom, F. &. (2001). *Whitfield Presentation ppt re Infrastructure Interdependencies.* Retrieved from ari.vt.edu/workshop: http://www.ari.vt.edu/workshop/whitfield-presentatrion.ppt

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*.

Reklaitis, G. R. (1983). *Engineering Optimization: Methods and Practices.* Boston: Wiley.

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.*

Skolnik, M. (2008). *Radar Handbook, 3rd Edition.* Boston: McGraw Hill.

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

Spratly. (1955). *Spratly Islands Fact Page.* Retrieved from Library of Congress: http://hdl.loc.gov/loc.gmd/g9237s.ct002223

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

Tewari, A. (2011). *Advanced Control of Aircraft, Spacecraft and Rockets.* Chichester, UK: Wiley.

Tsourdos, A. &. (2011). *Cooperative Path Planning of Unmanned Aerial Vehicles* . Reston, VA: American Institute of Aeronautics and Astronautics, Vol #235.

Warner, J. &. (2013). *A Simple Demonstration That the Global Positioning System (GPS) is Vulnerable to Spoofing.* Retrieved from Journal of Security Administration: https://pdfs.semanticscholar.org/8ddb/89f56dd3e2ae265047822bc47cfb06815d9a.pdf, LAUR-03-6163

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. (2020, July 26). *A* Algorithm.* Retrieved from Wikipedia: https://en.wikipedia.org/wiki/A*_search_algorithm

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*.

WWF. (2019, July 25). *South China Sea, between the Philippines, Borneo, Vietnam, and China.* Retrieved from worldwildlife.org/ecoregions/: https://www.worldwildlife.org/ecoregions/im0148

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

Zhang, Z. W. (2020). Rapid Penetration Path Planning Method for Stealth UAV in Complex Environment with POP-UP Threats. *International Journal of Aerospace Engineering*, TBA.

[1] (Kessler, 2020) discuss exactly this kind of scenario in their Preface. This excellent book is highly recommended for purchase. https://www.amazon.com/Maritime-Cybersecurity-Guide-Leaders-Managers/dp/B08HBDDSQD/ref=sr_1_1?dchild=1&keywords=kessler+Maritime+Cybersecurity&qid=1600025530&sr=8-1

[2] The full case with equations of closest point of approach (CPA) are given in www.newprairiepress.org/ebooks/27/

[3] The South China Seas GPS scenario is the sole speculation of the author based on his research and proposals during 2017-2018. It is not the opinion of KSU, NPP, CADS or any official in the line of publication. The USN has admitted that cybersecurity of its systems and commercial vessels has vulnerabilities. They have devoted significant resources to the cybersecurity threats / subject under command of an Admiral. There is significant work to mitigate these navigational threats.

[4] Triremes were used in the Peloponnesian Wars to ram at about 4 knots at a 60-degree angle of attack. The greater the angle of attack the lesser the speed requirement for ramming. What is interesting is that the Athenians used a multi-trireme attack, an early predecessor to Swarm tactics. They also used grappling hooks to engage the enemy ships directly up close. This was the predecessor to piracy tactics in the 1500's – 1830's. Wikipedia.

[5] Authors evaluation based on his research at KSU.

[6] ASICs= Application specific integrated Circuits & circuit boards

Appendices Chapters 10 & 12

Chapter 10: UAS, the Fourth Amendment and Privacy [Shay]

Appendix A – Summary of UAS Provisions in H.R. 302 (Association for Unmanned Vehicle Systems International, 2018)

SEC. 343. UNMANNED AIRCRAFT TEST RANGES.

The Administrator is directed to carry out and update a program for the use of six test ranges to facilitate the safe integration of unmanned aircraft systems into the national airspace. The program will coordinate with the Next Generation Air Transportation System and test range operators to develop standards for UAS that support UAS capabilities specific to beyond visual line of sight operations, nighttime operations, operations over people, operation of multiple UAS, and unmanned aircraft system traffic management. The Administrator is directed to collaborate with the Center of Excellence for Unmanned Aircraft Systems to carry out research supporting the above operations. Waivers for operations at test sites to support the above research will be streamlined.

SEC. 344. SMALL UNMANNED AIRCRAFT IN THE ARCTIC.

The Secretary of Transportation shall develop a plan to designate permanent areas in the Arctic where small unmanned aircraft may operate 24 hours per day, for research and commercial purposes. These operations include UAS operations beyond visual line of sight and below 2,000 feet in altitude.

SEC. 345. SMALL UNMANNED AIRCRAFT SAFETY STANDARDS.

The Administrator shall establish risk-based safety standards related to design, production, and modification of small UAS. The geographic location, altitude, and sense and avoid capabilities shall be taken into consideration when establishing such standards using a set of performance-based requirements. Manufacturers will be required to provide the FAA: aircraft operating instructions, maintenance procedures, be subject to inspections by FAA to

ensure compliance of aircraft and be required to provide a statement of compliance to the FAA for UAS platforms. The Center of Excellence for Unmanned Aircraft will establish an UAS research facility to study appropriate safety standards.

SEC. 346. PUBLIC UNMANNED AIRCRAFT SYSTEMS.

The Administrator shall create a streamlined process for issuance of a certificate of authorization to facilitate the capability of public agencies to develop and use test ranges. Government public safety agencies may operate an UAS under 4.4 pounds within visual line of sight, less than 400 feet above the ground, during daylight and at least 5 miles from an airport.

SEC. 347. SPECIAL AUTHORITY FOR CERTAIN UNMANNED AIRCRAFT SYSTEMS.

The Secretary shall use a risk-based approach to determine if certain UAS may operate safely in the national airspace prior to the completion of certain rulemakings if operations do not create a hazard to users of the national airspace system or the public.

SEC. 348. CARRIAGE OF PROPERTY BY SMALL UNMANNED AIRCRAFT SYSTEMS FOR COMPENSATION FOR HIRE.

Within one year of bill passage, the FAA shall update existing regulations to authorize the carriage of property by operators of small UAS for compensation or hire, considering performance-based requirements and varying levels of risk to other aircraft and people or property on the ground. The FAA shall create a certification process pending a rulemaking for persons seeking the carriage of property for hire.

SEC. 349. EXCEPTION FOR LIMITED RECREATIONAL OPERATIONS OF UNMANNED AIRCRAFT.

This section states that a person may operate a small UAS without certification or operating authority from the FAA if: the aircraft is flown for recreational purposes, the aircraft is operated in accordance with a community- based organization's safety guidelines developed in coordination with the FAA, is flown within visual line of sight, does not interfere with manned aircraft, is flown

below 400 feet above the ground, the operator passes an online aeronautical knowledge and safety test, and the aircraft is registered with the FAA. The FAA may periodically update the required community-based organization standards including the marking and remote identification requirements flying under these recreational parameters.

SEC. 350. USE OF UNMANNED AIRCRAFT SYSTEMS AT INSTITUTIONS OF HIGHER EDUCATION.

The Administrator shall update standards and procedures for the use of UAS at institutions of higher education for education and research purposes.

SEC. 351. UNMANNED AIRCRAFT SYSTEMS INTEGRATION PILOT PROGRAM (IPP).

The Administrator shall improve the acceptance of applications from state, local, or tribal jurisdictions for the IPP to accelerate the safe integration of UAS in the national air space with the focus of testing and validating new concepts, including beyond visual line of sight operations, detect and avoid technologies, command and control links, navigation, weather, and human factors. IPP operations are limited to operation during daylight hours, and limited operations over public roads and sporting events. The data from IPP operations will be made available to the FAA to inform future rulemaking and standards.

SEC. 352. PART 107 TRANSPARENCY AND TECHNOLOGY IMPROVEMENTS.

No later than 30 days after bill passage, the Administrator shall publish a sample of the safety justifications offered by applicants for small UAS waivers and airspace authorizations that have been approved by the Administrator. The Administrator shall review the authorization process to provide real time confirmation and review of application status capabilities.

SEC. 353. EMERGENCY EXEMPTION PROCESS.

The Administrator shall update the Special Government Interest process for local law enforcement agencies and first responders to

use UAS in response to catastrophe, disaster, or other emergency situations in addition to developing best practices for such uses.

SEC. 354. TREATMENT OF UNMANNED AIRCRAFT OPERATING UNDERGROUND.

An unmanned aircraft system that is operated underground for mining purposes shall not be subject to regulation or enforcement by the FAA under relevant law.

SEC. 355. PUBLIC UAS OPERATIONS BY TRIBAL GOVERNMENTS.

This section amends a section of the U.S. Code relating to public UAS operations by tribal governments.

SEC. 356. AUTHORIZATION OF APPROPRIATIONS FOR KNOW BEFORE YOU FLY CAMPAIGN.

The FAA is appropriated $1,000,000 for each fiscal year 2019-2023 for the Know Before You Fly educational campaign to broaden UAS safety awareness.

SEC. 357. UNMANNED AIRCRAFT SYSTEMS PRIVACY POLICY.

UAS operations shall be carried out in a manner that respects and protects personal privacy consistent with the United States Constitution and federal, state, and local law.

SEC. 358. UAS PRIVACY REVIEW.

The Comptroller General of the United States National Telecommunication and Information Administration shall review privacy issues and concerns associated with UAS operations. Such a review will include analysis of the response to the Presidential memorandum titled "Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems," dated February 15, 2015, as well as examine existing federal law related to personal privacy, identify specific issues and concerns that may limit the civil or criminal remedies regarding inappropriate operation of UAS, and identify deficiencies in federal, state, and local privacy protections. Such findings will be submitted in a report to Congress 180 days after passage of this bill.[1]

SEC. 359. STUDY ON FIRE DEPARTMENT AND EMERGENCY SERVICE AGENCY USE OF UNMANNED AIRCRAFT SYSTEMS.

The Administrator shall conduct a study on the use of UAS by fire departments and emergency service agencies regarding how such entities currently use UAS, obstacles to greater use of UAS by these entities, ways to provide greater support of UAS use by these entities, analysis of laws or regulations that present a barrier to career, combination, and volunteer fire department use of UAS, airspace limitations of emergency use of UAS, roles of UAS in fire/emergency services, and technical challenges to greater adoption of UAS by fire departments and emergency agencies.

SEC. 360. STUDY ON FINANCING OF UNMANNED AIRCRAFT SERVICES.

The Comptroller General of the United States shall conduct a study within 60 days of passage of the bill that studies appropriate fee mechanisms to recover costs of regulation and safety oversight of UAS and air navigation services for UAS. The study shall consider any recommendations of the Drone Advisory Committee, the costs incurred by the FAA for regulation and safety oversight of UAS, general classes of UAS activity, the number of FAA employees dedicated to UAS programs, the use of privately-operated unmanned traffic management (UTM) systems, and the projected growth of UAS, among other factors. A report of appropriate fee mechanisms will be provided to Congress 180 days after the passage of the bill.

SEC. 361. REPORT ON UAS AND CHEMICAL AERIAL APPLICATION.

No later than one year after passage of the bill the FAA shall submit to Congress a report evaluating which aviation safety requirements under Part 137 of title 14 of the Code of Federal Regulations should apply to UAS engaged in aerial spraying of chemicals for agriculture purposes.

SEC. 362. SENSE OF CONGRESS REGARDING UNMANNED AIRCRAFT SAFETY.

It is the sense of Congress that UAS operations near airports

pose a significant safety concern. The Administrator should pursue remedies available, including referrals to other government agencies for criminal investigations with respect to persons who operate unmanned aircraft in an unsafe manner. The Administrator should prioritize measures to educate the public about operating UAS over areas that have temporary flight restrictions in place due to the risk of wildfires, as well as partner with state and local law enforcement to enforce laws so that UAS do not interfere with efforts of emergency responders. Manufacturers should take steps to educate consumers about safe and lawful UAS operations.

SEC. 363. PROHIBITION REGARDING WEAPONS.

Unless authorized by the Administrator, a person may not operate a UAS that is equipped or armed with a dangerous weapon. Persons in violation are liable for a civil penalty not more than $25,000 for each violation.

SEC. 364. U.S. COUNTER-UAS SYSTEM REVIEW OF INTERAGENCY COORDINATION PROCESSES.

No later than 60 days after passage of this bill the Administrator shall review agencies currently authorized to operate Counter-Unmanned Aircraft Systems (C-UAS). The review should include the process of interagency coordination of C-UAS activity, standards for operation of C-UAS, safety of the NAS, protecting individuals' property on the ground, non-interference with avionics of manned aircraft and traffic control systems, operational procedures and protocols during C-UAS operations, adequate training for persons using C-UAS systems, best practices of C-UAS systems, and current airspace authorization information from LAANC. The Administrator shall report to congress on the above described review 180 days after passage of the bill.

SEC. 365. COOPERATION RELATED TO CERTAIN COUNTER UAS TECHNOLOGY.

The Secretary of Transportation shall consult with the Secretary of Defense to streamline deployment of C-UAS in the national airspace.

SEC. 366. STRATEGY FOR RESPONDING TO PUBLIC SAFETY

THREATS AND ENFORCEMENT UTILITY OF UNMANNED AIRCRAFT SYSTEMS.

Within one year of passage of the bill, the FAA shall develop a comprehensive strategy to provide outreach to state and local governments, local law enforcement agencies, and first responders on how to identify and respond to public safety threats posed by UAS, in addition to opportunities to use UAS to enhance effectiveness of local law enforcement and emergency responders. The FAA shall establish a website for the above entities that provides guidance on these topics.

SEC. 367. INCORPORATION OF FEDERAL AVIATION ADMINISTRATION OCCUPATIONS RELATING TO UNMANNED AIRCRAFT INTO VETERANS EMPLOYMENT PROGRAMS OF THE ADMINISTRATION.

The FAA will work with the Veterans Affairs Department to determine whether occupations in the Administration relating to UAS can be incorporated into the Veterans' Employment Program.

SEC. 368. PUBLIC UAS ACCESS TO SPECIAL USE AIRSPACE.

The Secretary of Transportation shall issue guidance for the expedited and timely access to special use airspace for public UAS to assist federal, state, local, or tribal law enforcement organizations in conducting law enforcement, emergency response, or other activities.

SEC. 369. APPLICATIONS FOR DESIGNATION.

This section makes corrections to now consider railroad facilities as critical infrastructure that could potentially restrict the nearby operation of UAS. It also mandates that by 31 March the Administrator will publish an NPRM regarding how to carry out the requirements outlined in this section.

SEC. 370. SENSE OF CONGRESS ON ADDITIONAL RULE-MAKING AUTHORITY.

It is the sense of Congress that UAS beyond visual line of sight operations, operations at night, and operations over people have tremendous potential to enhance commercial and academic use,

spur economic growth, improve emergency response as it relates to critical infrastructure like roads, bridges, utilities, water and power, ultimately speeding response times. Integrating UAS safely into the national air space including the above operations should be a top priority of the FAA as it pursues additional rulemakings.

SEC. 371. ASSESSMENT OF AIRCRAFT REGISTRATION FOR SMALL UNMANNED AIRCRAFT.

The Secretary of Transportation and the National Academy of Public Administration will estimate and assess compliance of small UAS registrations pursuant to the FAA rule "Registration and Marking Requirements for Small Unmanned Aircraft." The Secretary shall report to Congress the findings of the assessment one year after passage of this bill.

SEC. 372. ENFORCEMENT.

The Administrator shall establish a pilot program to take advantage of available remote identification technologies for purposes of safety and enforcement of UAS operators not in compliance with applicable federal laws and regulations. The pilot program will establish a mechanism for the public and law enforcement to report UAS operations that violate federal laws and regulations. The data from that reporting shall be reported to Congress one year after passage of the bill.

SEC. 373. FEDERAL AND LOCAL AUTHORITIES.

A study will be conducted on the roles of federal, state, local, and tribal governments in regulating low-altitude operations of UAS. The study shall include the state of law federally and locally as it pertains to UAS, potential gaps in authority, analysis of regulatory consistency, and infrastructure requirements necessary to monitor low-altitude UAS operations[2].

SEC. 374. SPECTRUM.

The FAA shall provide the relevant Congressional Committees of Jurisdiction a report on UAS allocation of Aeronautical Mobile R Service (AM(R)S) and control links for UAS by the World Radio Conferences in 2007 (L-band, 960-1164 MHz) and 2012 (C-band, 5030-5091 MHz) for operations within the UTM system or outside

of such system. The report will address operation barriers to using the spectrum and determine if some spectrum frequencies are not suitable for UAS use.

SEC. 375. FEDERAL TRADE COMMISSION AUTHORITY.

A violation of privacy policy by a person that uses an UAS for compensation or hire in the national airspace shall be an unfair and deceptive practice in violation of section 5(a) of the Federal Trade Commission Act (15U.S.C. 45(a)).

SEC. 376. PLAN FOR FULL OPERATIONAL CAPABILITY OF UNMANNED AIRCRAFT SYSTEMS TRAFFIC MANAGEMENT (UTM)

FAA and NASA shall develop a plan to allow the implementation of UTM services that expand operations beyond visual line of sight and ensure the safety and security of all aircraft as established in the FAA Extension, Safety, and Security Act of 2016. The UTM system pilot program will work with industry stakeholders to allow testing of UAS operations in airspace above test ranges including IPP sites. Testing of remote identification and tracking technologies is permitted and will be evaluated by the Unmanned Aircraft Systems Identification and Tracking Aviation Rulemaking Committee. Under this pilot program, blanket waiver authority will be granted to UAS operators by a UTM pilot program selectee that otherwise would fall under a case-by-case approval basis. The UTM pilot program will develop safety standards and outline roles and responsibilities of industry and government in establishing UTM services that allows commercial and noncommercial operations. This section outlines a number of additional logistical details to be considered in the implementation of the UTM pilot program that are more appropriate to be described in a separate forum.

SEC. 377. EARLY IMPLEMENTATION OF CERTAIN UTM SERVICES.

No later than 120 days from passage of this bill the FAA will determine if certain UTM services may operate safely in the national airspace system. If the FAA determines that certain UTM services

may operate safely in the national airspace, then requirements for safe operations will be established. The Administrator will provide expedited procedures for making the assessment and determinations where the UTM services will be provided primarily or exclusively in airspace above areas in which UAS operations pose low risk, such as croplands and areas that are not congested.

SEC. 378. SENSE OF CONGRESS.

It is the sense of Congress that any person that uses UAS for compensation or hire should have a written privacy policy consistent with section 357 that is appropriate in nature and scope of the activities regarding collection, use, retention, dissemination, and deletion of any data collected during operation of UAS. Such privacy policy should be publicly available.[3]

SEC. 379. COMMERCIAL AND GOVERNMENTAL OPERATORS.

The FAA should make available by website any certification of waiver or authorization, a spreadsheet of UAS registrations with relevant details, description of UAS operations in general locations and expirations of those operations, links to any applicable privacy laws associated with those operations, a list of any operations that collect personably identifiable information and relevant details of the collection of data, and details of the operations of the UAS including location, date, time, etc.

SEC. 380. TRANSITION LANGUAGE.

This section ensures that certain orders, determinations, rules, and other actions based on authority from the FAA Modernization and Reform Act of 2012 continue to have legal effect after their appeal or recodification.

SEC. 381. UNMANNED AIRCRAFT SYSTEMS IN RESTRICTED BUILDINGS OR GROUNDS.

This section amends the United States Code to make it a crime to knowingly operate UAS with the intent to enter or operate within or above restricted areas.

SEC. 382. PROHIBITION. § 40A. OPERATION OF UNATHORIZED UNMANNED AIRCRAFT OVER WILDFIRES

Any person who operates an UAS and knowingly or recklessly

interferes with a wildfire suppression or emergency response efforts related to wildfire suppression shall be fined or imprisoned for not more than two years.

SEC. 383. AIRPORT SAFETY AND AIRSPACE HAZARD MITIGATION AND ENFORCEMENT.

The FAA shall work with Department of Homeland Security (DHS) to ensure that technologies that are used for UAS mitigation do not adversely impact or interfere with safe airport operations, navigation, air traffic services, or the national air space. The FAA shall develop a plan to authorize, permit, and certify UAS mitigation systems and charter an Aviation Rulemaking Committee to provide recommendations on the matter. The FAA shall test UAS mitigation technology at five airports through year 2023. These activities are exempt from laws that previously restrict such activity like the Aircraft Sabotage Act, the Computer Fraud and Abuse Act of 1986, and the Wiretap Act.

SEC. 384. UNSAFE OPERATION OF UNMANNED AIRCRAFT.

Any person that operate an UAS and knowingly interferes with a manned aircraft or an airport, including the runway exclusion zone, shall be fined or face up to one year in jail. If serious bodily harm occurs, then UAS operators face a fine and up to 10 years of jail time.

Appendix B – Summary of CFR 14 Part 107 (Federal Aviation Administration, 2016)

Part 107. OPERATIONAL LIMITATIONS.

- Unmanned aircraft must weigh less than 55 lbs. (25 kg).
- Visual line-of-sight (VLOS) only; the unmanned aircraft must remain within VLOS of the remote pilot in command and the person manipulating the flight controls of the small UAS. Alternatively, the unmanned aircraft must remain within VLOS of the visual observer.
- At all times the small unmanned aircraft must remain close enough to the remote pilot in command and the person

manipulating the flight controls of the small UAS for those people to be capable of seeing the aircraft with vision unaided by any device other than corrective lenses.

- Small unmanned aircraft may not operate over any persons not directly participating in the operation, not under a covered structure, and not inside a covered stationary vehicle.
- Daylight-only operations, or civil twilight (30 minutes before official sunrise to 30 minutes after official sunset, local time) with appropriate anti-collision lighting.
- Must yield right of way to other aircraft.
- May use visual observer (VO) but not required.
- First-person view camera cannot satisfy "see-and-avoid" requirement but can be used as long as requirement is satisfied in other ways.
- Maximum groundspeed of 100 mph (87 knots).
- Maximum altitude of 400 feet AGL or, if higher than 400 feet AGL, remain within 400 feet of a structure.
- Minimum weather visibility of 3 miles from control station.
- Operations in Class B, C, D and E airspace are allowed with the required ATC permission.
- Operations in Class G airspace are allowed without ATC permission.
- No person may act as a remote pilot in command or VO for more than one unmanned aircraft operation at one time.
- No operations from a moving aircraft.
- No operations from a moving vehicle unless the operation is over a sparsely populated area.
- No careless or reckless operations.
- No carriage of hazardous materials.
- Requires preflight inspection by the remote pilot in command.
- A person may not operate a small unmanned aircraft if he or she knows or has reason to know of any physical or mental condition that would interfere with the safe operation of a small UAS.
- Foreign-registered small unmanned aircraft are allowed to

operate under part 107 if they satisfy the requirements of part 375.

- External load operations are allowed if the object being carried by the unmanned aircraft is securely attached and does not adversely affect the flight characteristics or controllability of the aircraft.
- Transportation of property for compensation or hire allowed provided that-
    - o The aircraft, including its attached systems, payload, and cargo weigh less than 55 pounds total.
    - o The flight is conducted within visual line of sight and not from a moving vehicle or aircraft; and
    - o The flight occurs wholly within the bounds of a state and does not involve transport between (1) Hawaii and another place in Hawaii through airspace outside Hawaii; (2) the District of Columbia and another place in the District of Columbia; or (3) a territory or possession of the United States and another place in the same territory or possession.
- Most of the restrictions discussed above are waivable if the applicant demonstrates that his or her operation can safely be conducted under the terms of a certificate of waiver.

Part 107. REMOTE PILOT IN COMMAND CERTIFICATION AND RESPONSIBILITIES.

- Establishes a remote pilot in command position.
- A person operating a small UAS must either hold a remote pilot airman certificate with a small UAS rating or be under the direct supervision of a person who does hold a remote pilot certificate (remote pilot in command).
- To qualify for a remote pilot certificate, a person must:
    - o Demonstrate aeronautical knowledge by either:
      Passing an initial aeronautical knowledge test at an FAA-approved knowledge testing center; or

§ Hold a part 61 pilot certificate other than student pilot, complete a flight review within the previous 24 months, and complete a small UAS online training course provided by the FAA.
    - o Be vetted by the Transportation Security Administration.
    - o Be at least 16 years old.
- Part 61 pilot certificate holders may obtain a temporary remote pilot certificate immediately upon submission of their application for a permanent certificate. Other applicants will obtain a temporary remote pilot certificate upon successful completion of TSA security vetting. The FAA anticipates that it will be able to issue a temporary remote pilot certificate within 10 business days after receiving a completed remote pilot certificate application.
- Until international standards are developed, foreign-certificated UAS pilots will be required to obtain an FAA-issued remote pilot certificate with a small UAS rating.

A remote pilot in command must:

- Make available to the FAA, upon request, the small UAS for inspection or testing, and any associated documents/records required to be kept under the rule.
- Report to the FAA within 10 days of any operation that results in serious injury, loss of consciousness, or property damage of at least $500.
- Conduct a preflight inspection, to include specific aircraft and control station systems checks, to ensure the small UAS is in a condition for safe operation.
- Ensure that the small unmanned aircraft complies with the existing registration requirements specified in § 91.203(a)(2).

A remote pilot in command may deviate from the requirements of this rule in response to an in-flight emergency.

Part 107. AIRCRAFT REQUIREMENTS.

- FAA airworthiness certification is not required. However, the remote pilot in command must conduct a preflight check of the small UAS to ensure that it is in a condition for safe operation.

Part 107. MODEL AIRCRAFT.

- Part 107 does not apply to model aircraft that satisfy all of the criteria specified in section 336 of Public Law 112-95.
- The rule codifies the FAA's enforcement authority in part 101 by prohibiting model aircraft operators from endangering the safety of the NAS.

Appendix C – Summary of changes due to CoViD-19 pandemic in UAS CFR 14 Part 107 & Part 135 ("Coronavirus guidance & resources from FAA," 2020)

Drone Use for Response Efforts

The FAA is enabling drone use for COVID-19 response efforts within our existing regulations and emergency procedures. Our small unmanned aircraft rule (Part 107) and Certificate of Authorization process allow operators to transport goods and certain medical supplies – including test kits, most prescription drugs and, under certain circumstances, blood – provided the flight complies with all provisions of the rule or authorization. The FAA also issues special approvals, some in less than an hour, for flights that support emergency activities and appropriate government, health, or community initiatives. The agency's Systems Operations Support Center is available 24/7 to process emergency requests. Safety is the top consideration as we review each request.

Expanded Drone Operations

The FAA has received inquiries about expanded drone operations to respond to COVID-19. We are addressing the inquiries using our existing Part 135 on-demand certification process. Follow us on Twitter @FAADroneZone and Facebook @FAADroneZone for the latest drone news.

Relief for Certain Persons and Operations during the COVID-19 Outbreak

The FAA has published a Special Federal Aviation Regulation (SFAR) that provides regulatory relief to a wide range of people and operations affected by the COVID-19 public health emergency. The relief applies to pilots, crew members and other FAA certificate holders including some drone pilots who have been unable to comply with certain training, recency-of-experience, testing, and checking requirements due to the outbreak. It also provides relief to certain people and pilot schools who are unable to meet duration and renewal requirements, including extending the validity period of FAA medical certificates. FAA has developed FAQs (PDF) to help explain the regulatory relief.

References [Chapter 10]

(NASIC), N. A. (2019, July 19). Emerging IADS Threats: Talking Points. *DoD Periodical*.

112 Congress. (2012, February 14). The FAA Modernization and Reform Act of 2012. *H.R. 658*. Washington D.C., United States.

49 U.S. Code §40103. Sovereignty and use of airspace. (1994, July 5). Retrieved July 2020, from law.cornell.edu: https://www.law.cornell.edu/uscode/text/49/40103

Al-Naji, A. P. (2017). Remote monitoring of cardiorespiratory signals from a hovering unmanned aerial vehicle. *Al-Naji, A., Perera, A. G., & Chahl, J. (2017). Remote monitoring of cardiorespiratory siBiomedical Engineering Online*, 16(1). doi: https://doi.org/10.1186/s12938-017-0395-y

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

Association for Unmanned Vehicle Systems International. (2018, September 26). *Summary of UAS Provisions in H.R. 302.* Retrieved April 2020, from auvsilink.org: http://auvsilink.org/AUVSIDocs/AUVSI%20Summary%20of%20HR%20302.pdf

AUVSI Advocacy. (2020, July). *2020 State Legislation Map.* Retrieved July 2020, from cqrcengage.com: https://cqrcengage.com/auvsi/statelegmap

1. Skorup & Haaland, C. (2020, March 1). *Which States Are Prepared for the Drone Industry? A 50-State Report Card. Mercatus Center.* Retrieved from https://www.mercatus.org/: https://www.mercatus.org/system/files/skorup-drone-report-card-mercatus-summary-v1_1.pdf

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/

Bomboy, S. (2014, February 7). A *legal victory for drones warrants a Fourth Amendment discussion.* Retrieved from news.yahoo.com: https://news.yahoo.com/legal-victory-drones-warrants-fourth-amendment-discussion-105607148.html

Bonifacic, I. (2020, April 27). *UPS will use drones to deliver prescriptions to retirees in Florida.* Retrieved May 2020, from engadget.com: https://www.engadget.com/ups-will-use-drones-to-deliver-prescriptions-to-retirees-in-flordia-171337603.html

Breitenbach, S. (2015, September 10). *States Rush to Regulate Drones Ahead of Federal Guidelines.* Retrieved July 2020, from

pewtrusts.org: https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2015/09/10/states-rush-to-regulate-drones-ahead-of-federal-guidelines

Busch, K. a. (2016, February 09). No Denial: How NATO Can Deter Creeping Russian Threat. *www.cer.org.uk/insights* .

Chen, C. (2020, April 9). *Drone-maker DJI rubbishes reports of mass layoffs, says it is busy meeting demand amid pandemic*. Retrieved April 2020, from scmp.com: https://www.scmp.com/tech/gear/article/3079211/drone-maker-dji-rubbishes-reports-mass-layoffs-says-it-busy-meeting

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 .

Davis, H. (2020, July 28). *Texas stadiums helping fight coronavirus with disinfectant-spraying drones*. Retrieved August 2020, from foxnews.com: https://www.foxnews.com/sports/coronavirus-texas-stadiums-disinfectant-spraying-drones

de León, R. (2020, May 27). *Zipline, Novant Health launch the first long-distance emergency drone operation in U.S. to deliver PPE and medical supplies*. Retrieved July 2020, from cnbc.com: https://www.cnbc.com/2020/05/27/zipline-novant-health-launch-us-drone-service-to-fight-pandemic.html

Defense, O. o. (2006). Annual Report to Congress: Military Power of the Peoples Republic of China . *US DoD* , pp. 21, 25. .

Diab, A. (2014, November 13). *Drones perform the dull, dirty, or dangerous work*. Retrieved from tech.co/news/drones-dull-dirty-dangerous-2014-11: https://tech.co/news/drones-dull-dirty-dangerous-2014-11#:~:text=Drones%20perform%20tasks%20generally%20categorized%20into%20the%20%22three,Often%2C%20the%20mission%20c

Dictionary.com. (2020). *Jurisprudence*. Retrieved August 2020, from Dictionary.com: https://www.dictionary.com/browse/jurisprudence

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

Dwyer-Moss, J. (2018). The Sky Police: Drones and the Fourth Amendment. *Albany Law Review*, Vol81_3/1047. Retrieved from Dwyer-Moss, J. (2018). The Sky Police: Drones and the Fourth Amendment. Albany Law Review. https://www.albanylawreview.org/Articles/Vol81_3/1047%20Dwyer-Moss%20PRODUCTION.pdf.

Dwyer-Moss, J. (2020). *Jessica Dwyer-Moss' Profile*. Retrieved July 2020, from LinkedIn.com: https://www.linkedin.com/in/jessicadwyermoss/

FAA. (2015, December 17). *State and Local Regulation of Unmanned Aircraft Systems (UAS) Fact Sheet*. Retrieved July 2020, from FAA.gov: https://www.faa.gov/uas/resources/policy_library/media/UAS_Fact_Sheet_Final.pdf

FAA. (2018, July 20). *Press Release – FAA Statement–Federal vs. Local Drone Authority*. Retrieved July 2020, from FAA.gov: https://www.faa.gov/news/press_releases/news_story.cfm?newsId=22938

FAA. (2018, July 20). *Press Release – FAA Statement–Federal vs. Local Drone Authority*. Retrieved June 2020, from faa.gov: https://www.faa.gov/news/press_releases/news_story.cfm?newsId=22938

FAA. (2020, July 8). *Coronavirus guidance & resources from FAA*. Retrieved from www.FAA.gov: https://www.faa.gov/coronavirus/guidance_resources/

FAA. (2020, April 16). *Regulatory updates due to coronavirus*. Retrieved from www.faa.gov/coronavirus/regulatory_updates/: https://www.faa.gov/coronavirus/regulatory_updates/

Freier, N. (2012). The Emerging Anti-Access/ Area Denial Challenge. *Center for Strategic and International Studies* .

Governing.com. (2020, July 23). *Drone Legislation Map*. Retrieved July 2020, from Governing.com: https://www.governing.com/

next/Legislative-Watch-The-Rise-of-Drones-During-the-Pandemic.html

Hayden, J. (2020, May 19). *Why the Drone Community Should Not Embrace Exclusive FAA Control of Drone Regulations.* Retrieved May 2020, from DroneLife.com: https://dronelife.com/2020/05/19/faa-and-drone-regulation-should-the-faa-have-excusive-control/

Kaminski, M. E. (2013, April 26). *Drone Federalism: Civilian Drones and the Things They Carry.* Retrieved July 2020, from SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2257080

Maynes, C. (2020, May 06). *Behind Russia's Coronavirus Fight, a Surveillance State Blooms.* Retrieved May 2020, from voanews.com: https://www.voanews.com/europe/behind-russias-coronavirus-fight-surveillance-state-blooms

McNabb, M. (2020, July 15). *LAANC Use Accelerates: Kittyhawk Reports All-Time Record Levels of Activity.* Retrieved July 2020, from dronelife.com: https://dronelife.com/2020/07/15/laanc-use/

McNabb, M. (2020, July 14). *Matternet and UPS Expand Hospital Delivery Network.* Retrieved 2020 July, from dronelife.com: https://dronelife.com/2020/07/14/matternet-and-ups-expand-hospital-delivery-network/

National Conference of State Legislatures. (2020, April 1). *Current Unmanned Aircraft State Law Landscape.* Retrieved June 2020, from ncsl.org: https://www.ncsl.org/research/transportation/current-unmanned-aircraft-state-law-landscape.aspx

Obama, B. (2015, February 15). *Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems.* Retrieved April 2020, from hsdl.org: https://www.hsdl.org/?view&did=762711

Orwell, G. (1949). *Nineteen Eighty Four: A Novel.* United Kingdom: Secker & Warburg.

Posen, B. (2003). Command of the Commons: The Military Foundation of US Hedgemony. *International Security, Vol 28, No1.* , pp. 5-46 .

Rouse, C. (2016, December). *What is disruptive technology? – Definition from WhatIs.com.* Retrieved from WhatIs.com:

https://whatis.techtarget.com/definition/disruptive-technology#:~:text=A%20disruptive%20technology%20is%20one%20that%20displaces%20an,Clayton%20M.%20Chris

Rupprecht, J. (2020, June 4). *Ultimate Guide to Drone Laws [2020] Written by a Lawyer*. Retrieved from jrupprechtlaw.com/drone-laws/: https://jrupprechtlaw.com/drone-laws/

Rupprecht, J. (n.d.). *Drone Legislation Directory*. Retrieved June 2020, from jrupprechtlaw.com: https://jrupprechtlaw.com/drone-legislation/

Seeking Alpha. (2019, January 22). *Robotics: Unmanned Traffic Management (UTM) Systems Outlook*. Retrieved April 2020, from seekingalpha.com: https://seekingalpha.com/article/4234878-robotics-unmanned-traffic-management-utm-systems-outlook

Sella-Villa, D. (2020, July 24). *David Sella-Villa's Profile page*. Retrieved July 2020, from LinkedIn: https://www.linkedin.com/in/dsellavilla/

Sella-Villa, D. (2020, January 30). Drones and Data: A Limited Impact on Privacy. *University of Richmond Law Review, Forthcoming*.

Smentkowski, B. P. (2020, July 12). *Fourth Amendment*. Retrieved from www.britannica.com/topic/Fourth-Amendment: https://www.britannica.com/topic/Fourth-Amendment#:~:text=Fourth%20Amendment%2C%20amendment%20%281791%29%20to%20the%20Constitution%20of,the%20text%20of%20the%20Fourth%20Amendment%2C%20see%20b

Smith, C. (2020, April 3). *Legislative Watch: The Rise of Drones During the Pandemic*. Retrieved April 2020, from governing.com: https://www.governing.com/next/Legislative-Watch-The-Rise-of-Drones-During-the-Pandemic.html

Smith, R. E. (2017, May). Drones and the Fourth Amendment. *Privacy Journal*, 5-7.

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

Summers, N. (2020, May 26). *Drone deliveries are making their case in a crisis*. Retrieved June 2020, from engadget.com: https://www.engadget.com/drone-wing-zipline-matternet-everdrone-coronavirus-133021691.html

Taleb, N. N. (2007). *The Black Swan: The Impact of the Highly Improbable*. Random House.

Thompson II, R. M. (2013). *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses*. United States Congress. Washington D.c: Congressional Research Service.

Thompson II, R. M. (2014). *The Fourth Amendment Third-Party Doctrine*. United States Congress. Washington D.C.: Congressional Research Service.

Thompson II, R. M. (2015). *Domestic Drones and Privacy: A Primer*. United States Congress. Washington D.C.: Congressional Research Service.

Tuccille, J. (2020, April 10). *The Surveillance State Thrives During the Pandemic*. Retrieved July 2020, from reason.com: https://reason.com/2020/04/10/the-surveillance-state-thrives-during-the-pandemic/

U.S. Senate. (2016). *FAA Extension: Safety, Security, Stability*. Retrieved July 2020, from commerce.senate.gov: https://www.commerce.senate.gov/services/files/f0ed7c52-f6aa-4bb7-86a4-562a5e468253

United States v. Jones (U.S. 400 2012).

US Department of Defense. (2013, May). Air Sea Battle: Service Collaboration to Address Anti Access Area Denial Challenges. *DoD Periodical*.

Weise, E. (2015, September 10). *California governor vetoes drone bill*. (Gannett Satellite Information Network, LLC) Retrieved Aug 2020, from usatoday.com: https://www.usatoday.com/story/tech/2015/09/10/california-drones-veto-governor-jerry-brown-news-photographers/71987132/

Zoldi, D. M. (2020, July 10). *Crawl, Walk, Run, Fly! – Urban Traffic Milestones*. (L. Autonomous Media, Producer) Retrieved July 2020, from insideunmannedsystems.com: https://insideunmannedsystems.com/crawl-walk-run-fly-urban-traffic-milestones/

[1] After a search for this report, the authors were unable to confirm whether or not the Office of the Comptroller General of the United States National Telecommunication and Information Administration produced a report or ever requested an extension on its delivery. It would have been due to congress by late March of 2019.

[2] After a search for this study, the authors were unable to confirm whether or not the study was produced. The assumption is the FAA would deliver this study. It is unclear who or when this study would be expected to be delivered and to whom.

[3] An important omission from this summary is the exemption from this section for "the media".

Chapter 12: Chinese Unmanned Proliferation Along New Silk Road Sea/Land routes [Carter]

APPENDIX A

Information provided by World Bank via the Green Belt and Road Initiative Center (Dahlquist E., 2017)

(International Institute for Green Finance II Central University for Finance and Economics, 2020)

Country	Region	Income Group
“Afghanistan	South Asia	Low income
Albania	Europe & Central Asia	Upper middle income
Algeria	Middle East & North Africa	Upper middle income
Angola	Sub-Saharan Africa	Lower middle income
Antigua and Barbuda	Latin America & Caribbean	High income
Armenia	Europe & Central Asia	Upper middle income
Austria	Europe & Central Asia	High income
Azerbaijan	Europe & Central Asia	Upper middle income
Bahrain	Middle East & North Africa	High income
Bangladesh	South Asia	Lower middle income
Barbados	Latin America & Caribbean	High income
Belarus	Europe & Central Asia	Upper middle income
Benin	Sub-Saharan Africa	Low income
Bolivia	Latin America & Caribbean	Lower middle income
Bosnia and Herzegovina	Europe & Central Asia	Upper middle income
Brunei Darussalam	East Asia & Pacific	High income
Bulgaria	Europe & Central Asia	Upper middle income
Burundi	Sub-Saharan Africa	Low income
Cabo Verde	Sub-Saharan Africa	Lower middle income
Cambodia	East Asia & Pacific	Lower middle income
Cameroon	Sub-Saharan Africa	Lower middle income
Chad	Sub-Saharan Africa	Low income
Chile	Latin America & Caribbean	High income
China	East Asia & Pacific	Upper middle income
Cook Islands	East Asia & Pacific	

Comoros	Sub-Saharan Africa	Low income
Congo, Rep.	Sub-Saharan Africa	Lower middle income
Costa Rica	Latin America & Caribbean	Upper middle income
Côte d'Ivoire	Sub-Saharan Africa	Lower middle income
Croatia	Europe & Central Asia	High income
Cuba	Latin America & Caribbean	Upper middle income
Cyprus	Europe & Central Asia	High income
Czech Republic	Europe & Central Asia	High income
Djibouti	Middle East & North Africa	Lower middle income
Dominica	Latin America & Caribbean	Upper middle income
Ecuador	Latin America & Caribbean	Upper middle income
Egypt, Arab Rep.	Middle East & North Africa	Lower middle income
El Salvador	Latin America & Caribbean	Lower middle income
Equatorial Guinea	Sub-Saharan Africa	Upper middle income
Estonia	Europe & Central Asia	High income
Ethiopia	Sub-Saharan Africa	Low income
Fiji	East Asia & Pacific	Upper middle income
Gabon	Sub-Saharan Africa	Upper middle income
Gambia, The	Sub-Saharan Africa	Low income
Georgia	Europe & Central Asia	Lower middle income
Ghana	Sub-Saharan Africa	Lower middle income
Greece	Europe & Central Asia	High income
Grenada	Latin America & Caribbean	Upper middle income
Guinea	Sub-Saharan Africa	Low income
Guyana	Latin America & Caribbean	Upper middle income

Hungary	Europe & Central Asia	High income
Indonesia	East Asia & Pacific	Lower middle income
Iran, Islamic Rep.	Middle East & North Africa	Upper middle income
Iraq	Middle East & North Africa	Upper middle income
Italy	Europe & Central Asia	High income
Jamaica	Latin America & Caribbean	Upper middle income
Kazakhstan	Europe & Central Asia	Upper middle income
Kenya	Sub-Saharan Africa	Lower middle income
Kiribati	East Asia & Pacific	Lower middle income
Korea, Rep.	East Asia & Pacific	High income
Kuwait	Middle East & North Africa	High income
Kyrgyz Republic	Europe & Central Asia	Lower middle income
Lao PDR	East Asia & Pacific	Lower middle income
Latvia	Europe & Central Asia	High income
Lebanon	Middle East & North Africa	Upper middle income
Lesotho	Sub-Saharan Africa	Lower middle income
Liberia	Sub-Saharan Africa	Low income
Libya	Middle East & North Africa	Upper middle income
Lithuania	Europe & Central Asia	High income
Luxembourg	Europe & Central Asia	High income
Madagascar	Sub-Saharan Africa	Low income
Malaysia	East Asia & Pacific	Upper middle income
Maldives	South Asia	Upper middle income
Mali	Sub-Saharan Africa	Low income
Malta	Middle East & North Africa	High income
Mauritania	Sub-Saharan Africa	Lower middle income

Micronesia, Fed. Sts.	East Asia & Pacific	Lower middle income
Moldova	Europe & Central Asia	Lower middle income
Mongolia	East Asia & Pacific	Lower middle income
Montenegro	Europe & Central Asia	Upper middle income
Morocco	Middle East & North Africa	Lower middle income
Mozambique	Sub-Saharan Africa	Low income
Myanmar	East Asia & Pacific	Lower middle income
Namibia	Sub-Saharan Africa	Upper middle income
Nepal	South Asia	Low income
New Zealand	East Asia & Pacific	High income
Niger	Sub-Saharan Africa	Low income
Nigeria	Sub-Saharan Africa	Lower middle income
Niue	East Asia & Pacific	
North Macedonia	Europe & Central Asia	Upper middle income
Oman	Middle East & North Africa	High income
Pakistan	South Asia	Lower middle income
Panama	Latin America & Caribbean	High income
Papua New Guinea	East Asia & Pacific	Lower middle income
Peru	Latin America & Caribbean	Upper middle income
Philippines	East Asia & Pacific	Lower middle income
Poland	Europe & Central Asia	High income
Portugal	Europe & Central Asia	High income
Qatar	Middle East & North Africa	High income
Romania	Europe & Central Asia	Upper middle income
Russian Federation	Europe & Central Asia	Upper middle income
Rwanda	Sub-Saharan Africa	Low income
Samoa	East Asia & Pacific	Upper middle income

Saudi Arabia	Middle East & North Africa	High income
Senegal	Sub-Saharan Africa	Low income
Serbia	Europe & Central Asia	Upper middle income
Seychelles	Sub-Saharan Africa	High income
Sierra Leone	Sub-Saharan Africa	Low income
Singapore	East Asia & Pacific	High income
Slovak Republic	Europe & Central Asia	High income
Slovenia	Europe & Central Asia	High income
Solomon Islands	East Asia & Pacific	Lower middle income
Somalia	Sub-Saharan Africa	Low income
South Africa	Sub-Saharan Africa	Upper middle income
South Sudan	Sub-Saharan Africa	Low income
Sri Lanka	South Asia	Lower middle income
Sudan	Sub-Saharan Africa	Lower middle income
Suriname	Latin America & Caribbean	Upper middle income
Tajikistan	Europe & Central Asia	Low income
Tanzania	Sub-Saharan Africa	Low income
Thailand	East Asia & Pacific	Upper middle income
Timor-Leste	East Asia & Pacific	Lower middle income
Togo	Sub-Saharan Africa	Low income
Tonga	East Asia & Pacific	Upper middle income
Trinidad and Tobago	Latin America & Caribbean	High income
Tunisia	Middle East & North Africa	Lower middle income
Turkey	Europe & Central Asia	Upper middle income
Uganda	Sub-Saharan Africa	Low income
Ukraine	Europe & Central Asia	Lower middle income
United Arab Emirates	Middle East & North Africa	High income

Uruguay	Latin America & Caribbean	High income
Uzbekistan	Europe & Central Asia	Lower middle income
Vanuatu	East Asia & Pacific	Lower middle income
Venezuela, RB	Latin America & Caribbean	Upper middle income
Vietnam	East Asia & Pacific	Lower middle income
Yemen, Rep.	Middle East & North Africa	Low income
Zambia	Sub-Saharan Africa	Lower middle income
Zimbabwe	Sub-Saharan Africa	Low income" (Dahlquist E., 2017)

References [Chapter 12]

International Institute for Green Finance II Central University for Finance and Economics. (2020, March). *Countries of the Belt and Road Initiative (BRI)*. Retrieved from Green Belt and Road Initiative Center: https://green-bri.org/countries-of-the-belt-and-road-initiative-bri?cookie-state-change=1596286450104

Alden, C., Fiala, L., Krol, E., & Whittle, R. (2020, May 28). *Wings Along the BRI: Exporting Chinese UCAVs and Security*? Retrieved from Medium: https://medium.com/@lseideas/wings-along-the-bri-exporting-chinese-ucavs-and-security-a4bf7a3324df

Asia Maritime Transparency Initiative. (2020, June 16). *Exploring China's Unmanned Ocean Network*. Retrieved from Asia Maritime Transparency Initiative: https://amti.csis.org/exploring-chinas-unmanned-ocean-network/

Calabrese, J. (2020, May 19). *China's Maritime Silk Road and the Middle East: Tacking Against the Wind*. Retrieved from Middle East Institute: https://www.mei.edu/publications/chinas-maritime-silk-road-and-middle-east-tacking-against-wind

Chaziza, M. (2020, March 25). *Belt and Road Initiative, BRI,*

Business, China, Economic Growth, Economy, Middle East. Retrieved from The Asia Dialogue: https://theasiadialogue.com/2020/03/25/chinas-partnership-diplomacy-and-the-successful-implementation-of-the-bri/

Dahlquist E., H. S. (2017). System Perspective. . In H. S. Dahlquist E., *In: Dahlquist E., Hellstrand S. (eds) Natural Resources Available Today and in the Future*. Springer, Cham. Retrieved from https://doi.org/10.1007/978-3-319-54263-8_1

Electronics Science & Technology Committee of MIIT. (2019, July 27). *Electronics Science & Technology Committee of MIIT*. Retrieved from Ministry of Industry and Information Technology: http://www.miitestc.org.cn/uploadfile/2019/0727/20190727050055199.pdf

Greene, R., & Triolo, P. (2020, May 8). *Will China Control the Global Internet with the Digital Silk Road*. Retrieved from Carnegie Endowment for International Peace: https://carnegieendowment.org/2020/05/08/will-china-control-global-internet-via-its-digital-silk-road-pub-81857

Hamilton, C., & Ohlberg, M. (2020). *Hidden Hand Exposing How the Chinese Communist Party is Reshaping the World*. Richmond: Hardie Grant Books.

Harding, R. (2020, September 20). *China's Belt and Road Initiative and the Impact on the Middle East and North Africa* . Retrieved from International Banker: https://internationalbanker.com/finance/chinas-belt-and-road-initiative-and-its-impact-on-the-middle-east-and-north-africa/

Japan Center for Asian Historical Records. (2020, July 28). *Japan Center for Asian Historic Records*. Retrieved from National Archives of Japan: https://www.jacar.go.jp/english/nichiro/map.htm

Ministry of Industry and Information Technology. (2019, July 27). *Electronics Science & Technology Committee of MIIT*. Retrieved from Ministry of Industry and Information Technology: http://www.miitestc.org.cn/uploadfile/2019/0727/20190727050055199.pdf

Pan, C. (2020, March 27). *UK university study identifies Chinese*

drone maker XAG as best fit for disinfection operations to fight coronavirus spread. Retrieved from South China Morning Post : https://www.scmp.com/tech/gear/article/3077296/uk-university-study-identifies-chinese-drone-maker-xag-best-fit

Roblin, S. (2020, July 9). *Missile-Armed Chinese Drones Arrive In Europe As Serbia Seeks Airpower Edge*. Retrieved from Forbes: https://www.forbes.com/sites/sebastienroblin/2020/07/09/missile-armed-chinese-drones-arrive-in-europe-for-serbian-military/#4af9aff679d2

Shi-Kupfer, K., & Ohlberg, M. (2019). *China's Digital Rise : Challenges for Europe*. Berlin: Mercator Institute for China Studies.

Stevenson, B. (2019, November 17). *Dubai Airshow*. Retrieved from AIN Online: https://www.ainonline.com/aviation-news/defense/2019-11-17/uavs-continue-grow-strength-middle-east

Tybring-Gjedde, C. (2020). *China's Belt and Road Initiative: A Strategic and Economic Assessment*. Brussels: Nato Economics and Security Commitee.

Xuanzun, L. (2020, June 6). *PLA special mission aircraft approaches Taiwan after the island's missile test*. Retrieved from Global Times: https://www.globaltimes.cn/content/1191424.shtml