Unmanned Aircraft Systems (UAS) in the Cyber Domain: Protecting USA’s Advanced Air Assets

Nichols Ryan Mumm Lonstein Carter
UNMANNED AIRCRAFT SYSTEMS (UAS) IN THE CYBER DOMAIN: PROTECTING USA'S ADVANCED AIR ASSETS

DEDICATIONS

From: Professor Randall K. Nichols, DTM

I dedicate this book to three groups: All US serving military personnel, US Coast Guard and law enforcement for keeping our blessed country safe; to my Angel wife of 35 years, Montine, and children Robin, Kent, Phillip, Diana and Michelle who have lived with a Dragon and survived; and finally, to all my students (over 50 years) who are securing the 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.
FORWARD
by R. Kurt Barnhart, Ph.D.

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-Étienne 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
forward 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
PREFACE

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 government 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](http://www.globalincidentmap.com) or [www.aviation.globalincidentmap.com](http://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](http://linkedin.com/in/randall-nichols-dtm-2222a691)  
Illi nunquam cedunt.  
"We Never Yield"

**Bibliography**


ACKNOWLEDGEMENTS

Books such as this are the products of contributions by many people, not just the musings of the authors. *Unmanned Aircraft Systems UAS in the Cyber Domain: Protecting USA’s Advanced Air Assets*, 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, 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 Kahn, Professor, SIS KSUP; 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 and Joel Anderson, KSU 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, a previous Dragon (Nichols ‘student) has gained recognition (licenses and certifications) in both law and cybersecurity. Professor Candice C. Carter, another Dragoness who is the creator of a cybersecurity program at Wilmington University and travels globally closing specialized cybersecurity breaches in major corporations. 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, Capt. John Paul Hood, US Army, Randall Mai, Jeremy Shay, Vincent Salerno, John Boesen, Diana K. Nichols, Josh Jacobs and Jordon McDonald.
We have a special place in our hearts for the excellent support from the *Cyber Conflict Documentation Project (CCDP)*, Herndon, VA. This type of advanced thinking is rare, and we are humbled, honored and pleased to be associated with their team headed by Mr. J. D Work, VP, Research Director and Principal.

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, counter-intelligence, INFOSEC, and sensitive computer applications. Throughout his career, Nichols has published six 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

- Counter-Terrorism / Counter- Intelligence / Counter-Espionage / Computer Security
- Countermeasures Asymmetric Warfare and Attack / Defense Scenarios against National Critical Infrastructure
Risk Assessment / Threat Analysis / Vulnerabilities Analysis / Countermeasures
SCADA – Advanced Cyber-weapons Creation / Deployment / Defense
UAS- Integrating Unmanned Aircraft Systems into National Airspace System

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 Doctorate 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 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. Subsequently, he accepted a Branch Chief position with the CIA and built a unique set of continuous monitoring capabilities in support of the ICD503 Risk Management Framework. He has spent a combined twenty-four years in government service building teams to address hard problems in the areas of national security, homeland security, and advanced technologies. 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 winning grants and contracts for UAV research and the creation of an advanced multiple fuel system where he operated the world’s first and only helicopter that flies 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 fellowship with the Cyber Conflict Documentation Project (CCDP) as he expands their research into autonomous systems in the virtual and physical worlds. Additionally, he serves as an adjunct professor at California University of Pennsylvania (CALU) instructing Homeland Security courses in the Criminal Justice Department.

Contact Information: Dr. Hans C. Mumm, 703-303-1752, hans@hansmumm.com, www.HansMumm.com
Wayne D. Lonstein, Esq. CISSP (Co-Author)

Wayne Lonstein holds a Bachelor of Arts Degree in Political Science from Wilkes University, a Bachelor of Science Degree in Cyber Forensics and Information Security from Syracuse University – Utica College, 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.

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

Mrs. 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). Mrs. Carter conducts research and constructs Asymmetric Warfare and Attack/Defense Scenarios against National Critical Infrastructure. She is the Team Lead for NASA Aeronautics Research Institute for Transformative Vertical Flight (TVF) Commercial Intra-City On-Demand VTOL group. Mrs. 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. Mrs. 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.

R. Kurt Barnhart, Ph.D. (Foreword)

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.
### Abbreviations: Acronyms

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

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AA</td>
<td>Anti-aircraft / Adaptive Antennas</td>
</tr>
<tr>
<td>AAA</td>
<td>Anti-aircraft artillery</td>
</tr>
<tr>
<td>AAIB</td>
<td>Air Accidents Investigation Board</td>
</tr>
<tr>
<td>AAM</td>
<td>Air-to-air missile</td>
</tr>
<tr>
<td>AAV</td>
<td>Autonomous air vehicle</td>
</tr>
<tr>
<td>A/C</td>
<td>Aircraft</td>
</tr>
<tr>
<td>ACAS</td>
<td>Airborne collision avoidance system / Assistant Chief of the Air Staff</td>
</tr>
<tr>
<td>ACL</td>
<td>Agent communication language / Autonomous control levels</td>
</tr>
<tr>
<td>ACS</td>
<td>Airborne control station (system)</td>
</tr>
<tr>
<td>ACTD</td>
<td>Advanced Concept Technology Demonstration</td>
</tr>
<tr>
<td>AD</td>
<td>Ansar Dine terrorist group</td>
</tr>
<tr>
<td>A/D</td>
<td>Attack / Defense Scenario</td>
</tr>
<tr>
<td>ADAC</td>
<td>Automated Dynamic Airspace Controller</td>
</tr>
<tr>
<td>ADC</td>
<td>Air data computer</td>
</tr>
<tr>
<td>ADF</td>
<td>Automatic direction finder/finding</td>
</tr>
<tr>
<td>ADS</td>
<td>Air Defense System (USA)</td>
</tr>
<tr>
<td>ADS-B</td>
<td>Automatic Dependent Surveillance – Broadcast systems</td>
</tr>
<tr>
<td>ADT</td>
<td>Air Data Terminal</td>
</tr>
<tr>
<td>AEW</td>
<td>Airborne early warning</td>
</tr>
<tr>
<td>AF</td>
<td>Adaptive Filtering</td>
</tr>
<tr>
<td>AFCS</td>
<td>Automatic flight control system</td>
</tr>
<tr>
<td>AFRICOM</td>
<td>US Africa Command</td>
</tr>
<tr>
<td>AGM</td>
<td>Air-to-surface missile</td>
</tr>
<tr>
<td>AGARD</td>
<td>Advisory Group for Aerospace Research and Development (NATO)</td>
</tr>
<tr>
<td>AGM-65</td>
<td>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.</td>
</tr>
<tr>
<td>AHA</td>
<td>Autopilot Hardware Attack</td>
</tr>
<tr>
<td>AHRS</td>
<td>Attitude and heading reference system</td>
</tr>
<tr>
<td>AI</td>
<td>Artificial intelligence</td>
</tr>
<tr>
<td>AIAA</td>
<td>American Institute of Aeronautics and Aerospace</td>
</tr>
<tr>
<td>AIC</td>
<td>Aeronautical Information Circular</td>
</tr>
<tr>
<td>AIP</td>
<td>Aeronautical Information Publication</td>
</tr>
<tr>
<td>AIS</td>
<td>Automated Identification System for Collision Avoidance</td>
</tr>
<tr>
<td>AJ</td>
<td>Anti-Jam</td>
</tr>
<tr>
<td>AM</td>
<td>Amplitude Modulation / al-Mourabitoun terrorist group</td>
</tr>
<tr>
<td>ANSP</td>
<td>Air Navigation Service Provider</td>
</tr>
<tr>
<td>AO</td>
<td>Area of Operations</td>
</tr>
<tr>
<td>AoA</td>
<td>Angle of Attack</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>APKWS</td>
<td>Advanced precision kill weapon system</td>
</tr>
<tr>
<td>AQ</td>
<td>Al-Qaida Terrorist Group – “the Base”</td>
</tr>
<tr>
<td>AOA</td>
<td>Aircraft operating authority</td>
</tr>
<tr>
<td>AQIM</td>
<td>al-Qaeda in the Islamic Maghreb</td>
</tr>
<tr>
<td>$A_r$</td>
<td>Receive antenna effective area, m$^2$</td>
</tr>
<tr>
<td>AR</td>
<td>Aspect ratio</td>
</tr>
<tr>
<td>AR drone</td>
<td>$AR$ stands for &quot;Augmented Reality&quot; in AR drone. AR Drone can perform tasks like object recognition and following, gesture following.</td>
</tr>
<tr>
<td>ARM</td>
<td>Anti-Radiation Munitions</td>
</tr>
<tr>
<td>ARS</td>
<td>Airborne Remote Sensing</td>
</tr>
<tr>
<td>ARW</td>
<td>Anti-radiation weapons</td>
</tr>
<tr>
<td>ASB</td>
<td>Advisory Service Bulletin</td>
</tr>
<tr>
<td>ASL</td>
<td>Airborne Systems Laboratory</td>
</tr>
<tr>
<td>ASMS</td>
<td>Automated Separation Management System</td>
</tr>
<tr>
<td>ASTM</td>
<td>American Society of Testing and Materials (ASTM)</td>
</tr>
<tr>
<td>ASTER</td>
<td>Agency for Science, Technology and Research</td>
</tr>
<tr>
<td>ASW</td>
<td>Anti-submarine warfare</td>
</tr>
<tr>
<td>AT</td>
<td>Aerial target</td>
</tr>
<tr>
<td>ATC</td>
<td>Air Traffic Control</td>
</tr>
<tr>
<td>ATM</td>
<td>Air Traffic Management</td>
</tr>
<tr>
<td>ATR</td>
<td>Automatic Target Recognition</td>
</tr>
<tr>
<td>ATS</td>
<td>Air Traffic Service</td>
</tr>
<tr>
<td>AUDS</td>
<td>Anti-UAV Defense System</td>
</tr>
<tr>
<td>AUV</td>
<td>Autonomous Underwater Vehicle</td>
</tr>
<tr>
<td>AUVSI</td>
<td>Association for Unmanned Vehicle Systems International</td>
</tr>
<tr>
<td>AV</td>
<td>Air Vehicle</td>
</tr>
<tr>
<td>AWSAS</td>
<td>All Weather Sense and Avoid System</td>
</tr>
<tr>
<td>BAMS</td>
<td>Broad Area maritime surveillance</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Defined as the Range within a band of wavelengths, frequencies or energy.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>BDA</td>
<td>Battle Damage assessment</td>
</tr>
<tr>
<td>BSR</td>
<td>Bilinear Signal Representation</td>
</tr>
<tr>
<td>BLOS</td>
<td>Beyond line-of-sight</td>
</tr>
<tr>
<td>BNF</td>
<td>Bind and Fly – with custom transmitter</td>
</tr>
<tr>
<td>BR&amp;T</td>
<td>Boeing Research and Technology</td>
</tr>
<tr>
<td>BVR</td>
<td>Beyond visual range</td>
</tr>
<tr>
<td>$c$</td>
<td>Speed of light ($3 \times 10^8$ m/s)</td>
</tr>
<tr>
<td>C</td>
<td>Combined methods of CR</td>
</tr>
<tr>
<td>C2 / C2W</td>
<td>Command and control / Command and Control Warfare</td>
</tr>
<tr>
<td>C3I</td>
<td>Command, control, communications and Intelligence</td>
</tr>
<tr>
<td>C4</td>
<td>Command, control, communications and computers</td>
</tr>
<tr>
<td>C4ISTAR</td>
<td>Command, control, communications, computers, intelligence, surveillance, target Acquisition and reconnaissance</td>
</tr>
<tr>
<td>CA</td>
<td>Collision Avoidance / Clear Acquisition (GPS) / Cyber Assault (aka CyA)</td>
</tr>
</tbody>
</table>
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
CAT  Collision Avoidance Threshold
CC / CyC  Cyber Crime
CCE  Cyber Counter Espionage
CCI  Command control interface / Cyber Counterintelligence
CCS  Cyber Counter Sabotage
CCT  Cyber Counter Terrorism
CD  Conflict Detection
CDL  Common datalink
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
CM / CyM  Cyber Manipulation
CN3  Communications / navigation network node
CNO  Chief Naval Operations
COA  Certificate of Waiver or Authorization
COB  Chief of the Boat
COMINT  Communications intelligence
COMJAM  Communications Jamming
COMSEC  Communications Security
CONOP(S)  Concepts of Operations
CONUS  Continental United States
COS  Continued Operational Safety
COTS  Commercial off-the-shelf
CPA  Closest Point of Approach
CPASpoof  CPA spoof involves faking a possible collision with a target ship
CPL  Commercial pilot’s license
CR  Conflict Resolution / Close range / Cyber Raid (aka CyR)
CRH  Coaxial rotor helicopter
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
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. \( \text{Pi} = \text{Probability of incapacitation} \). 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.
EA  Electronic Attack
EAS  Equivalent airspeed
EAU  East Africa union comprising of Israel and six East African states, Kenya, Ethiopia, Tanzania, Uganda, Rwanda and South Sudan
ECCM / EP  Electronic counter-countermeasures / Electronic Protection
ECM  Electronic countermeasures
ECR  Electronic combat reconnaissance
EDC  Estimated Date of Completion
EHS  Enhanced surveillance
Electrolaser  Electroschok 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
EMI  Electromagnetic interference
EMP  Electromagnetic pulse
EMR  Electromagnetic Radiation
EMS  Electromagnetic Spectrum
EMSVIS  Electromagnetic Spectrum Visible Light
EMW  Electromagnetic Waves
EO  Electro-optical (sensing)
ERP  = the effective radiated power of the jammer, in dBm
ERPs  = the effective radiated power of the desired signal transmitter, in dBm
ESM / ES  Electronic support measures / Electronic warfare support
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  Frequency, cycles / second RRE
F  Frequency in MHz, FM 34-40-7
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
FCS  Flight control systems
FDF  Frequency Domain Filtering
FHSS  Frequency hopping spread spectrum
FIR  Far-Infrared (25-40) to (200-350) um
FIRES  definition (US DoD – JP 3-0) the use of weapon systems to create a specific lethal or nonlethal effect on a target.
FL  Flight Level
FLIR  Forward-looking infrared
Fly-by-Wire  Predetermine flight mission path based on GPS coordinates
IEDs  Improvised Explosive Devices
IEWS  Intelligence, electronic warfare and sensors
IFF  Identification, friend or foe
IFR  Instrument flight rules
I&I  Interchangeability and Interoperability
IIT  Intentional Insider Threats
Imaging Sensors  ARS sensors that build images
IMINT  Imagery intelligence
IMM  Interacting-multiple-models tracker
INS  Inertial navigation system
IMU  Inertial Measurement Unit
INFOSEC  Information Security
IO  Information Operations
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
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)
K  2 for jamming frequency modulated receivers (jamming tuner accuracy), FM 34-40-7
KAMIKAZI  Means “Divine Wind,” Tactic best known for Japanese suicide A/C attacks on Allied Capital Vessels in WWII. UAS TEAMS or SWARMS could be directed in the same way.
KM  Katiba Macina Groups
λ  Wavelength in Hz
LAANC  Low Altitude Authorization and Notification Capability
LASER  “A laser is a device that emits light through a process of optical amplification based on the stimulated emission of electromagnetic radiation. The term "laser" originated as an acronym for "light amplification by stimulated...
emission of radiation". A laser differs from other sources of light in that it emits light coherently, spatially and temporally. Spatial coherence allows a laser to be focused to a tight spot, enabling applications such as laser cutting and lithography. Spatial coherence also allows a laser beam to stay narrow over great distances (collimation), enabling applications such as laser pointers. Lasers can also have high temporal coherence, which allows them to emit light with a very narrow spectrum, i.e., they can emit a single color of light. Temporal coherence can be used to produce pulses of light as short as a femtosecond. Used: for military and law enforcement devices for marking targets and measuring range and speed.” (Wiki-L, 2018)

Laser rangefinder Scope to assist targeting of munitions. Countermeasure: laser-absorbing paint
Latency Processing difference between time interval signal is transmitted and signal is received
Laser-guided weapons
LCDR Lieutenant Commander
L/D Lift to drag ratio
LDCM Low Duty cycle methods
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
LIPC laser-induced plasma channel
L = the 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
LRCS Low radar cross section
LRE Launch and recovery element
LRF Laser range-finder
L5 Losses existing in the system (lumped together), dB (RRE)
L5 The propagation loss from the desired signal transmitter, in dBm
LSDB Laser Small Diameter Bomb
LST Laser spot trackers
LWIR Long wave Infrared (sensor or camera)
MA Multi-agent methods of CR
MAD Magnetic anomaly detection
MAE Medium-altitude endurance
MAGTF Marine air-ground task force
MALDRONE Malware injected into critical SAA for UAS
MALE Medium-altitude, long endurance
MALE-T Medium altitude long endurance – tactical UAS
MAME Medium altitude, medium endurance.
MASINT Measurement and Signal Intelligence
MATS Mobile Aircraft Tracking System
M-AUDS Mobile Anti-UAV Defense System
MAV Micro-air vehicle
Maverick AGM -65 (USA) Missile
MCE Mission control element
MCM Mine countermeasures
MCU Master Control Unit
MDR Missed Detection Rates
MEB Marine expeditionary brigade (14,500 marines and sailors);
MEMS Micro-electromechanical system
MFD Multifunctional display
MGTOW Maximum gross take-off weight
MHT Multiple-hypotheses-testing
MIM Man in the Middle cyber attack
MINUSMA Multidimensional Integrated Stabilization Mission in Mali
MIR Mid Infrared 5 to (25-40) um
MIM Man in the Middle cyber attack
MMI Man-machine interface
MORS Military Operations Research Society
MPI Message-passing interface
MPO Mission payload operator
MR Medium-range
MRE Medium-range endurance
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.
MTI Moving target indication
MTOM Maximum take-off mass
Modulation Signal Modulation is the process of varying one or more properties of a periodic waveform, called the carrier signal, with a modulating signal that typically contains information to be transmitted
MORS Military Operations Research Society
MTOW Maximum takeoff weight of an aircraft at which the pilot can attempt to take off, due to structural or other limits.
MTS Multi Spectral Targeting System
MTTR Multitarget tracking radar/Mean time to repair
MUAV Mini-UAV or maritime UAV
MUJAO Movement for Unity and Jihad in West Africa
MUM Manned-unmanned teaming
MWIR Midwave Infrared
MW microwave towers
N Terrain and ground conductivity factor, FM 34-40-7
5 = very rough terrain with poor ground conductivity
4 = moderately rough terrain with fair to good ground conductivity
3 = Farmland terrain with good ground conductivity
2 = Level terrain with good ground conductivity

Note. 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
NEC, Network enabled capability
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, the National Movement for Liberation of Azawad (Tuareg Rebellion)
NO, Numerical Optimization methods of CR
NOLO, No onboard live operator (USN)
NOTAM, Notice to airmen
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 Manufacture
OIO, Offensive Information Operations
OLOS, Out-of-the-line-of-sight
OODA, Decision Loop: Observe, Orient, Decide, Act
OPA, Optionally piloted aircraft
OPAV, Optionally piloted air vehicle
OPSEC, Operations Security
OSI, Open systems interconnection
OTH, Over-the-horizon
P, Isotropic source of an electromagnetic pulse of peak power, Mw
PANCAS, Passive Acoustic Non-Cooperative Collision Alert System
PCAS, Persistent close air support
PFMS, Predictive Flight Management System

---

1 FM 34-40-7
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
PLAN  Peoples Liberation Army Navy (China)
PLC  Programmable Logic Controllers
PNF  Plug and Fly with custom transmitter, receiver, battery and charger
PO  Psychological Operations
POS  Position and Orientation System
PPS  Precise positioning service (GPS)
PRC  Peoples 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)
QUAS  QUT UAS
QUT  Queensland University of Technology
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)
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
RIMPAC  Rim of the Pacific Exercise - Maritime
RL  Ramp launched
RMS  Reconnaissance management system /Root-mean-square
ROA  Remotely operated aircraft
ROC  Republic of China (Taiwan)
RPA  Remotely piloted aircraft
RPH  Remotely piloted helicopter
RPV  Remotely piloted vehicle
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>RRE</td>
<td>Radar Range Equation</td>
</tr>
<tr>
<td>RSA</td>
<td>RSA (Rivest–Shamir–Adleman) -authors of early public –key cryptographic system</td>
</tr>
<tr>
<td>RSTA</td>
<td>Reconnaissance, surveillance and target acquisition</td>
</tr>
<tr>
<td>RTA</td>
<td>Dubai Roads and Transport Authority</td>
</tr>
<tr>
<td>RTF</td>
<td>Off- the- shelf, Ready -to -Fly</td>
</tr>
<tr>
<td>RTS</td>
<td>Remote tracking station/Request to send/Release to service</td>
</tr>
<tr>
<td>RTU</td>
<td>Remote Terminal Unit</td>
</tr>
<tr>
<td>RUAV</td>
<td>Relay UAV</td>
</tr>
<tr>
<td>RWR</td>
<td>Radar warning receiver</td>
</tr>
<tr>
<td>$\Sigma$</td>
<td>Radar Cross Sectional Area, m$^2$</td>
</tr>
<tr>
<td>SAA</td>
<td>Sense and Act Systems; replaces See and Avoid function of a human pilot</td>
</tr>
<tr>
<td>SAASM</td>
<td>Selective Availability Anti-Spoofing Module</td>
</tr>
<tr>
<td>SAE</td>
<td>Society of Automotive Engineers</td>
</tr>
<tr>
<td>SAM</td>
<td>Aces- to -Air Missle</td>
</tr>
<tr>
<td>SAMPLE</td>
<td>Survivable autonomous mobile platform, long-endurance</td>
</tr>
<tr>
<td>SAR</td>
<td>Synthetic aperture radar / Search and rescue- especially using helicopters</td>
</tr>
<tr>
<td>SAS</td>
<td>Safety Assurance System</td>
</tr>
<tr>
<td>SATCOM</td>
<td>Satellite communications</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition systems</td>
</tr>
<tr>
<td>SCHEMA</td>
<td>Security Incident Identification</td>
</tr>
<tr>
<td>SCIF</td>
<td>Sensitive Compartmented Information Facility</td>
</tr>
<tr>
<td>SCS</td>
<td>Shipboard control system (or station) / Stereo Camera System</td>
</tr>
<tr>
<td>SE</td>
<td>Synthetic environment</td>
</tr>
<tr>
<td>SECDEF</td>
<td>Secretary of Defense</td>
</tr>
<tr>
<td>SIGINT</td>
<td>Signals Intelligence</td>
</tr>
<tr>
<td>Signature</td>
<td>UAS detection by acoustic, optical, thermal and radio /radar</td>
</tr>
<tr>
<td>SJM</td>
<td>Salafi-Jihad Movement</td>
</tr>
<tr>
<td>SKASaC</td>
<td>Seeking airborne surveillance and control</td>
</tr>
<tr>
<td>SM</td>
<td>Separation Management</td>
</tr>
<tr>
<td>SME</td>
<td>Subject matter expert</td>
</tr>
<tr>
<td>SMR</td>
<td>Single main rotor</td>
</tr>
<tr>
<td>S/N</td>
<td>$S / N =$ is one pulse received signal to noise ratio, dB</td>
</tr>
<tr>
<td>SOA</td>
<td>Static Obstacle – Avoidance system</td>
</tr>
<tr>
<td>SPS</td>
<td>Standard position service (GPS)</td>
</tr>
<tr>
<td>Spoofing</td>
<td>A Cyber-weapon attack that generates false signals to replace valid ones</td>
</tr>
<tr>
<td>Spot sensors</td>
<td>ARS sensors that measure single locations without image library.</td>
</tr>
<tr>
<td>SQL</td>
<td>SQL Injection – common malevolent code injection technique</td>
</tr>
<tr>
<td>SR</td>
<td>Short range</td>
</tr>
<tr>
<td>SRL</td>
<td>Systems readiness level</td>
</tr>
<tr>
<td>SSA</td>
<td>Static Sense-and -Act</td>
</tr>
<tr>
<td>SSP</td>
<td>Smart Skies Project</td>
</tr>
<tr>
<td>SSR</td>
<td>Secondary Surveillance Radar</td>
</tr>
<tr>
<td>SST</td>
<td>Self – Separation Threshold</td>
</tr>
<tr>
<td>STANAG 4856</td>
<td>Standard interfaces of UAV Control System for NATO UAV</td>
</tr>
</tbody>
</table>
STK   Satellite toolkit
STOL  Short take-off and landing
sUAS  Small Unmanned Aircraft System
SUAVE Small UAV engine
SWARM High level, dangerous collaboration of UAS, UUV, or unmanned boats
SWAT  Special Weapons and Tactics (police / para military)
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     Time, sec (RRE)
TA    Traffic Advisory
TAC   Target air controller
TACAN Tactical air navigation
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
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.
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
TSTCP Trans-Sahara Counterterrorism Partnership. TSCTP partners include Algeria,
       Burkina Faso, Cameroon, Chad, Mali, Mauritania, Morocco, Niger, Nigeria,
       Senegal, and Tunisia.
TUAV  Tactical UAV
UA    Unmanned Aircraft (non-cooperative and potential intruder)
U-Actors Unintentional Cyber Actors
UAM   Urban Air Mobility
UAPO  Unmanned Aircraft Program Office
UAS   Unmanned aircraft system
UAScdr Unmanned aircraft system commander
UASIPP UAS Integration Pilot Program
UAS-p  UAS pilot
UAV  Unmanned aerial vehicle
UAV-p  UAV pilot
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
UIT  Unintentional Insider Threats
UN  United Nations
UNICEF  United Nations Children’s Fund
USD  Unmanned surveillance drone
UTM  Unmanned Traffic Management
UTV  Unmanned target vehicle
UUU  Unmanned underwater vehicle
UUNs / DUNSS  Urgent / deliberate universal needs statements
V  Visible
VFR  Visual flight rules
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 Volocopter
VTOL  Vertical take-off and landing
VTUAV  Vertical take-off UAV
WEZ  Weapon Engagement Zone
XO  Executive Officer of Naval vessel
ZIGBEE or KILLERBEE  Sniffing / penetration tools specific to UAS

Sources:


TABLE OF CONTENTS

Title Page
Copyright/Publication Page
Dedication
Foreword
Preface
Acknowledgements
List of Contributors
Acronyms
Table of Contents
Table of Figures
Table of Tables
Table of Equations

Section 1: The UAS Playing Field
Unmanned Aircraft Systems (UAS) – Defining UAS Cyber Playground

Chapter 1: A View of the UAS Market

- Student Learning Objectives
- Marketplace History
- UAS Marketplace Drivers
- Public Acceptance
- Infrastructure Influence
- Restricting Drones Flight
- Commercial
- Retail
- UAS For Hire – Urban Air Mobility and eVTOL
- E-VTOL Cybersecurity
- Agriculture
- Architecture and Construction
- Chinese drones
- Discussion Questions
- Bibliography
- References

Chapter 2: UAS Law - Legislation, Regulation and Adjudication

- Student Learning Objectives
- Law & Technology – The Tortoise and the Hare
- Transportation in the United States – Lessons from the Past Help Guide the Future
- Regulation of the Automobile
- The Next Transportation Challenge – Aviation
- Aviation Design and Manufacture Standards
Regulated Activity Coexisting with Unregulated Activity
Regulating Unmanned Aerial Systems – Smaller Aircraft Larger Problems
Class A Airspace
Class B Airspace
Class C Airspace
Class D Airspace
Class E Airspace
Class G Airspace
Regulating UAS Operation in the NAS
Civilian UAS Operations – Striking Legislative Balance
UAS and Constitutional Rights
Scenario 1
Scenario 2
Common Law Fills the Technology Gap
UAS Manufacturing and Design Standards
Conclusions
Discussion Questions
Bibliography
References


Student Learning Objectives
What Is The Counter-UAS Problem?
Operational Protection from Hostile UAS Attacks – A Helicopter View
Countering UAS Air Threats
Vulnerabilities Perspective
Conventional Vulnerabilities of Air Defense Systems (ADS), Attacks by sUAS and Countermeasures
Conventional Countermeasures Against sUAS / UAS
Passive
Aggressor Counter-Countermeasures Specific to UAS Deployment – Swarm
Autonomy vs. Automation
Commercial Small Unmanned Aircraft Systems (sUAS) Overview
Airborne Sensing Systems
Sensor Parameters
Autopilot
SAA Subsystems
SAA Services and Sub-Functions
Low Hanging Fruit
SCADA
“UAS Are Just Flying SCADA Machines!”
Attack Vectors
Cyber-Attack Taxonomy
Espionage
Software Based Vulnerabilities
Insider Threat Vulnerabilities
Intentional Insider Threats
Hardware-Based Vulnerabilities
General Attack Possibilities
Conclusions
Discussion Topics
Bibliography
Readings
Secondary References

Section 2: UAS Information Security, Intelligence and Risk Assessment
Information Security (INFOSEC), Intelligence and Risk Assessments

Chapter 4: INFOSEC – Protecting UAS Information Channels & Components

Student learning objectives.
Basic Concepts in Information Security
Policy Questions
How Much Protection is needed?
How long the information must be protected?
Security Attributes
Confidentiality
Integrity
Availability
Security Phases
Protection
Detection
Protected Class
The Unprotected Class
Unknown Class
Insider Class
Counter – Detection Class
Risk
Now Risk
Threats
Vulnerabilities
Now Risk decisions
Future Risk analysis
Systems Engineering an Information Security Solution
Identifying Security Requirements for an Enterprise
Explicit Requirements
Implicit Requirements
Derived Requirements
Security Solutions Consideration
UAS Security Challenges
Chapter 5: Intelligence and Red Teaming

Student learning objectives.
Basic Concepts in Intelligence
The Intelligence Cycle
Common Problems in Intelligence
Sources of Intelligence Data
Understanding Attack/Defend as a Tool
Red Teaming
Blue Teaming
Benefits
Discussion Questions
Sources for more information

Chapter 6: Case Studies in Risk for UAS

Student learning objectives
Case 1: When the Enemy Hacks Your Data Stream
Case 2: When Your Drone Goes Missing
Case 3: When Pilots Are Targeted for Assassination
Case 4: When Commercial Drones Spy Domestically
Case 5: The Drone That Steals Your Wi-Fi Password
Concluding Thoughts
References

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: UAS 7 SAA Methodologies, Conflict Detection & Resolution Principles

Student Learning Objectives
Sense and Avoid (SAA) Function
System Configurations and Subsystems
Sensor Categories
In situ Sensing
Remote Sensing
Units
Sensor Types
Spot sensors
Imaging Sensors
Camera
Visible Spectrum Cameras (VIS) and Near-Infrared (NIR) Cameras
Long-Wave Infrared Cameras (LWIR)
Hyperspectral Images
LIDAR
Synthetic Aperture Radar (SAR)
Live Video Gimbals for VIS, MWIR and LWIR Cameras
Predicting Conflict
Conflict Detection and Resolution Principles
CDR Architecture
Sensing
Cooperative Sensors
Non-Cooperative Sensors
Intruder Aircraft
Trajectory Prediction
Conflict Detection
Conflict Resolution
Evasion Maneuvers
CDR Taxonomy
Discussion Questions
Bibliography
Readings

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
Section 4: UAS Weapons & ISR & IO
Payloads - UAS Delivery Systems

Chapter 10: UAS Intelligence, Surveillance and Reconnaissance (ISR)

Student Learning Objective
History/Background of UAS ISR
History of Photography
Remote Sensing
UAS ISR-Purpose/Market Sector/Product/Economic Opportunity
Purpose of Technology
Product/ Economic Opportunity
Mission Drives the Sensor Requirements
Standard ISR Camera Sensors
Multispectral and Hyperspectral Sensors
A Changing World Creates a Changing Target Set and Sensor Requirement- SWIR
Bomb-Sniffing Drone Technology
Cave Mapping
Mission and Sensor Planning and Considerations
Importance of stabilized head
Protecting the Systems from the Cyber Threat
Conclusions
Chapter 11: UAS Weapons

Student Learning Objective
History
Desert Storm:
Events in 2000
Post 9/11/2001
Weapons Systems (Lethal)
Hellfire
GBU-12
GBU-38/GBU-54
Repetition Frequency (PRF) Codes
Code Description
Code Allocation and Assignment
Future weapons
Weapons (Non-lethal)
Anti-Personnel
Optical Weapons
Acoustics
Directed Energy (High Powered Microwaves)
Restraining Mechanisms
Anti-Materials
Chemical / Biological
Directed Energy/Electromagnetic Pulse (DE/EP)
Restraining Mechanisms
Protecting the Weaponized Systems from the Cyber Threat/Response
Conclusions
Questions
Bibliography
References

Chapter 12: UAS System Deployment and Information Dominance (ID)

Student Learning Objectives
UAS in Military and Commercial Service
Information Dominance (ID)
Information Warfare
Information-Based Warfare
High-Altitude Endurance (HAE) and Medium – Altitude Endurance Unmanned Air Vehicles (UAVs)
Offensive Information Operations (OIO)
Network-centric Operations (NCO)
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 and Latency

Student Learning Objectives
What are the Types of UAV’s and how are they Categorized?
Components of the UAS Data-Link and their functions
The UAV and Ground Control Station
The Datalink - Essential Operations, Functions and Capabilities
Attributes to consider in the design of the Data Link
Globally available secure frequency with sufficient bandwidth and assignability
Resistance to unintentional interference
Low Probability of detection and interception
Signal Encryption and Security
Anti-Deception Capability
ARM Resistant Capability
Anti-Jam Capability
Global Radio Frequency Functionality and Adaptability
Resistance to Unintentional Interference
Low Probability of Intercept (“LPI”)
Signal Encryption and Security
Resistance to Deception
Anti-ARM
Anti-Jam (AJ) Capabilities
Additional Considerations
Digital vs Analog
System Interface Considerations
Data-Rate
Closed Loop Control
Interchangeability, Interoperability and Standardization
Datalink Latency
The Current Environment
Flight Control Technology
Low Endurance
Medium Endurance
High Endurance
Discussion Questions
References
Chapter 14: Exposing UAS Vulnerabilities via Electronic Warfare (EW) and Countering with Low Probability Intercept Signals (LPI)

Student Learning Objectives
Modern Communication Threats to UAS
Definitions
Cyber Infiltration (CI / CyI)
Cyber Manipulation (CM / CyM)
Cyber Assault (CA / CyA)
Cyber Raid (CR / CyR)
Cyber-Attack. See CyI, CyM, CyA, or CyR
Cybercrime (CC / CyC)
C^4ISR
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
Radar Range Equation
LPI Communication Signals
LPI Restrictions
Discussion Questions /Assignment
Bibliography
Readings

**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*

Student Learning Objectives
Africa – Overview
Africa - The Facts
Economics
The Spread of Radical Islam across Africa
Africa - Al-Qaeda and Islamic State
The Spread of Radical Islam across Africa
Africa - Al-Qaeda and Islamic State
Salafi-Jihad Movement
Africa - Katiba Macina Groups (KM)
Africa - Al-Qaeda and Islamic State
Tuareg Rebellion [NMLA]
Africa - Ansar Dine (AD)
Islamic State of Iraq and al Sham (ISIS)
Africa - Counterterrorism Efforts
Why Fight Terror Groups in Africa?
Joint European Union Counterterrorism
G5 Sahel – Five Africa States United
United Nations Counterterrorism
France - Operation Serval
France - Operation Barkhane
French EADS Harfangs
France - West Africa
Trans-Saharan Counterterrorism Partnership (TSCTP)
Partnership for Regional East Africa Counterterrorism (PREACT)
United States - West Africa
United States - East Africa
United States - North Africa
United States - Central Africa
Cameroon
China Counterterrorism
Israel Counterterrorism Efforts
Germany - West Africa
Pakistan - West Africa
Egypt - North Africa
Italy/France/United States - East Africa
Africa Maritime Piracy and Violence
Africa’s Maritime Security
China – Africa’s Maritime
European Union Naval Force’s (EUNAVFOR)
Morocco’s Commercial Activity in Africa
UNICEF and Virginia Tech
Summary
Discussion Questions
Bibliography
Readings

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

Student Learning Objectives
Location of the Spratly Islands and Their Strategic Importance
Target Drones
Shark Swarm and Wanshan Marine Test Field
Fast Drone Ship
Long-Range UUV
Crisis Watch
A Birds’ Eye View
Red Drones over Disputed Seas
S-100 by Scheibel
ASN-209
BZK -005
GJ- 1 Chinese UCAV
Interference with US Ships – Exploring the Cyberweapon deployed from UAS against US Capital Ships
The Case for Cyber Weapon Spoofing of Legacy GPS Signals Affecting Us Navy and Commercial Vessels in Pacific
U.S Navy Vessel Collisions in the Pacific
Navy Response
The Navy Official Reaction regarding the possibility of Cyber-Weapon or Cyber-Attack
The Case for a Cyber Weapon
Surfacing Questions
Closest Point of Approach (CPA) Spoofing
How could be the GPS chaos to US Vessels be achieved?
Discussion Questions
Bibliography
Readings
Patents
TABLE OF FIGURES

Chapter 1: A View of the UAS Market

Figure 1-1 Consumer sUAS registration as of December 31, 2017
Figure 1-2 U.S. Postal Service Survey Results
Figure 1-3 State of Florida Drone Signage
Figure 1-4 Airspace Systems Interceptor autonomous aerial drone
Figure 1-5 Amazon Prime Air
Figure 1-6 Zipline drone testing package drop
Figure 1-7 Uber Elevate
Figure 1-8 Uber Flying Skies
Figure 1-9 Uber UAM Station Check-in
Figure 1-10 EHang 184 E-VTOL
Figure 1-11 Model X 2017
Figure 1-12 Nero temperature data collection
Figure 1-13 DJI Founder Frank Wang

Chapter 2: UAS Law - Legislation, Regulation and Adjudication

Figure 2-1 Tortoise and Hare
Figure 2-2 Ford Motor Company Production Plant
Figure 2-3 (National Safety News 1922)
Figure 2-4 Flights Everywhere
Figure 2-5 Jet Setting
Figure 2-6 Two 747 aircraft crashed on the runway
Figure 2-7 Boeing Company
Figure 2-8 Tragedy in Pacific South West, 1978
Figure 2-9 FAA Airspace Classification
Figure 2-10 Sample COA
Figure 2-11 Drone Crash into Commercial Airline
Figure 2-12 Scenario 1 Part 1
Figure 2-13 Scenario 1 Part 2
Figure 2-14 Scenario 2
Figure 2-15 No Trespassing
Figure 2-16 Three Mile Island


Figure 3-1 Drone Crash into 737-700 Passenger Jet While Landing At Mozambique
Figure 3-2 Self-Separation and Collision Volume
Figure 3-3 Decision Process to Avoid Collision of Two Aircraft
Figure 3-4 for Legacy SCADA System for Chemical Plant
Figure 3-5 for Corporate SCADA System
Figure 3-6 UAS SCADA System Internals
Figure 3-7 IT Systems vs. Control Systems

Chapter 4: INFOSEC – Protecting UAS Information Channels & Components
Figure 4-1 the Detection Timeline

Chapter 5: Intelligence & Red Teaming
Figure 5-1 the Intelligence Cycle

Chapter 7: UAS SAA Methodologies, Conflict Detection & Resolution Principles
Figure 7-1 Drone Survival Guide
Figure 7-2 SAR Imaging Geometry for Strip Mapping Option
Figure 7-3 SAR Modes of Operation
Figure 7-4 shows a TASE 500 that works with VIR, MWIR and LWIR cameras.
Figure 7-5 Drone Jammer Model KWT-FZQ used for Police interception.
Figure 7-6 Intruder Aircraft and SAA Decisions
Figure 7-7 TCAS II Terminology
Figure 7-8 TCAS II Conceptual Framework
Figure 7-9 TCASS II Cockpit View

Chapter 8: Designing UAS Systems for Stealth
Figure 8-1 EMS
Figure 8-2 EMS Functions
Figure 8-3 show the conversion for sound and acoustic wave period to frequency and back.
Figure 8-4 shows the Sound EMS Regions
Figure 8-5 Equal Loudness Contours
Figure 8-6 EMS Reduced
Figure 8-7 Conversion Chart – Frequency to Wavelength Radio and Light Waves in a Vacuum
Figure 8-8 RADAR Frequency Bands
Figure 8-9 RADAR Bands
Figure 8-10 Path through Link
Figure 8-11 One – Way RADAR Equation
Figure 8-12 Two Way RADAR Equation (Bi-Static)

Chapter 9: Case Study Smart Skies Project
Figure 9-1 SSP Architecture
Figure 9-2 Cessna 172R Cockpit
Figure 9-3 Cessna 172R Flying View
Figure 9-4 ARCAA Flamingo UAS
Figure 9-5 ARCAA Heli UAS
Figure 9-6 MATS
Figure 9-7 ARCAA ASMS
Chapter 10: UAS Intelligence, Surveillance and Reconnaissance (ISR)

Figure 10-1 Boston Harbor, 1860, James Wallace Black.
Figure 10-2 GoPro Camera Comparisons
Figure 10-3 Raytheon’s Multi-Spectral Targeting System (MTS) for Predator MQ-1
Figure 10-4 Hyperspectral Imaging
Figure 10-5 Shortwave Infrared (SWIR) bands
Figure 10-6 SWIR advantage over old ISR sensors
Figure 10-7 for bomb sniffing logic for UAS
Figure 10-8 Importance of stabilized head
Figure 10-9 MIM Attack Effects

Chapter 11: UAS Weapons

Figure 11-1 BGM-34B
Figure 11-2 MQ-1 in the Smithsonian
Figure 11-3 MQ-9 Reaper
Figure 11-4 Typical Reaper load out with the Hellfire missiles on the right and a GBU-12 on the left
Figure 11-5 Hellfire Weapon Engagement Zone
Figure 11-6 GBU-12 loaded on the Reaper UAS
Figure 11-7 Sample GBU-12 delivery envelope
Figure 11-8 GBU-38 left and GBU-54 right
Figure 11-9 MQ-9 Reaper with GBU-38 JDAMs loaded
Figure 11-10 GBU-39B/B
Figure 11-11 Active Denial System
Figure 11-12 Counter-electronics High-powered Microwave Advanced Missile
Figure 11-13 Portable Jammer
Figure 11-14 Drone launches a net to capture another drone

Chapter 12: UAS System Deployment and Information Dominance (ID)

Figure 12-1 UAS Surveillance Network
Figure 12-2 UAV Evolution
Figure 12-3 United States Coast Guard and Navy
Figure 12-5 sUAS Puma
Figure 12-6 United States Coast Guard UAS Concept

Chapter 13: Data Links Functions, Attributes and Latency

Figure 13-1 Mini Drones
Figure 13-2 Remote-Controlled Attack UAS, MQ-9
Figure 13-3 Data Links Overlay: Ground Station, Satellite, UAS
Figure 13-4 Partial EMS
Figure 13-5 LDCM Method Overlay
Figure 13-6 Harris KGV-72 encryption device for secure messages
Figure 13-7 Enemy Captured RQ-170
Figure 13-8 Spoofing the Spoofee
Figure 13-9 ARM Processes
Figure 13-10 BSR Representation.
Figure 13-11 BSR Representation (alt)
Figure 13-12 US Army Warning Letter
Figure 13-13 Data Lifecycle of UAS
Figure 13-14 Flight Simulation Game
Figure 13-15 JTIDS View
Figure 13-16 Lightning Strike and Latency
Figure 13-17 Security - Latency Trade-off

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

Figure 14-1 Information Operations
Figure 14-2 DOD JOPES
Figure 14-3 DOD Vision: Future of Internet with IW / IO integration
Figure 14-4 PCAS Vision: precise, digital, portable air-ground strike coordination
Figure 14-5 High -Level C4 Operational Concept Incorporating UAS
Figure 14-6 NASA’s Unmanned Aircraft Systems (UAS) Integration in the National Airspace
Figure 14-7 Intelligence Cycle
Figure 14-8 shows the communication jamming geometry
Figure 14-9 UAV Link Jamming Geometry
Figure 14-10 J/S Calculation Example
Figure 14-11 Chain Home Radar Stations Defending England
Figure 14-12 Chain Home Radar Station
Figure 14-13 Simple Radar Block Diagram
Figure 14-14 Simple Surveillance Radar
Figure 14-15 Spread Spectrum Signal
Figure 14-16 Cyber Electromagnetic Activities
Figure 14-17 CEA / CEW in the view of Total War

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

Figure 15-1 Africa: Economics
Figure 15-2 Islamic Militant Groups in Africa
Figure 15-3 Africa -Population Distribution
Figure 15-4 Africa: Primary Resources
Chapter 16: Chinese Drones in Spratly Islands, and Chinese Threats to USA forces in Pacific

Figure 16-1 Spratly Islands
Figure 16-2 Spratly Islands
Figure 16-3 Chinese Dove Drone
Figure 16-4 S-100 Drone Trajectories in Spratly Islands
Figure 16-5 S-100 Chinese Drone
Figure 16-6 ASN-209 Chinese Drone
Figure 16-7 BZK -005 Chinese Drone
Figure 16-8 GJ-1 Chinese UCAV Drone (Armed)
Figure 16-9 GJ-1 Chinese UCAV Drone (Armed)
Figure 16-10 Chinese UAS Chinese Intelligence Assets Deployment in Spratlys
Figure 16-11 GPS Signals
Figure 16-12 CPA Algorithm
Figure 16-13 CPA Algorithm Details
## TABLE OF TABLES

**Chapter 3: Understanding Hostile Use and Cyber-Vulnerabilities of UAS: Components, Autonomy vs. Automation, Sensors, SAA, SCADA and Cyber Attack Taxonomy**

Table 3-1 UAS Automation Scale  
Table 3-2 UAS Collaboration  
Table 3-3 Commercial sUAS Parameters  
Table 3-4 Typical Sensor Coordinate Systems  
Table 3-5 Standard Sensor Parameters  
Table 3-6 Common components found in UAS autopilots  
Table 3-7 SAA Systems Include (Smart Skies Project)  
Table 3-8 SCADA  
Table 3-9 SCADA Functions  
Table 3-10 Examples of SCADA Design Vulnerabilities  
Table 3-11 Common Attack Vectors

**Chapter 4: INFOSEC – Protecting UAS Information Channels & Components**

Table 4-1 Policy and Security Attributes  
Table 4-2 Information Security Parameters and Process

**Chapter 7: UAS SAA Methodologies, Conflict Detection & Resolution Principles**

Table 7-1 2007 Listing Remote Sensing Use of EMS  
Table 7-2 Common Wavelengths units for Electromagnetic Radiation

**Chapter 8: Designing UAS Systems for Stealth**

Table 8-1 Battlespace Dimensions

**Chapter 10: UAS Intelligence, Surveillance and Reconnaissance (ISR)**

Table 10-1 ISR Platform Tradeoffs  
Table 10-2 Surface, map shape, and flight altitude

**Chapter 11: UAS Weapons**

Table 11-1 Future Weapons

**Chapter 12: UAS System Deployment and Information Dominance (ID)**

Table 12-1 General Technology Categories for Information Warfare  
Table 12-2 Extracted Information Infrastructure Row from Waltz Attack Categories
Chapter 13: Data Links Functions, Attributes and Latency

Table 13-1 Standard Definitions of Radio Spectrum Segments
Table 13-2 shows the RF band designations

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

Table 14-1 Types of Jamming
Table 14-2 Tri-band Anti Drone Rifle KWT-FZQ/DG10-A
### TABLE OF EQUATIONS

**Chapter 3: Understanding Hostile Use and Cyber-Vulnerabilities of UAS: Components, Autonomy vs. Automation, Sensors, SAA, SCADA and Cyber Attack Taxonomy**

Eq. 3-1 Qualitative Information Systems Risk as a Function of Threats, Vulnerabilities, Impact, and Countermeasures

Eq. 3-2 Qualitative Information Systems Risk as a Function of Threats and Countermeasures at State = 0

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

Equation 14-1 Formula for communication J/S

Equation 14-2 Simplified J/S communications

Equation 14-3 Amount of jammer power output required

Equation 14-4 Radar Range Equation