UNMANNED AIRCRAFT IN THE CYBER DOMAIN

PROTECTING USA'S ADVANCED AIR ASSETS

2ND EDITION

NICHOLS

RYAN

MUMM

LONSTEIN

CARTER

HOOD

UNMANNED AIRCRAFT SYSTEMS IN THE CYBER DOMAIN

PROTECTING USA'S ADVANCED AIR ASSETS

Second Edition

R.K. Nichols, J.J.C.H. Ryan, H.C. Mumm, W.D. Lonstein, C. Carter, and J.P. Hood

NEW prairie PRESS
open access scholarly publishing

Second Edition

A PDF version of this book is available at
https://newprairiepress.org/ebooks/27/

The webbook is available at
https://kstatelibraries.pressbooks.pub/unmannedaircraftsystems/

Cover design by Kira Miller
Cover image created by the Defense Advanced Research Projects Agency (DARPA)
and is available at https://www.darpa.mil/news-events/2016-03-31

New Prairie Press,
Kansas State University Libraries
Manhattan, Kansas

ISBN 978-1-944548-15-5

The first edition, published in 2018, was supported in part by Kansas State University Libraries' Center for the Advancement of Digital Scholarship under their Open/Alternative Textbook Initiative, grant approved by KSU Panel, January 2018.

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, 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 cybersecurity and Unmanned Aircraft Systems (UAS). It is not intended to turn counter terrorism, information technology, engineers or forensics investigator professionals or drone operator / pilots 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.

Dedications

From: Professor Randall K. Nichols, DTM

I dedicate this book to three groups: **All USA serving and retired military personnel**, USA Coast Guard and federal and state law enforcement for keeping our country safe; to my Angel wife of 35 years, Montine, and children Robin, Kent, Phillip (USA Army), Diana (USA 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.

Foreword To 1st Edition

by R. Kurt Barnhart, Ph.D., KSUP Associate Dean of Research

It gives me great pleasure to commend this work to you the reader after having spent a great deal of time with the manuscript in recent weeks. Although still in draft form at the time of my review, I can say with certainty that the breadth and quality of information you will find herein is unparalleled in the unclassified sphere. This book will fully immerse and engage the reader in the cyber-security considerations of this rapidly emerging technology we know as unmanned aircraft systems (UAS). Many of these same vulnerabilities affect unmanned technology across the board and regardless of mode, however the focus of this work is exclusively on those vehicles which operate in the National Airspace System (NAS).

Aircraft without on-board human pilots have been around in various forms longer than piloted aircraft. In 1783 Joseph-Michael and Jacques-Ètienne Montgolfier performed the first heavier-than-air vehicle flight in Annonay France. The passengers were a sheep, a pig, and a chicken (at least the chicken had a fighting chance if things went awry). It has, however, only been within the last couple of decades that this technology has burst onto the modern stage driven by the distinct technological advantages associated with eliminating the risks and limitations of protecting humans on-board. Advances in hardware and software have driven UAS capabilities far beyond what many imagined just a few short years ago. Today we stand at the precipice of a period in history where, looking forward, most vehicles in the air will not be occupied. As a result, given that we in the U.S. are constantly on the receiving end of withering cyber-attacks, a detailed treatment of this subject matter is of national importance as we protect and secure our national interests.

When noted cyber-security pioneer and lead author professor Nichols and I began to engage in a dialogue on this topic several years ago, it was clear that there were large and looming gaps in unmanned systems that had already been exploited on the international stage from a cyber-perspective. Many of those gaps remain unaddressed today. Understandably, commercial technology developers remain keenly focused on gaining a competitive advantage and delivering products to market albeit often without thorough cyber risk assessments and mitigations. This book will give system designers, users, and their management teams an introduction to what it will take to begin to close many of the vulnerabilities associated with UAS in order to produce systems that will serve the market better by being much more reliable, capable, and secure than they would be otherwise. This book takes advantage of the extensive knowledge of multiple working experts in the realm of cyber-security and they have each done an excellent job at uncovering and detailing the core issues at hand as we continue the march toward full NAS

integration of UAS in the not-to-distant future. Let's take a brief look at what the reader will find herein.

In Section one, "The UAS Playing Field" the reader will gain an understanding of the history and scope of UAS as a technology and will come to have a greater understanding of the UAS market and of the policies which both enable, and inhibit the deployment of the technology into the NAS. In chapter three, the final in section one, some of the key vulnerabilities associated with UAS are introduced and discussed.

In section two, "UAS Information Security, Intelligence, and Risk Assessment", the reader will gain a more detailed exposure to the vulnerabilities of the information necessary for UAS to operate and thereby will appreciate the differences between explicit, implicit, and derived security requirements. Chapter four concludes with a paragraph which says that "Communications may need to have confidentiality, integrity, and availability protected". How that is integrated into UAS design is of high importance. Chapter five examines types of, and sources of, intelligence data and discusses common attack/defense scenarios for UAS. Finally, section two concludes with case studies that highlight the vulnerabilities of UAS in the cyber-domain.

Section three is all about collision avoidance systems which are indeed the "heart and soul" of a fully integrated and useful system of unmanned aircraft. Sense and avoid (SAA) systems are discussed in depth along with one significant antagonist of SAA systems which is "stealth design". Finally this section concludes with a detailed discussion of a related system which is the 'smart skies' collaborative commercial project of which SAA is a critical component.

Section four primarily relates to the defense applications of Intelligence, Surveillance, and Reconnaissance (ISR), weapon systems security, and electronic warfare considerations and other information-centric operations. This section should not be dismissed by those without a focus on military applications as often it is the military that simply encounters technological vulnerabilities first given the dynamic operational environment they are associated with.

Section five looks at the data vulnerabilities of the various system components and explores the relationships and associated vulnerabilities of intra-system communication pathways. Chapter 14 delves into the realm of electronic warfare from a detailed perspective including a discussion of the intelligence information cycle as well as "jamming" operational vulnerabilities. This section concludes with discussion of current international threats and considerations related to still-emerging political scenarios where UAS technology is front and center.

As I conclude this overview of the work you are about to delve into I would encourage you to read this work along with a ready-copy of today's most current headlines. In doing so you will discover that the topics covered in this book are not only of interest today, but of critical importance to the future of us all.

Dona nobis pacem,

R. Kurt Barnhart, Ph.D.
Associate Dean of Research
Kansas State University Polytechnic

Salina, KS

Foreword To 2nd Edition

by Alysia Starkey, Ph.D., KSUP CEO & Dean

I am delighted to write the forward for the second edition *of Unmanned Aircraft Systems in the Cyber Domain: Protecting the USA's Advanced Air Assets.* The first edition was published in 2018 and quickly established itself as a must-have text for academic programs and individuals looking to expand their knowledge in this emerging cyber discipline. Thanks to that text, conversations at conferences and other professional networking events this year were easy and spirited. As soon as *Kansas State University* was spotted on my name tag, individuals asked if I knew of the book and were eager to share their experiences.

The fact that the second edition follows so quickly after the first is indicative of the rapid pace in which the manned and unmanned airspaces continue to converge and the need to fully understand the direct impact on the civilian market. During the past year, I watched and listened as the authors electronically discussed and passionately debated the topics of national interest presented in this text. Their collective intellect coupled with the depth of their professional experience challenged my assumptions and continued to do so as I read the completed second edition.

As an educator, I appreciate that the second edition is structured in the same way as the first. Each chapter starts with the student learning objectives found therein, include value-added graphics, and concludes with scenarios and discussion questions for in-class use. This brings increased efficiency when creating a course syllabus or developing content-related assessments. The second edition further expands on the topics presented in the first edition. Prior knowledge of manned and unmanned aviation regulations, military/civilian/commercial unmanned applications, and basic cybersecurity concepts is beneficial for the reader to fully engage with the material.

It is my expectation that this text will provide an effective learning experience and become a referenced resource for students and professionals working to secure the national airspace and reduce known and unknown threats with this developing technology.

Alysia Starkey, Ph.D.
Interim CEO and Dean
College of Technology and Aviation
Kansas State University Polytechnic
Salina, KS

Preface To 1st Edition

HISTORICAL PERSPECTIVE

Unmanned Aircraft Systems (UAS) In the Cyber Domain: Protecting USA's Advanced Air Assets is the working product of five talented authors to meet the needs of students enrolled in Kansas State University Polytechnic's (KSUP) graduate Certificate in UAS – Cybersecurity. The book also serves as one of the technical resources for the KSUP Professional Masters in Technology (PMT) offering in their UAS – Cybersecurity discipline.

Interest in UAS-Cybersecurity Certificate / PMT specialty programs developed from two directions; one internal and external to the college. Internally it dates to 2014, when the KSUP Associate Dean for Research and Executive Director of the UAS Research Laboratory, Dr Kurt C. Barnhart, met with Professor Nichols to discuss the possibility of state-of-the-art Cybersecurity Masters and / or Certificate program. These would meet the need for outside online programs to enhance the University profit structure. Associate Dean Barnhart in 2014 approved the concept of a Graduate Certificate in UAS – Cybersecurity and gave permission to move forward with its development. The program was placed under the purview of the College of Technology and Aviation. Final program approval was given by the KSU Board of Trustees in January, 2017. The five courses in the Graduate Certificate UAS – Cybersecurity program were also approved for the Professional Masters of Technology (PMT) in 2017.

In 2014, Professor Nichols had discussions with students and professionals in multiple schools and states inquiring about the prospect of an Unmanned Aircraft Systems – Cybersecurity Masters curriculum or graduate certificate program at KSUP, especially the on-line component. Their perception was that there was a market of not only freshmen / transfers / graduate students who might be interested in such a program, but a larger market of working professionals in need of skill advancement, and of a forum for the discussion of developments in the industry. They also felt that the college could anticipate financial assistance from federal, state, aviation, corporate, law enforcement, and defense organizations to get such a program launched. There was considerable enthusiasm and a general feeling that a cybersecurity concentration to defend UAS assets and their Command, Control, Communications, Computers, Intelligence, Reconnaissance and Surveillance (C4IRS) systems from cyber-attacks would serve the interests of the college and its students, as well as those of the security / defense industries.

The outside interests from the intelligence and aviation communities became acute after the 2011 RQ-170 incident where Iran was credited with its capture. In addition, in 2014, Iran claimed the downing of an Israeli Hermes 450 Drone over Natanz. Reports like these caused major gov-

ernment concerns. Better risk assessment and teaching active cyber defenses is required to protect UAS assets. Hence, the graduate Certificate program in UAS – Cybersecurity was born.

The new MPT / Certificate discipline in UAS – Cybersecurity is NOT about drone training like that of Embry-Riddle Aeronautical University. **Its mission is CYBERSECURITY protection of UAS / UAV / Drones as Information Assets in the Air, all the networked computer systems related to the Intelligence / Counter Intelligence functions, and their payloads.**

MISSION

A key concern is the safety of integration of UAS systems into the National Air Space (NAS). **A critical component of this safety is the hardening of UAS/ sUAS /UAVs to cyber-attacks.**

The focus of this new program is on leadership, planning, and state-of-the-art practice for professionals in UAS / UAV aviation concerned with protecting this advanced technology against cyber-attacks or hostile/ intentional control of Command, Control, Communications, Computers, Intelligence, Reconnaissance and Surveillance (C4IRS) systems, or Loss of Signal (LOS) to critical navigational components. This program applies to all UAS / UAV personnel preparing to act or working as pilots, operators, communications, payload, navigation, ground support, satellite coordination with assets, or air-to-air delivery.

The Graduate Certificate Program in Unmanned Aircraft Systems – Cybersecurity requires five three-hour credit courses for certification. Each course is required to reflect current knowledge and practice in terms of cybersecurity, Information Security (INFOSEC), Communications Security (COMSEC), and Risk Assessment (RA) as applied to both safe integration of UASs into the National Airspace (NAS) and deployment for global Counter Terrorism operations (CT).

All courses in the proposed certificate focus on knowledge and skills to understand UAS / UAV issues related to UAS cyber security. If students desire to complete a Professional Masters in Technology (PMT), four courses from this certificate can be applied as electives towards the professional Master's Degree in College of Technology and Aviation.

The certificate program has one concentration – cybersecurity. CyberSecurity (in the context of cyber-conflicts) is defined in this document as, "the broad *tree* of investigation and practice devoted to cybercrimes, computer forensics, Information Assurance, Information Security (INFOSEC), Communications Security (COMSEC), and especially Cyber Counter Intelligence (CCI)" (Nichols, 2008). Cyber Counter Intelligence indicates the involvement of computer-based sensitive information, or information operations for three distinct sciences operating in the cyber realm: Cyber Counter Sabotage (CCS), Cyber Counter Terrorism (CCT), and Cyber Counter Espionage (CCE). (Nichols, 2008) In this book, Cybersecurity is limited to the prior three investigation areas. Computer *forensics* is the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless

communications, and storage devices in a way that is admissible as evidence in a court of law (US-CERT, 2015)

The primary concerns of the graduate certificate program are protection of UASs / Small UAS (sUAS) / Unmanned Aircraft Vehicles (UAVs) from cyber-attacks, through negligent or hostile means, and teaching cyber security risk assessment principles to practitioners involved with UAS operations on land, sea, air, or satellite platforms. The impact of Loss of Signal (LOS) or intentional interference in UAS communications or navigation systems cannot be overstated. At the lowest end of the scale is the risk of a downed vehicle, mid-range risk is collision and failure to sense and avoid other vehicles or commercial / military traffic, and at the top of the risk scale is the hostile takeover of a payload to be used against US or US interests. It is not "good enough" to operate, fly or support UASs. Professionals must be concerned with protection of their charges.

Unmanned Aircraft Systems (UAS) In the Cyber Domain: Protecting USA's Advanced Air Assets is the authors attempt to provide some of the raw materials / tools for our students at a reasonable cost. (Free download like the MIT Open courseware project under a CCL open license arrangement.)

UAS – CYBERSECURITY CERTIFICATE PROGRAM COURSES

COT 680. Unmanned Aircraft Systems and Risk Assessment. (3) Fall. This course is an introductory course in Unmanned Aircraft Systems (UAS) history, elements, US aviation regulations, operations, use of geospatial data, automation and safety issues; detect and avoid systems, sensors and payloads, and human factors. Special attention to UAS Cyber Security Risks, Threats, Impact, Vulnerabilities, and Countermeasures will be identified. Various risk assessment equations will be used for qualitative risk analysis of threats so identified.

COT 682. Open Source Cyber Surveillance / Intelligence. (3) Fall. One of the key public concerns for safe integration of UAS into the NAS is privacy. This course questions the technical gaps, Intelligence Community (IC) assumptions, and important legal issues related to open source cyber surveillance / intelligence with emphasis on UAS activities/ deployment. Topics addressed include the responsible, legal, and ethical use of data and information gathered from the use of unmanned, semiautonomous systems, web data mining, social networks, and other modern technological systems.

COT 684. Advanced Topics in Cyber Data Fusion and Cyber Counter Intelligence. Prerequisites: three of four courses in the sequence. (3) Spring. This course is scenario-based applying cyber surveillance techniques and analysis of collected data to realistic, terrain-oriented problems. Topics include the digital soldier and sailor, 360-degree battlefield awareness and the use of unmanned, semiautonomous technologies. Risk assessment and cyber security countermeasures are the "glue" to successful implementation of data fusion techniques. Various risk

assessment equations and other methods will be used for qualitative risk analysis of identified cyber threats. Cyber Counter Intelligence technology is applied to cases.

COT 686. Risk Management for UAS Operators, Pilots, and Ground Personnel. (3) Spring. UAS operators, pilots, and ground personnel must be committed to safety if the goal of UAS integration into NAS is to be accomplished. The best tool for assessment and determination of safest possible flight is risk management. This course introduces three risk assessment tools for UAS operators, pilots, and ground personnel to manage the workloads associated with each phase of flight.

COT 688. Sense and Avoid Technologies in UAS. (3) Summer / fall. This course is an advanced course in Sense and Avoid (SAA) technologies for UAS. SAA is extremely important concept and is the main obstacle for wider application of UAS in non-segregated airspace related to traffic safety in civilian and military/ defense domains.

TARGET AUDIENCE

Clearly, the students in the UAS -Cybersecurity Certificate and MPT programs, along with KSU's Aviation and Technology Department and UAS Research Laboratory, are the targets for this book. Cyber attacks and hostile control of UAS should not be underestimated.. It is as real as cyber attacks on computers, networks, personal identities, intellectual property loss, and delivery of cyber weapons on the battlefield. The larger audience are UAS operators, pilots, and ground personnel, owners and computer network analysts to manage the workloads associated with each phase of flight in any service: military, commercial, or recreational. Those concerned with UAS communications, navigation, payload, battery, sense and avoid, emergency components, satellite links, ground station links, materials construction and risk assessment / management associated with novel designs may well benefit from our textbook. All are factors in the vulnerable cyber domain.

STRUCTURE OF THE BOOK

Several themes covered in this text:

- C4ISR, Payload recovery, communications interference in the many different platforms,
- SAA and navigational functions and their interactions in the NAS (i.e. vulnerabilities)
- Protecting UASs from hostile intent in the Cyber Domain, and
- SCADA systems and how they may be exploited and protected in UAS vehicles.

Unmanned Aircraft Systems (UAS) In the Cyber Domain: Protecting USA's Advanced Air Assets is divided into five sections:

Section 1: The UAS Playing Field

Unmanned Aircraft Systems (UAS) – Defining UAS Cyber Playground

Chapter 1 A view of the UAS Market

Chapter 2 UAS Law – Legislation, Regulation and Adjudication

Chapter 3 Understanding Hostile Use and Cyber-Vulnerabilities of UAS: Components, Autonomy vs. Automation, Performance Trade-offs, SCADA and Cyber Attack Taxonomy

Section 1 above is concerned with the basic components and taxonomy of UAS that are vulnerable to cyber influence.

Section 2: UAS Information Security, Intelligence and Risk Assessment

Information Security (INFOSEC), Intelligence and Risk Assessments

Chapter 4 INFOSEC – Protecting UAS Information Channels & Components

Chapter 5 Intelligence and Red Teaming

Chapter 6 Case Studies in Risk for UAS

Section 2 above introduces the concepts and tools of Risk Assessment, Open Cyber Intelligence / Reconnaissance, network security, INFOSEC and vulnerability analysis. The use of Attack / Defense scenarios is introduced.

Section 3: UAS Heart & Soul – Sense and Avoid (SAA) Systems / Stealth

Sense and Avoid (SAA) – Heart of the UAS Package & Stealthy Design, its Soul

Chapter 7 SAA Sensors, Conflict Detection, and Resolution Principles

Chapter 8 Designing UAS systems for Stealth

Chapter 9 Smart Skies Project

Section 3 above focusses on the Sense and Avoid systems and common approaches to reduction of risk for failure of those systems. It also studies the brilliant Smart Skies project with speculations as to how the systems could be breached.

Section 4: UAS Weapons & ISR &IO

Payloads – UAS Delivery Systems

Chapter 10 UAS Intelligence / Reconnaissance / Surveillance Technologies (ISR)

Chapter 11 UAS Weapons

Chapter 12 UAS System Deployment and Information Dominance (ID)

Section 4 above concentrates on the unclassified UAS weapons systems, EW and IO systems, Information Dominance (ID) and surveillance technologies – all that can potentially be breached via cyber means.

Section 5: Computer Applications & Data Links – Exposing UAS Vulnerabilities via Electronic Warfare (EW) & Countering with Low Probability Intercept Signals (LPI)

UAS Vulnerabilities and Electronic Warfare (EW)

Chapter 13 Data – Links Functions, Attributes, & Latency

Chapter 14: Exposing UAS Vulnerabilities via Electronic Warfare (EW) & Countering with Low – Probability Intercept Signals (LPI)

Section 5 above is concerned with the attributes, functions, latency features of UAS communications links on ground, air, sea, and satellite.

Section 6: UAS / UAV Hostile Use & Countermeasures

Adversary UAS / Drone Hostile Use

Chapter 15: Africa – World's First *Busiest* Drone Operational Proving Ground – Where Counter-Terrorism and Modernization Meet

Chapter 16: Chinese Drones in Spratly Islands, and Threats to USA forces in Pacific

Section 6 above steps into the headlines of today. Part of the material comes from Professor Nichols' presentations to the public about hostile use of drones.

As our book goes to press, more potent examples of UAS Cyber intrusion (globally) may arise and will be included as time permits. In the meantime, the authors suggest that interested readers follow www.globalincidentmap.com or www.aviation.globalincidentmap.com both track the current global terror and non-terror incidents involving planes, and UAS.

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

Linkedin Profile:
http://linkedin.com/in/randall-nichols-dtm-2222a691

Illi nunquam cedunt.
“We Never Yield”

Bibliography

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

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

Preface to 2nd Edition

Summary

It has been less than a year since the first edition of *Unmanned Aircraft Systems in the Cyber Domain: Protecting USA's Advanced Air Assets* was published. Three different factors have spurred the authors into updating their textbook. First, unmanned aircraft technology has seen an economic explosion in production, sales, testing, specialized designs and friendly / hostile usages of deployed UAS / UAVs / Drones. There is a huge global growing market and entrepreneurs know it. Small UAS companies have been reproducing like rabbits. Only the FAA has been stumbling block trying to balance UAS safe integration into the National Airspace against hundreds of thousands new recreational and commercial operators testing their meddle in the skies. FAA's best efforts surround its decision to register UAS and provide a process for Part 107 Certification. Certification brings sanity and education into a chaotic public market in the US.

Second, hostile use of UAS is on the forefront of DoD defense and offensive planners. They are especially concerned with SWARM behavior. The author presented at several international C-UAS conferences which were attended by commercial, educational and military organizations for the purpose of hardening USA air assets against hostile drone activities. These were serious conversations and workshops – many of them behind closed doors and interacting with military brass.

Third, UAS technology was outpacing our first edition. Everyday our group read / discussed new UAS developments in navigation, weapons, surveillance, data transfer, fuel cells, stealth, weight distribution, tactics, GPS / GNSS elements, SCADA protections, privacy invasions, terrorist uses, specialized software and security protocols and more. As authors we felt compelled to address at least the edge of some of the new UAS developments. It was clear that we would be lucky if we could cover some of the more interesting and priority technology updates. The 2nd Edition adds six more chapters (see below) to harvest information on important advances in the UAS theater. We were privileged to bring on Captain John P Hood (US Army) as our military advisor and co-author.

Here is an outline of topics in the new chapters in our 2nd Edition:

Section 7: Technology Updates

Chapter 17: High – Altitude Platforms (HAPS) – A Promise not Reached

Student Learning Objectives
Introduction

Missions
Telecommunications
Earth Observation
GNSS
UAV-Aided Wireless Communications
UAV-aided ubiquitous coverage
UAV – aided relaying
UAV – aided information dissemination and data collection
Challenges
Simple HAPS UAV Network Architecture
Control and Non-Payload Communications Link (CNPC)
CNPC links operate in protected spectrum
Backhaul Links
Data Links
Channel Characteristics, Propagation and Channel Modelling
UAV-Ground Channel
HAPS UAV – UAV Channel
From the Designers Shoes
Stratosphere Segment
Platforms
Aerodynamic Platforms (UAVs)
Platform Choice – Key Designer Issues
Telecommunications Payload
Telemetry, Tracking and Command (TT & C)
Table 17-5 Functions of TT & C Subsystem
Avionics
Electrical Power Subsystem
Ground Segment
Spectrum Allocation for HAPS
HAPS Link Budget
One-Way Link Budget Analysis
Uplink equation
Downlink equation
Discussion Questions
Bibliography

Chapter 18: C-UAS and Large-scale Threats

Student Learning Objectives
Countering Emerging Unmanned Air System Threats
Introduction

Compromising the Sound Source
Drone on Drone Attack
GPS Denied Navigation
MEMS
Resonance Effects on MEMS
What is Resonance Tuning?
What is the "so what" for Acoustics? Here are the author's thoughts:
Are there Countermeasures for Acoustic attack on Gyroscope?
South Korean experiment
NOISE
UAS Collaboration – SWARM
Discussion Questions
Bibliography
Readings

Chapter 20: Legal and Regulatory – Where it Was, where it is and what's Ahead?

Student Learning Objective
Introduction
Current Regulatory Overview
Future Regulatory Framework
Conflict of Laws
Putting It Together – Where Law Meets Reality
Scenario 1 Interference with Fire Fighting
Scenario 2 Military, Legal, Public Safety
Decisions and Dilemmas for Student Consideration
Conclusions
Bibliography

Chapter 21: Chinese UAS Proliferation along New Silk Road Sea/ Land routes

Student Learning Objectives
Chinese Government Building the "The Belt & Road"
The Belt
Central Role in Road: Kazakhstan
The Belt Achievements to Date
Maritime Silk Road (MSR)
Chinese Military Build Up to Support the New Silk Road
Digital Silk Road
Drones are a critical part of China's New Silk Road
In Plain Sight: China Drones Manufacturers
US involvement in the New Silk Road

Digital Belt and Road
Conclusions
Discussion Questions
Bibliography
Secondary Web Sources

Chapter 22: Ethics in the New Age of Autonomous Systems and Artificial Intelligence (AI)

Student Learning Objective
History
Can ethics and morals be logically extended to AI and autonomous systems?
Balance V. Bias in AI and autonomous fields
If an AI system becomes self-aware, does it deserve human rights? Citizenship?
Lethal and none-lethal decisions; do we allow Skynet to be built?
Can we build autonomous systems that will obey the "rules of the road?
Ethics in new technology manufacturing
Conclusions
Discussion Questions
Bibliography

Chapter 17 looks at the promise of UAS High Altitude Platforms (HAPS). It follows a similar investment path as that of UAM (Urban Air Mobility) systems for transportation. Lots of money, lots of new technology, lots of players, and failure to complete the mission.

Chapter 18 is an interesting look at Counter Unmanned Aircraft Systems (C-UAS), large scale UAS, and restrictions that the DoD and government has to suffer to extinguish UAS threats.

Chapter 19 presents the research formulations / Intellectual Property of Professor Nichols which were presented at two 2018 conferences.[1] It discusses the technology behind use of loud ultrasonic sound at specific frequencies to disrupt the MEMS components driving the rotors of a Hostile UAS, forcing the aircraft into a destructive path. It works best with SWARMS because the number and organization can be matched by the LRAD weapons. Chapter 19 also presents the novel idea that the same frequencies that can be used to down a UAS can also be used to identify friend or foe (IFF) by creating a searchable library of sound frequency signa-

1. Prof Nichols was the Invited Keynote Speaker and Panel Moderator, (29-30 March 2019) 1st UAS CON for Law Enforcement and First Responders, speaking on Drone Wars: Threats, Vulnerabilities and Hostile Use of Unmanned Aircraft Systems (UAS) and Small UAS (sUAS), and Acoustic Defensive Countermeasures against SWARMS, Hazard Community & Technical College, Hazard, KY.He also was an Invited Speaker and Panelist (13-14 March 2019) 7th Annual DoD Summit, speaking on: Hardening USA Unmanned Systems Against Enemy Countermeasures, Alexandria, VA.

tures. Currently IFF units are too expensive and require too many SCADA and power communications to be included in SUAS / mid-level UAS. Prof. Nichols and his team are seeking grant / funding for testing at a national anechoic chamber.

Chapter 20 addresses the legal and regulatory conditions in the US that UAS operators / owners and defense planners face. Globally, restrictions are much lighter than in the US. It is a mess that FAA and others need to solve for the industry to grow in a challenging multi-issue environment.

Chapter 21 brilliantly addresses the Chinese Land / Sea New Silk Road Strategy and how UASs are being deployed for ISR operations and people control as well as interference with other nations assets. It presents a disturbing picture and one that should be taken to heart. The reader should also engage in self – learning by reading two seminal texts on the subject: 1) Brenner, J. (2011) *America the Vulnerable: Inside the Threat Matrix of Digital Espionage, Crime and Warfare.* New York: Penguin Books; and 2) Corr, A., Editor. (2018) *Great Powers, Grand Strategies: The New Game in the South China Sea.* Annapolis: The Naval Institute Press.

Chapter 22 presents a subject rarely discussed in public or regulatory offices – ethics. It looks at UAS and AI interfaces and how they present a real problem for society and act as a market barrier for an expanding UAS market. Several tough ethical cases are presented for evaluation.

We trust our 2nd edition will enrich our students and readers understanding of the purview of this wonderful technology we call UAS.

Best

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

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

Acknowledgments

Books such as this are the products of contributions by many people, not just the musings of the authors. *Unmanned Aircraft Systems in the Cyber Domain: Protecting USA's Advanced Air Assets*, 2nd Edition, 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. 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 several people we would like to shout out a special thank you for your guidance, 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, Acting Dean & CEO of KSUP; Dr. Terri Gaeddert, Director of Academics, School of Integrated Studies (SIS) KSUP; Dr. Donald V. Bergen, prior Director of Graduate Studies KSUP; Fred Guzek, Professor and current Director of Graduate Studies KSUP; Dr. Kurt Caraway, Executive Director UAS, Dr. Michael Most. (Retired) UAS Department Chair, Dr. Mark J. Jackson, Professor, SIS KSUP; Dr. Saeed Khan, Professor, SIS KSUP; Professor Raju Dandu; Dr. Katherine Jones, KSUP Research and Library; Rachel Miles, Assistant Professor, Hale Library KSU; Lisa Shappee, Director, KSUP Library; Beth Drescher, Grant Specialist KSUP; Charlene Simser, Professor and Coordinator of Electronic Publishing at New Prairie Press, Chad Bailey, Instructor SIS KSUP, Professor Troy Harding; and especially Joel Anderson, KSU OVPR and Research Director.

Next comes our writing team: Dr Julie J. C. H. Ryan, CEO, Wyndrose Technical Group, is hands down the best subject matter expert (SME) in the Information security field. Dr. Hans C. Mumm is an expert in leadership and UAS weapons – a lethal combination. Dr. Wayne C. Lonstein, Esq., a previous Dragon (Nichols 'student) has gained recognition (licenses and certifications) in both law and cybersecurity. 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 advisor and previous Dragon) stepped up for a chapter in the 2nd edition. Professor Nichols is author / developer of six Masters and Certificate programs in Cybersecurity at Utica College and KSUP with five decades of experience.

Our textbook has been developed to replace two expensive textbooks in four of his graduate classes in the KSU graduate UAS Cybersecurity Certificate program and the KSU Professional Masters in Technology specialty. We would have failed our mission without our editor Aris

Theocharis. Many times, we growled under our breath for the changes required knowing always, Aris was right.

Finally, E. Montine Nichols deserves a commendation for her help on the final drafts and copy edit work for our book. Several KSUP UAS pilot – students helped with the "student view," and made valid suggestions for improvement, Randall Mai, Jeremy Shay, Vincent Salerno, Senior Airman in Kansas Air National Guard, John Boesen, (our handwriting expert); Diana K. Nichols, Josh Jacobs and Jordan McDonald. Special thanks go out to Devon S. Carter for website ideas and Kira C. Miller who professionally developed (more like "nailed") our cover art.

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

List Of Contributors

Professor Randall K. Nichols, DTM (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 seven best-selling textbooks. Nichols has provided counsel to the United States government and is certified as a federal subject matter expert (SME) in both cryptography and computer forensics. His most recent work involves creating master and certificate graduate – level programs for KSU and Utica College. To wit:

- Author/ Developer: MPT/ MS / Certificate in Unmanned Aerial Systems (UAS) -Cybersecurity
- Author/ Developer: BS Unmanned Aerial Systems (UAS) -Cybersecurity
- Retired Chair and Program Developer: MS – Cybersecurity –Intelligence and Forensics
- Retired Chair and Program Director: BS – Cybersecurity and Information Assurance
- Co-Author / Developer: MPS – Risk Assessment and Cybersecurity Policy
- Author / Developer: MS Cyber Surveillance and Warfare

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

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

Nichols served as Technology Director of Cryptography and Biometrics for the International

Computer Security Association (ICSA), President, and Vice President of the American Cryptogram Association (ACA).

Areas of Expertise / Research Interests

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

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

*Direct all inquiries about this book to Prof. Randall K. Nichols, DTM 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.Hans-Mumm.com

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

Wayne Lonstein holds a Bachelor of Arts Degree in Political Science from Wilkes University, a Bachelor of Science Degree in Cyber Forensics and Information Security from Syracuse University – Utica Collage, A Master of Science Degree in Homeland Security with a concentration in Information Security from The Pennsylvania State University and a Juris Doctor Degree from Pace University School of Law. Additionally he holds a CISSP Certification from The Pennsylvania State University. He is a member of the state bars of New York, New Jersey, Massachusetts an Pennsylvania as well as being admitted to over 30 United States District Court Bars, The

Court of Veterans Appeals, United States Tax Court and the bar of the United States Court of Appeals of the 2nd, 3rd and 5th Circuits.

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

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

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

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

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

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

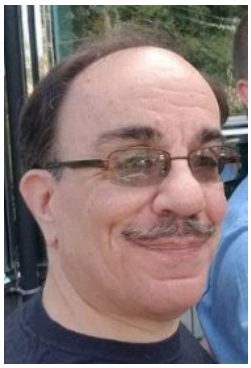
She is the author /co-author of several books, including *Defending Your Digital Assets Against*

Hackers, *Crackers*, *Spies*, *and Thieves* (McGraw Hill 2000), and a Fellow of the American Academy of Forensic Sciences (AAFS). At Wyndrose Technical Group, she focuses on futures forecasting and strategic planning with an eye on technology surprise and disruption.

Candice Carter (Co-Author)

Ms. Candice Carter is a cybersecurity expert with over 15 years of hands-on experience in the areas of 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 (expected 2019) from Kansas State University.

Aris Theocharis (Co-Editor)



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

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

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

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

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

Dr. Barnhart's Research agenda is focused in aviation psychology and Human Factors as well as the integration of Unmanned Aircraft Systems into the National Airspace System. His industry experience includes work as a R&D inspector with Rolls Royce Engine Company where he worked on the RQ-4 Unmanned Reconnaissance Aircraft development program, as well as serving as an aircraft systems instructor for American Trans-Air airlines. Formerly, Dr. Barnhart was an Associate Professor and Acting Department Chair of the Aerospace Technology at Indiana State University where he was responsible for teaching flight and upper division administrative classes. Courses taught include Aviation Risk Analysis, Citation II Ground School, King Air 200 Flight, Air Navigation, Air Transportation, Instrument Ground School and many others.

CPT John-Paul Hood USA (Co-Author)

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

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

Dr. Starkey is a Professor and currently serves as the Interim 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.

Abbreviations: Acronyms

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

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
A/C	Aircraft
ACAS	Airborne collision avoidance system / Assistant Chief of the Air Staff
ACL	Agent communication language / Autonomous control levels
ACS	Airborne control station (system)
ACTD	Advanced Concept Technology Demonstration
AD	Ansar Dine terrorist group
A/D	Attack / Defense Scenario Analysis
ADAC	Automated Dynamic Airspace Controller
ADC	Air data computer
ADF	Automatic direction finder/finding
ADS	Air Defense System (USA)
ADS-B	Automatic Dependent Surveillance – Broadcast systems
ADT	Air Data Terminal

AEW	Airborne early warning
AF	Adaptive Filtering
AFCS	Automatic flight control system
AFRICOM	US Africa Command
AGM	Air- to- surface missile
AGARD	Advisory Group for Aerospace Research and Development (NATO)
AGM-65	Maverick (USA) is an air-to-surface missile (AGM) designed for close air support. It is the most widely produced precision-guided missile in the Western world, and is effective against a wide range of tactical targets, including armor, air defenses, ships, ground transportation and fuel storage facilities
AHA	Autopilot Hardware Attack
AHRS	Attitude and heading reference system
AI	Artificial intelligence
AIAA	American Institute of Aeronautics and Aerospace
AIC	Aeronautical Information Circular
AIP	Aeronautical Information Publication
AIS	Automated Identification System for Collision Avoidance
AJ	Anti-Jam
AM	Amplitude Modulation / al-Mourabitoun terrorist group
ANSP	Air Navigation Service Provider
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, m^2
AR	Aspect ratio
AR drone	AR stands for “Augmented Reality” in AR *drone*. AR *Drone* can perform tasks like object recognition and following, gesture following
ARM	Anti-Radiation Munitions
ARS	Airborne Remote Sensing
ARW	Anti-radiation weapons
AS	Airborne Sensing Systems
ASB	Advisory Service Bulletin
ASEA	Active electronically scanned arrays
ASEAN	Association of Southeastern Asian Nations
ASL	Airborne Systems Laboratory
ASMS	Automated Separation Management System
ASTM	American Society of Testing and Materials
ASTER	Agency for Science, Technology and Research
ASW	Anti-submarine warfare
AT	Aerial target
ATC	Air Traffic Control
ATM	Air Traffic Management
ATR	Automatic Target Recognition
ATS	Air Traffic Service
AUDS	Anti-UAV Defense System
AUV	Autonomous Underwater Vehicle
AUVSI	Association for Unmanned Vehicle Systems International
AV	Air Vehicle
AWSAS	All Weather Sense and Avoid System
B	IF equivalent bandwidth, Hz
BAMS	Broad Area maritime surveillance

Backhauling	Intermediate links between core network or internet backbone and small subnets at the edge of the network
Bandwidth	Defined as the Range within a band of wavelengths, frequencies or energy.Think of it as a range of radio frequencies occupied by a modulated carrier wave, assigned to a service over which a device can operate. Bandwidth is also a capacity for data transfer of electrical communications system.
BDA	Battle Damage assessment
BER	Bit error rate
BLOS	Beyond line-of-sight
BNF	Bind and Fly – with custom transmitter
BRI	Belt and Road Initiative (Chinese)
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 [Conflict Resolution]
C2 / C2W	Command and control / Command and Control Warfare
C3I	Command, control, communications and Intelligence
C4	Command, control, communications and computers
C4ISTAR	Command, control, communications, computers, intelligence, surveillance, target Acquisition and reconnaissance
CA	Collision Avoidance / Clear Acquisition (GPS) / *Cyber Assault (aka CyA)*
CAA	Control Acquisition cyber attack
CAS	Close Air Support / Common situational awareness
CASA	Civil Aviation Safety Authority

C of A	Certificate of Airworthiness
CAP	Civil Air Publication / Combat Air Patrol
CAT	Collision Avoidance Threshold
CC / CyC	Cyber Crime
CCCI/II	*Classical Cryptography Course Volume I/II* (Nichols R. K., *Classical Cryptography Course Volume I / II*, 1996)
CCE	Cyber Counter Espionage
CCI	Command control interface / *Cyber Counterintelligence*
CCS	Cyber Counter Sabotage
CCT	Cyber Counter Terrorism
CD	Conflict Detection
CDL	Common data link
CDMA	Code division multiple access
CDR	Collision detection and resolution systems (automated SAA in UAS)
CEA	Cyber electromagnetic activities
CETC	Chinese Electronics Technology Group
CF	Computer Forensics
CFTA	Continental Free Trade Area
CFT	Certificate of flight trials
CI / CyI	Cyber Infiltration
CIA	Confidentiality, Integrity, Availability / Central Intelligence Agency
CIN	Common Information Network
CIR	Color Infrared – artificial standard where NIR bands shifted so that humans can see the infrared reflectance
C/N	Carrier to Noise ratio in HAPS, => C/ N_0
CM / CyM	Cyber Manipulation
CN3	Communications / navigation network node
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)	Concept(s) of Operations
CONUS	Continental United States
COS	Continued Operational Safety
COTS	Commercial off-the-shelf
CPA	Closest Point of Approach
CPA Spoof	CPA spoof involves faking a possible collision with a target ship
CPL	Commercial pilot's license
CPRC	Communist Party of the Republic of China
CR	Conflict Resolution / Close range / Cyber Raid (aka CyR)
CRH	Coaxial rotor helicopter
C_{RX}	Received Signal Power, watts
CS	Control station
CSDP	Common Security and Defense Policy missions (EU)
CSfC	Commercial Solutions for Classified Program
CSIRO	Commonwealth Scientific and Industrial Research Organization
CT	Counter Terrorism / Counter Terrorism Mission
CTOL	Conventional take-off and landing
C-UAS	Counter Unmanned Aircraft Systems (defenses / countermeasures)
CUAS	CSIRO Unmanned Aircraft Systems
CV	Collision Volume
CW / CyW	Cyber Warfare

D	Distance from transmitter in Range equation (Adamy D. -0., 2015)
DA	Danger area
Danger Close	Definition www.benning.army.mil/infantry/magazine/issues/2013/May-June/Myer.html Nov 14, 2013 – 1) *Danger close* is included in the "method-of-engagement" line of a call-for-fire request to indicate that friendly forces are close to the target. … *Danger close* is a term that is exclusive from risk estimate distance (RED) although the RED for 0.1 percent PI is used to define danger close for aircraft delivery. Pi = Probability of incapacitation. 2) Definition of "*Danger close*" (US DoD) In close air support, artillery, mortar, and naval gunfire support fires, it is the term included in the method of engagement segment of a call for fire which indicates that friendly forces are within close proximity of the target.
DARO	Defense Airborne Reconnaissance Office
DARPA	Defense Advanced Research Projects Agency
DAS	Detection by Acoustical Signature
dB	decibels
DC	Direct current
DCPA	Distance between vessels approaching CPA
DDD	Dull, dangerous, and dirty
DDOS	Distributed Denial of Service cyber attack
DE	Directed Energy
DEFCON	DEFCON is the world's longest running and largest underground hacking conference
DE / EMP /EP	Directed energy / Electromagnetic pulse
DEW	Directed – energy weapons
DF	Direction finding
DFCS	Digital Flight Control System
DHS	Department of Homeland Security
DIME	Diplomatic, information, military and economy
Dj	Jammer location – to-target receiver location distance, in km, FM 34-40-7

DJ	Data Jamming / Drone Jammer
DJI	Popular and functional Chinese made drone series: Mavic, Phantom, Ryze, Matrix, Spark, Enterprise, Inspire, Tello {However, banned by USA Army} (Newman, 2017)
DL	Downlink in HAPS
DLA	Date last accessed (usually a web reference)
DLI	Data Link interface
DNA	Deoxyribonucleic acid – genetic key to human life
DoD	Department of Defense
DOF	Degrees of Freedom
DOS	Denial of Service cyber attack
DPM	Direct power management / Dynamic Power Management
DPRK	*Democratic* People's Republic of Korea
DSA	Detect, sense and avoid / Dynamic Sense-and-Act
DSSS	Direct sequence spread spectrum
Dt	Enemy transmitter location -to- target receiver location, in km, FM 34-40-7
DT	Directional transmission
DTDMA	Distributed Time Division Multiple Access network radio system
DTED	Digital terrain evaluation data
DTH	Direct-To-Home
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
(E_b / N_0)	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
EHS	Enhanced surveillance
EIRP	Effective Isotropic 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
EMI	Electromagnetic interference
EMP	Electromagnetic pulse
EMR	Electromagnetic Radiation
EMS	Electromagnetic Spectrum
EMSVIS	Electromagnetic Spectrum Visible Light
EMW	Electromagnetic Waves
EO	Electro-optical (sensing) / Earth Observation
ERP_J	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
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

F	Field theory methods of CR
F	F*undamental frequency* is defined as the lowest frequency of a periodic waveform
f	Frequency, cycles / second RRE)
F_0	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: Predetermine flight mission path based on GPS coordinates
FCS	Flight control systems / Flight Control Station
FDF	Frequency Domain Filtering
FDM	Frequency division multiplexing
FHSS	Frequency hopping spread spectrum
FIR	Far Infrared (25-40) to (200-350) um
FIRES	Definition (US DoD – JP 3-0) the use of weapon systems to create a specific lethal or nonlethal effect on a target
FL	Flight level
FLIR	Forward-looking Infrared
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
FPGA	Field programmable gate array
FS	Fixed service

FSS	Fixed satellite service
FW	Fixed wing
G	Geometric methods of CR
G5S	G5 Sahel (G5S) Joint Force, has membership of five states; Burkina Faso, Mali, Mauritania, Niger, and Chad
gAR	Receiving Antenna Gain as a Factor
GBU	Guided Bomb Unit
GCHQ	Government Communications Headquarters (Britain)
GCS	Ground Control Station
GDPR	European Union's (EU) General Data Protection Regulation
GDT	Ground data terminal
GEO	Geostationary Earth orbit satellite
GeoFence	A geofence is a virtual perimeter for a real-world geographic area
GLOW	Gross lift-off weight for a missile / rocket
GNSS	Global Navigation Satellite 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
Harmonic	Frequency, which is an integer multiple of the fundamental frequency
H	Elevation of the jammer location above sea level, feet, FM 34-40-7
HAE	High altitude endurance
HALE	High altitude – long endurance
HAPS	High Altitude Platforms (generally for wireless communications enhancements)
HAPS UAVs	UAVs dedicated to HAPS service (example to communicate via CNPC links)
HEAT	High-explosive anti-tank warhead
HITL	Human in-the-loop
HMI	Human machine interface
HPA	High power amplifier
Ht	Elevation of enemy transmitter location above sea level, in feet, FM 34-40-7
HUD	Heads-up display
HUMINT	Human intelligence (spy's)
HVT	High value target (generally, for assassination)
I	Sound intensity, W x m^{-2} [Source strength S / $4\pi r^2$] (Uni-wuppertal, 2019)
IA	*Information Assurance* / Intentional cyber warfare attack
I-actors	Intentional Cyber Actors
IAS	Indicated air speed
ICAO	International Civil Aviation Organization
I.C.B.C.	International Center for Boundary Cooperation (China)

ICGs	Information centers of gravity
ICS	Internet Connection Sharing
ID	Information Dominance / Inspection and Identification
IEDs	Improvised Explosive Devices
IEEE	Institute of Electrical and Electronics Engineers
IEWS	Intelligence, electronic warfare and sensors
IFF	Identification, friend or foe (see chapter 19)
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
INS	Inertial navigation system
IMU	Inertial Measurement Unit
INFOSEC	*Information Security*
IO	Information Operations
IOC	Intergovernmental Oceanographic Commission
IOR	India Ocean Region
IoT	Internet of things
IPL	Insitu Pacific Limited
IR	Infrared
IRST	Infrared search and tracking
IS	Information Superiority
ISIS	*Islamic State of Iraq and al Sham* (ISIS)
ISR	Intelligence, Reconnaissance and Surveillance UAS Platform
ISTAR	Intelligence, surveillance, target acquisition and reconnaissance

ITU	International Telecommunications Union – Standards Organization
ITU-R	International Telecommunications Union – Radio Sector
IW	Information Warfare
JAGM	Joint-Air-to-Ground Missile
JAUS	Joint architecture for UAS
JDAM	Joint direct attack munitions
JFO	Joint fires observer
JP	Joint Publication – followed by military identifier
JDAM	Joint Direct Attack Munition
JNIM	Jama'at Nusrat al-Islam wal-Muslimin
JOPES	Joint Operation and Planning System / Execution System
JP	Joint Publication
J/ S	= the ratio of the jammer power to the desired signal power at the input to the receiver being jammed in dB
JTAC	Joint Terminal Attack Controller
JTIDS	Joint Tactical Information Distribution System (JTIDS) is an L band DTDMA
K	Boltzmann's constant (Noise component, RRE) (1.38 x 10 -23 J/K), Kelvin
K	for jamming frequency modulated receivers (jamming tuner accuracy), FM 34-40-7
KAMIKAZE	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.
KM	Katiba Macina Groups
L	λ / 2 in Eq. 20-5
LAANC	Low Altitude Authorization and Notification Capability

LASER	“A laser is a device that emits light through a process of optical amplification based on the stimulated emission of electromagnetic radiation. The term “laser” originated as an acronym for “light amplification by stimulated emission of radiation”. A laser differs from other sources of light in that it emits light coherently, spatially and temporally. Spatial coherence allows a laser to be focused to a tight spot, enabling applications such as laser cutting and lithography. Spatial coherence also allows a laser beam to stay narrow over great distances – collimation, enabling applications such as laser pointers. Lasers can also have high temporal coherence, which allows them to emit light with a very narrow spectrum. i.e., they can emit a single color of light. Temporal coherence can be used to produce pulses of light as short as a femtosecond. Used: for military and LEO devices for marking targets and ,measuring range and speed.” (Gould, R.G. 1959)
Laser JDAM	Laser Joint Direct Attack Munition – dumb bombs, all weather precision –guided munitions. Guided by an integrated inertial guidance system.
Laser rangefinder	Scope to assist targeting of munitions. Countermeasure: laser-absorbing paint
LGWs	Laser-guided weapons
Latency	Processing difference between time interval signal is transmitted and signal is received
LCDR	Lieutenant Commander
L/D	Lift to drag ratio
LDCM	Low Duty cycle methods
LEO	Low Earth Orbit Satellite
LGB	Laser-guided bomb, a guided bomb that uses semi-active laser guidance to strike a designated target with greater accuracy than an unguided one
LGTF	Liptako-Gourma task force (LGTF) established by Burkina Faso, Mali, and Niger to secure their shared border region
LIDAR	Light (Imaging) Detection and Ranging
LFS	Free-Space Loss as a Factor
LIPC	Laser-induced plasma channel
LJ	Propagation loss from jammer to receiver, in dBi

LMM	Lightweight Multi-role Missile (by Thales)
LOS	*Line-of-sight / Loss of Signal / Loss of Separation*
LOSAS	Low cost Scout UAV Acoustic System
LPA	Log periodic array
LPI	Low Probability of Intercept
LR	Long range
LRAD	Long Range Acoustic Device (Weapon) (Yunmonk Son, 2015)
LRCS	Low radar cross section
LRE	Launch and recovery element
LRF	Laser rangefinder
LS	Losses existing in the system (lumped together), dB (RRE)
LS	The propagation loss from the desired signal transmitter, in dBm
LSDB	Laser Small Diameter Bomb
LST	Laser spot trackers
LTA	Lighter than Air (airship) / Low noise amplifier
LTE /LTE+	Long Term Evolution – refers to mobile telecommunications coverage
LWIR	Long wave Infrared (sensor or camera)
M	Mass in Eq. 20-5
MA	Multi-agent methods of CR
MAD	Magnetic anomaly detection / Mutually Assured Destruction (International Nuclear Policies in 50s-70s)
MAE	Medium-altitude endurance
MAGTF	Marine air-ground task force
MALDRONE	Malware injected into critical SAA for UAS
MALE	Medium-altitude, long endurance UAS
MALE-T	Medium altitude long endurance – tactical UAS
MAME	Medium altitude, medium endurance
MASINT	Measurement and Signal Intelligence

MATS	Mobile Aircraft Tracking System
M-AUDS	Mobile Anti-UAV Defense System
MAV	Micro-air vehicle
Maverick	AGM -65 (USA) Missile
MCE	Mission control element
MCM	Mine countermeasures
MCU	Master Control Unit (SCADA)
MDR	Missed Detection Rates
MEB	Marine expeditionary brigade (14,500 marines and sailors)
MEMS	Micro-electromechanical systems (see chapter 19)
MEO	Medium Earth Orbit satellite
MFD	Multi Function display
MGTOW	Maximum gross takeoff weight
MHT	Multiple-hypotheses-testing
MIM	Man in the Middle cyber attack
MINUSMA	Multidimensional Integrated Stabilization Mission in Mali
MIR	Mid Infrared 5 to (25-40) um
MIT	Massachusetts Institute of Technology
MMI	Man-machine interface
MORS	Military Operations Research Society
MPI	Message-passing interface
MPO	Mission payload operator
MR	Medium range
MRE	Medium-range endurance
MRZR LMADIS	A Light Marine Air Defense Integrated System. System mounted on a Polaris MRZR diesel tactical combat vehicle. Comprised of two vehicles – one a command node and the other a sensor node. Once the threat is detected , the LMADIS uses jamming to disrupt the signals of the drone.
MS	Mobile service

MSL / AGL	MSL altitudes are measured from a standard datum, which is roughly equal to the average altitude of the ocean. So, an aircraft traveling 5,000 feet directly above a mountain that's 3,000 feet tall would have an altitude of 5,000 feet Above Ground Level (AGL) and 8,000 feet MSL.
MSR	Maritime Silk Road (China)
MTCR	Missile Technology Control Regime
MTI	Moving target indication
MTOM	Maximum take-off mass
Modulation	Signal Modulation is the process of varying one or more properties of a periodic waveform, called the carrier signal, with a modulating signal that typically contains information to be transmitted
MTOW	Maximum takeoff weight of an aircraft at which the pilot can attempt to take off, due to structural or other limits
MTS	Multi Spectral Targeting System
MTTR	Multitarget tracking radar/ Mean time to repair
MUAV	Mini-UAV or maritime UAV
MUJAO	Movement for Unity and Jihad in West Africa
MUM	Manned-unmanned teaming
MWIR	Midwave Infrared
MW	Microwave towers
N	Available Noise power, watts for HAPS
N	Terrain and ground conductivity factor, FM 34-40-7, where 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. 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)

NAV	Nano-air vehicle / NAV data message for GPS systems
NBC	Nuclear, biological and chemical warfare
NCO	Network-centric operations
NCW	Network Centric Warfare
NDRC	National Development and Reform Commission (China)
NEC	Network enabled capability
NGO	Non-Governmental Organization
NIEM	National Information Exchange Model
NIR	Near Infrared
NLOS	Non-line-of-sight
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	National Movement for Liberation of Azawad (Tuareg Rebellion)
NO	Numerical Optimization methods of CR
NOLO	No onboard live operator (USN)
NOTAM	Notice to airmen
NPS	National Park Service
NSA	National Security Agency (US)
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
OPA	Optionally piloted aircraft

OPAV	Optionally piloted air vehicle
OPSEC	Operations Security
OSI	Open systems interconnection
OTH	Over-the-horizon
P	Isotropic source of an electromagnetic pulse of peak power, MW
PANCAS	Passive Acoustic Non-Cooperative Collision Alert System
PCAS	Persistent close air support
PEIRP	Transmitter effective isotropic radiated power, watts
PFMS	Predictive Flight Management System
PEMSIA	Partnership in Environmental Management of the Seas of East Asia
PGM	Precision guided missile
PHOTINT	Photographic intelligence (usually sky – ground)
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 (SCADA)
PMIAA	Permissions Management: Identification, Authentication and Authorization
PNF	Plug and Fly with custom transmitter, receiver, battery and charger
PO	Psychological Operations
POS	Position and Orientation System
POV	Point of View
PPP	Precise Point Positioning

PPS	Precise positioning service (GPS)
PRC	People's Republic of China (China)
PSD	Power Spectral Density
PREACT	*Partnership for Regional East Africa Counterterrorism (PREACT)*
PRF	Pulse repetition frequency codes
PRM	Precision Runway Monitor
PSH	Plan-symmetric helicopter
PSR	Primary Surveillance Radar
P_t	Power output of the enemy drone, in watts, FM 34-40-7
PW / PSYWAR	Psychological Warfare
PWO	Principal Warfare officer
P(Y)	Precise Signal (GPS)
QOS	Quality of Service in HAPs
QUAS	QUT UAS (see below)
QUT	Queensland University of Technology
R	1 /Tb is the bit rate (b/s) in link equation
R^4	Energy density received at detected target range, R, nm
RA	Resolution Advisory
RAC	Range air controller
RADAR	Radio Detection and Ranging
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
RF	Radio Frequency

RGB	Red Green Blue for VIS camera
RGT	Remote ground terminal
Rician PDF	Rician probability density function
RIMPAC	Rim of the Pacific Exercise – Maritime
RL	Ramp launched
RMS	Reconnaissance management system /Root-mean-square
RN	Ryan-Nichols Qualitative Risk Assessment Equations 17-2, 17-3
RNRA	Ryan – Nichols Attack / Defense Scenario Risk Assessment for Cyber cases
ROA	Remotely operated aircraft
ROC	Republic of China (Taiwan)
RPA	Remotely piloted aircraft
RPH	Remotely piloted helicopter
RPV	Remotely piloted vehicle
RR	Radio regulations
RRE	Radar Range Equation
RSA	RSA (Rivest–Shamir–Adleman) -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
SAA	Sense and Avoid / *Sense and Act Systems*; replaces *See and Avoid function* of a human pilot

SAASM	Selective Availability Anti-Spoofing Module
SAE	Society of Automotive Engineers
SAM	Ace-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
SECDEF	Secretary of Defense
Shadowing	Airframe shadowing – UAV- Ground signal degradation during maneuver
SEZ	Special economic zones
SHM	Simple harmonic motion – represented by sine wave
SHORAD	Short Range Air Defense systems
SIGINT	Signals Intelligence
Signature	UAS detection by *acoustic*, optical, thermal and radio / radar
SJM	Salafi-Jihad Movement
SKASaC	Seeking airborne surveillance and control
SKYNET	Fictional artificial intelligence system that becomes self-aware
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
SPL	Sound pressure level, dB = 20 Log p / p_o [measured pressures to reference pressure] See Eq. 20-3,4; 6-7
SPS	Standard position service (GPS)
Spoofing	A Cyber-weapon attack that generates false signals to replace valid ones
Spot Sensors	ARS sensors that measure single locations without image library
SQL	SQL Injection – common malevolent code injection technique
SR	Short range
SRL	Systems readiness level
SSA	Static Sense-and-Act
SSP	Smart Skies Project
SSR	Secondary Surveillance Radar
SST	Self–Separation Threshold
STANAG 4856	Standard interfaces of UAV Control System for NATO UAV
STK	Satellite tool kit
STOL	Short take-off and landing
sUAS	Small Unmanned Aircraft System
SUAVE	Small UAV engine
SWARM	High level, dangerous collaboration of UAS, UUV, or unmanned boats
SWAT	Special Weapons and Tactics (police / paramilitary)
SWAP	Size, weight and power
SWIR	Shortwave infrared, 1400-3000 nm, 1.4 -3.0 um wavelength range

SZ	Safety Zone is defined as the horizontal and vertical separation criteria which form a cylindrical airspace volume around the UAS. In figure 3-2 that volume is defined by 1000 ft radius and 200 ft height. It is assumed that initially the UAS is in the center with 100 ft above and below the A/C.
T	In Range equation & environment, strength of a received signal, function of square or fourth power of distance, d, from transmitter (Adamy D. -0., 2015)
T	Time, sec (RRE)
T	Tension in Eq.20-5
TA	Traffic Advisory
TAC	Target air controller
TACAN	Tactical air navigation
TAR	Antenna noise temperature, Kelvin
TAS	True airspeed
TBO	Time between overhauls
TC	Type certificate
TCAS	Traffic alert and collision avoidance system
TCPA	Time to reach Closest Point of Approach
T_e	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
TIR	Thermal infrared = 8000 – 15000 nm, 8 -15 um
TL	Team Leader
TO	Take-off
Tort	A tort is an act or omission that gives rise to injury or harm to another and amounts to a civil wrong for which courts impose liability.
TP	Trajectory Prediction

TRANSCOM	U.S. Transportation Command networks
TRL	Technology readiness level
TS	Measured noise temperature, Kelvin units above absolute zero / Top Secret classification
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
UASC	Unmanned aircraft system commander
UASIPP	UAS Integration Pilot Program
UAS-p	UAS pilot
UAV	Unmanned aerial vehicle
UAV-p	UAV pilot
UBR	Uplink bit rate, Mb/s
UCAR	Unmanned combat armed rotorcraft
UCARS	UAV common automated recovery system
UCAV	Unmanned combat air vehicle
UCWA / UA	Unintentional cyber warfare attack
UGCS	Unmanned Ground Control Station
UGS	Unmanned ground-based station
UGV	Unmanned ground vehicle
UHF	Ultra High Frequency, 300 MHz – 3 GHz
UIT	Unintentional Insider Threats

UL	Upload link
UMTS	Universal Mobile Telecommunications System
UN	United Nations
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNICEF	United Nations Children's Fund
USD	Unmanned surveillance drone
UTM	Unmanned Traffic Management
UTV	Unmanned target vehicle
UUV	Unmanned underwater vehicle
UUNs / DUNSs	Urgent / deliberate universal needs statements
V	Visible
VFR	Visual flight rules
VIKI	Virtual Interactive Kinetic Intelligence
VLA	Very light aircraft
VLJ	Very Light Jet
VLAR	Vertical launch and recovery
VLOS	Visual Line of Sight
VMC	Visual Meteorological Conditions
VNIR	Visible light and near infrared 400 – 1400 nm, 0.4 – 1.4 um wavelength range
Voloport	Landing site for Volcopter
VTOL	Vertical take-off and landing
VTUAV	Vertical take-off UAV
WEF	World Economic Forum
WEZ	Weapon Engagement Zone
WRC	World Radio Conference Standards Organization
XO	Executive Officer of Naval vessel
ZIGBEE or KILLERBEE	Sniffing / penetration tools specific to UAS

Greek Symbols

λ	Wavelength in Hz, c / f where c= speed of light 344 m/s and f = frequency, Hz.
Σ	Radar Cross Sectional Area, m^2

Sources plus Bibliography below:

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.

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, http://www.Dtic.Mil/Dtic/Tr/Fulltext/U2/A487951.Pdf

Bibliography

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

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

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

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

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

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

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

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

Administrator. (2015, June 15). *Standing Wave and Fundamental Frequency.* Retrieved from Electronics Hub: https://www.electronicshub.org/?s=fundamental+frequency

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

entokey.com/acoustics-and-sound-measurement/: https://entokey.com/acoustics-and-sound-measurement/

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

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

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

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

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

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

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

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

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

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

Gould R. Gordon (1959). "The LASER, Light Amplification by Stimulated Emission of Radiation". In Franken, P.A.; Sands R.H. (eds.). *The Ann Arbor Conference on Optical Pumping, the University of Michigan, 15 June through 18 June* 1959. p. 128.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Mahon, J. (2012). *Classical Natural Law Theory St. Thomas Aquinas (1227-1274) – the "Angelic Doctor" Lecture.* Retrieved from Mahon, J. (2012). Classical Natural Law Theory St. Thomas Aquinas (1227-1274) – 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).

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

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

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

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

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

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

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

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

Muspratt, A. (2018, November 22). *New global drone standards proposed.* Retrieved from Defence

iQ: https://www.defenceiq.com/defence-technology/news/new-global-drone-standards-proposed

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

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

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

Newman, L. H. (2017, August 7). *THE ARMY GROUNDS ITS DJI DRONES OVER SECURITY CONCERNS.* Retrieved from WIRED: https://www.wired.com/story/army-dji-drone-ban/

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

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

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

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

Nichols, R. K., 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Said Emre Alper, Y. T. (December 2008). Compact Angular Rate Sensor System Using a Fully

Decoupled Silicon-on-Glass MEMS Gyroscope. *JOURNAL OF MICROELECTROMECHANICAL SYSTEMS, VOL. 17, NO. 6.*

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

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

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

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

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.

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

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

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

news.com/2018/03/
ras-consulting-investigations-hire-jeff-parisse-offer-sophisticated-uas-security-surveillance-services/

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

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

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

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

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

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

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

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

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

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

WebFinance, Inc. (2019). *Definition of Ethics. (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/

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

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

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

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

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

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

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

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

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

DETAILED TABLE OF CONTENTS

Chapter 8: Designing UAS Systems for Stealth

Student Learning Objectives
Designing a UAS for Stealth
Detection Signatures
Electromagnetic Spectrum (EMS)
Acoustic waves and Sound Waves in Air
Radio Waves and Light Waves in a Vacuum
RADAR / EW / Range Equation
One – Way Link Equation
Effective Range
Closer
Acoustic Signature Reductions
Visual Signature
Thermal Signature
Radio / RADAR Signature
Low flying UAS – Use Navigation Collision Avoidance RADAR
Discussion Questions
Bibliography
Readings

Chapter 9: Case Study Smart Skies Project

Student Learning Objectives
Safety
See and Avoid
Case Study: The Smart Skies Project
Smart Skies Architecture
Flight Test Capability
The Mobile Aircraft Tracking System (MATS)
The MATS Radar System
The MATS ADS-B Receiver
MATS Performance and Flight Characterization Testing
MATS Results
Sense-and Act
Dynamic SAA
SAA Experiments
UAS Actions
SAA Results
Sense-and Act Systems (Static)
SSA SOA Results
Automated Separation Management System (ASMS)

Cyber Manipulation (CM / CyM)
Cyber Assault (CA / CyA)
Cyber Raid (CR / CyR)
Cyber-Attack. See CyI, CyM, CyA, or CyR
Cybercrime (CC / CyC)
C4ISR
Electronic Warfare (EW)
Information Assurance (IA)
Information Operations (IO)
Information Superiority (IS)
Information Warfare (IW)
Intentional Cyber Warfare Attack (ICWA).
Intentional Cyber Actors (I-actors)
Network Centric Operations (NCO)
OPSEC
OPSEC – The Official Definition
Psychological Operations (PO)
Psychological Warfare (PW / PSYWAR)
Unintentional Cyber Actors (U-actors)
Unintentional Cyber Warfare Attack (UCWA/ UA)
Information Operations (IO) and the part EW plays
Electronic Warfare (EW) Purview
Communication Links for UAS are critical and must be secured
Intelligence Cycle
EW Generalities
Legacy EW definitions
ESM
ECM
ECCM
ES
EA
EP
COMINT
ELINT
ES/ESM
Main Contention
Communications Jamming
Jammer-to-Signal Ratio
Functions and features
Technical parameters
Equation 14-3 amount of jammer power output required

TABLE OF FIGURES

TABLE OF TABLES

TABLE OF EQUATIONS

of pressure squared because (I ≈ p2).
Eq. 19-4 Convenient form of Eq. 19-3 recognizes that log x^2 = 2 log x. So, SPL = 20 log p / p_o.
Eq. 19-5 Formula for the string's resonant frequency Fo
Eq. 19-6 Sound Pressure Level (SPL) & Sound Amplitude- derives the attack distance, d
Eq. 19-7 SPL as a f (SPL_{ref} – 20 log (d / dref))