DISRUPTIVE TECHNOLOGIES WITH APPLICATIONS IN AIRLINE & MARINE AND DEFENSE INDUSTRIES

DISRUPTIVE TECHNOLOGIES WITH APPLICATIONS IN AIRLINE & MARINE AND DEFENSE INDUSTRIES

BART SHIELDS; CANDICE CARTER; HANS C MUMM; JOHN PAUL HOOD; MARK JACKSON; PROFESSOR RANDALL K. NICHOLS; RANDALL MAI; SUZANNE SINCAVAGE; AND W.D. LONSTEIN

NEW PRAIRIE PRESS
MANHATTAN, KS

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

Contents

Part I. Main Body

Title Page

A PDF version of this book is available at
[https://www.newprairiepress.org/ebooks/38/]

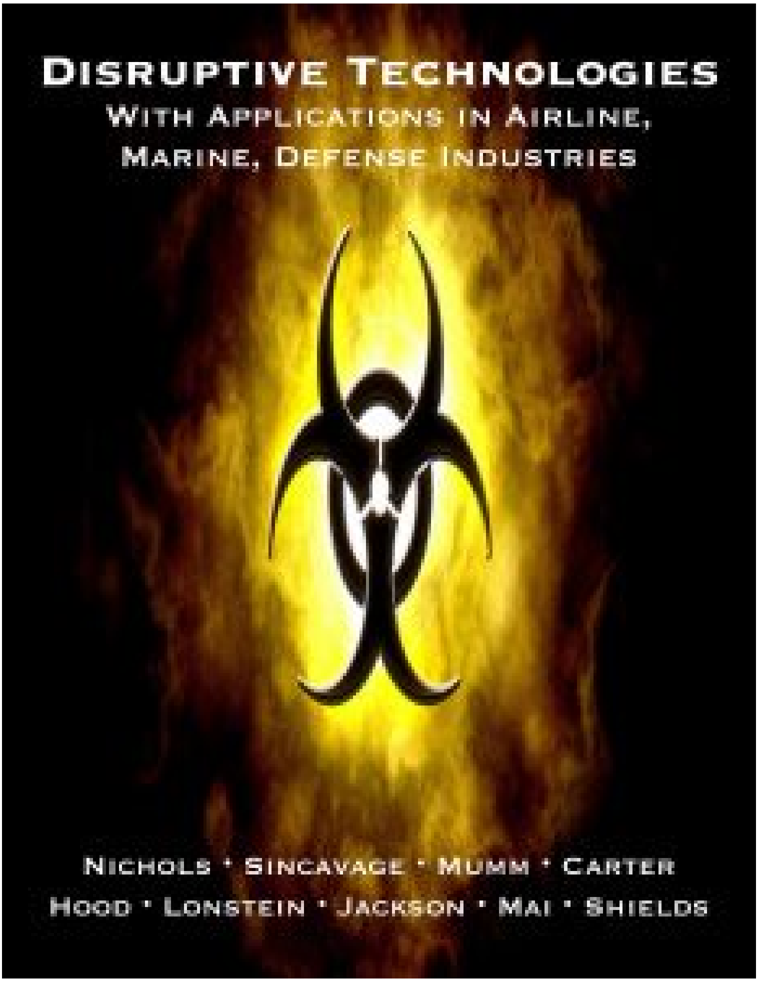
Cover design by R.K. Nichols and Kira Miller
Cover image: **Gauging the Risk From Bioterrorism**

Courtesy of Texas National Security Review – War on The Rocks (Mauroni, 2014)

New Prairie Press
Kansas State University Libraries
Manhattan, Kansas

Pressbooks ISBN: 978-1-944548-34-6

Cover Art



Disruptive Technologies
With Applications in Airline,
Marine, Defense Industries

Nichols • Sincavage • Mumm • Carter
Hood • Lonstein • Jackson • Mai • Shields

References

Mauroni, A. (2014, January 6). *Gauging the Risk of Bioterrorism.*

Retrieved from warontherocks.com/: https://warontherocks.com/2014/01/gauging-the-risk-from-bioterrorism/ >

Copyright and Publication Page

A PDF version of this book is available at
[https://www.newprairiepress.org/ebooks/38/]
Cover design by R.K. Nichols and Kira Nichols
Cover image: *Gauging the Risk from Bioterrorism* (Mauroni, 2014)
Courtesy of Texas National Security Review
New Prairie Press
Kansas State University Libraries
Manhattan, Kansas
Pressbooks ISBN: 978-1-944548-34-6

Books also by Professor Randall K. Nichols

Nichols, Randall K.; Mumm, Hans. C.; Lonstein, Wayne D.; Ryan, Julie J.C.H; Carter, Candice M.; Hood, John-Paul; Shay, Jeremy S.; Mai, Randall W.; and Jackson, Mark J., ***Unmanned Vehicle Systems & Operations on Air, Sea, Land*** (2020) Copyright 2020-2021, All Rights Reserved . NPP eBooks. 35. https://newprairiepress.org/ebooks/35/

Nichols, Randall K.; Mumm, Hans C.; Lonstein, Wayne D.; Ryan, Julie J.C.H; Carter, Candice; and Hood, John-Paul, **Counter *Unmanned Aircraft Systems Technologies, and Operations*** (2020). Copyright 2019-2021, All Rights Reserved, NPP eBooks. 31. https://newprairiepress.org/ebooks/31/

R.K. Nichols, J.J.C.H. Ryan, H.C. Mumm, C. Carter, W.D. Lonstein, J.P. Hood, (2019) ***Unmanned Aircraft Systems in the Cyber Domain Protecting USA's Advanced Air Assets*,** 2nd Ed. 26 July 2019, Copyright 2019-2021, All Rights Reserved, Manhattan: New Prairie Press (NPP eBooks 31). ISBN:978-1-944548-15-5. https://newprairiepress.org/ebooks/27

R.K. Nichols, J.J.C.H. Ryan, H.C. Mumm, C. Carter, W.D. Lonstein. (2018) ***Unmanned Aircraft Systems (UAS) in the Cyber Domain: Protecting USA's Advanced Air Assets***, 14 September 2018, Copyright 2018-2021, All Rights Reserved, Manhattan: New Prairie Press (NPP eBooks 21). ISBN:978-1-944548-14-8. https://newprairiepress.org/ebooks/21

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

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

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

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

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

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

Dedications

From: Professor Randall K. Nichols

I dedicate this book to three groups: **All USA serving and retired military personnel**, USA Coast Guard, and federal and state law enforcement for keeping our blessed country safe; to my Angel wife of 37 years, Montine, and children Robin, Kent, Phillip (USA Army), Diana (USA Army), and Michelle who have lived with a Dragon and survived; to the newest family member Kira Nichols (Phillip's wife); and finally, to all my students (over 50 years ~10,000 Dragons / Dragonesses in the field) who are securing our blessed United States from terrorism and evil. Lastly, to my wonderful, talented writing team, my deepest gratitude. It has been a true Honor.

From: Dr. Suzanne Sincavage

I would like to dedicate this book to: My beloved Joseph D. Duffie for giving me his legacy and intelligence for all things Unmanned. To Randall Nichols for his leadership, mentorship, and opening the door for all things possible. Words cannot be expressed in one paragraph that addresses my gratitude in believing in me. I'm so grateful to you for this opportunity. To Candice Carter, a true colleague, friend, researcher and patriot for uncovering all the unknown unknowns to protect our country and her special abilities to put our "outside the sphere" thoughts to paper. Your support has been invaluable. To Dr. Steve Herrick, "A Coach for Life" who intersected the time and space in my life to make this research possible.

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 who continue to support me through this journey. Thank you for your love, encouragement, and presence in my life.

From Mark J. Jackson:

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

From Randall W. Mai:

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

From Bart Shields:

I dedicate this book to my five children, Kyle, Tiffany, Taylor, Terra, and Marysia, as well as my wife, Hanna, and my mother, Pam, for allowing me to pursue my dreams and the sacrifice they all made as a consequence of that. They are all incredibly important to me and I hope they all know that. I could not have done any of this without them. It has been long, difficult, and unfortunately, I am still in transition, but thankfully, it will be coming to a close soon.

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 (Managing editor / Publisher), the U.S Army, U.S. Air Force, U.S. Navy, the Department of Defense, Kansas State University, nor any of its authors guarantees the accuracy or completeness of the information published herein and neither any of the above mentioned parties nor its authors shall be responsible for any errors, omissions, or damages arising out of use of this information.

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

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

Foreword

By
Julie JCH Ryan, D.SC.
CEO, Wyndrose Technical Group

It cannot be denied: the inventions and uses of technologies over the long eons of human existence have both improved and disrupted our existence. Cooking food improved the efficiency of caloric intake, freeing up time and energy for other pursuits (Wrangham, 2009). Mastering symbolic representation by painting on the walls of caves enabled the capture and transfer of intellectual capital (Mthen, 2006). Over the centuries, curious inventors have improved, replaced, and combined technologies in ways that have radically altered the way we interact with and live in the world. With each step forward, it may seem like only small bits of progress are being made. It is only when one sits back and considers where we are, and what technologies are rapidly being integrated into our living experience, that the magnitude of disruption becomes apparent.

With the publication of this book, *Disruptive Technologies With Applications In Airline, Marine, Defense Industries*, the writing team assembled by Professor Randall K. Nichols takes a hard look at the autonomous technologies that are being incorporated into the dimensions of air, land, and sea, the potential disruptive effects of those technologies, and the implications to societal norms and rules. While this book is primarily intended to be a textbook, it should be of interest to anyone who needs to understand the changes that are being unleashed by the revolutions in size, capability, and diversity of autonomous vehicles. The authors come from an extremely diverse background, ranging from law to science, and bring a wealth of experience, knowledge, and opinion. Why are these important? Knowledge is the fundamental understanding of something, experience is a sophisticated appreciation of real world impacts, and opinion is the application of experience to knowledge with a view to the future.

Foretelling the future — what will happen — is an interesting problem: the only thing the forecaster can possibly know is that they will be wrong about the forecast. The question is how wrong. Forecasts are important and useful even though they will get aspects wrong. Good and lucky forecasts get only minor details wrong while other forecasts can be subverted through sloppy analysis or simply bad luck. But every forecast brings useful information to the table. Thinking about what could potentially happen in the future informs our ability to make choices. These choices could include policies to make a potential future more likely, or they could include policies to keep a potential future from happening. Understanding and thinking about disruptive technologies and what futures they can possibly bring about is important for students, educators, and leaders in every field. This book provides an underpinning for that type of analysis by bringing together the diversity of topics in one sweeping consideration of technological development.

The future is upon us. We simply need to understand the implications.

Julie JCH Ryan, D.SC.
CEO, Wyndrose Technical Group

References

Mthen, S. (2006). *After the Ice: A Global Human History*, 20,000–5000 BC. Harvard University Press.

Wrangham, R. (2009). *Catching Fire: How Cooking Made Us Human*. Basic Books.

Preface

Disruptive Technologies With Applications in Airline, Marine, Defense Industries is our fifth textbook in a series covering the world of Unmanned Vehicle Systems & Operations On Air, Sea, Land; Counter Unmanned Aircraft Systems Technologies and Operations; Unmanned Aircraft Systems in the Cyber Domain: Protecting USA's Advanced Air Assets, 2nd edition; and Unmanned Aircraft Systems (UAS) in the Cyber Domain Protecting USA's Advanced Air Assets, 1st edition; have seen considerable global recognition in the field. (Nichols R. K., et al., 2020) (Nichols R. , et al., 2020) (Nichols R. , et al., 2019) (Nichols R. K., 2018)

The authors have expanded their purview beyond UAS / CUAS / UUV systems we have written extensively about in our previous four books. Our new title shows our concern for the emergence of *Disruptive Technologies and how they apply to the Airline, Marine and Defense industries.*

There is a difference between emerging technology trends and disruptive ones. *Emerging technologies* are technologies whose development, practical applications, or both are still largely unrealized, such that they are figuratively emerging into prominence from a background of nonexistence or obscurity. (Wiki, 2021) Some sources say that emerging technologies are taking over the world by a storm and if misused, it could turn out to be our worst enemy. (Rose, 2019) Toward Data Science magazine lists Drone Swarms as number one in their list. The topic covered in detail in (Nichols R. , et al., 2020). Smart home devices that spy, ex. IoT or AI / IoT is number two, followed by facial recognition, spy dust and autonomous robots. (Rose, 2019)

A D*isruptive technology* is one that displaces an established technology and shakes up the industry or a ground-breaking product that creates a completely new industry. (Rouse, 2021)

That is what our book is about. We think we have found technology trends that will replace the status quo or disrupt the conventional technology paradigms.

We have written some explosive chapters in Book 5. Dr. Hans Mumm has written about the advances in Automation & Human Machine Interface. Wayne Lonstein, JD has given the reader a solid look at Social Media as a Battleground in Information Warfare (IW). CEO Bart Shields has delivered a viable, less risky, more robust cyber-security alterative / replacement for the popular Blockchain Algorithm and a clean solution for Ransomware. Professor Randall Nichols has written about the advanced sensor technologies that are used by UUVs for munitions characterization, assessment, and classification. He reports on their counter hostile use of UUVs against US capital assets in the South China Seas. In a second chapter, Professor Nichols has challenged the status quo and debunked the climate change fraud with verifiable facts. In his third chapter, he explodes our minds with nightmare technologies that if they come to fruition may do more harm than good. Some of them might reach Black Swan event status. [1]

Dr. Mark Jackson has written authoritatively about Propulsion and Fuels: Disruptive Technologies for Submersible Craft Including UUVs. CEO Randall Mai has penned a chapter to challenge the ammunition industry by grassroots use of recycled metals and an alternative propellant – air. Captain John – Paul Hood writes about the changing landscape of UAS regulations and privacy. 2021 will prove to be challenging for owners and manufacturers of UAS. CEO & Dr. Suzanne Sincavage and Professor Candice Carter have teamed up to scare the pants off of us – especially during the COVID-19 pandemic – by detailing Bioterrorism Risks, Biodefense, Biological Threat Agents, and the need for advanced sensors to detect these attacks.

Over two years of solid research by a team of nine SMEs is incorporated into our book. We trust you will enjoy reading it as much as we have in its writing.

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

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

References

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., Ryan, J., Mumm, H., Lonstein, W., Carter, C., Hood, J., . . . & Jackson, M. (2020). *Unmanned Vehicle Systems & Operations on Air, Sea, Land.* Manhattan, KS: New Prairie Press #35.

Nichols, R. K., Sincavage, S., Mumm, H., Lonstein, W., Carter, C., Hood, J., . . . & Shields, B. (2021). *Disruptive Technologies With Applications In Airline, Marine, Defense Industries.* Manhattan, KS: New Prairie Press, #TBA.

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

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

Rose, S. (2019, December 24). *5-horrifying-emerging-technology-trends-that-will-shake-you.* Retrieved from towardsdatascience.com: https://towardsdatascience.com/5-horrifying-emerging-technology-trends-that-will-shake-you-c7150c1f7eac

Rouse, M. (2021, January 4). *disruptive technology.* Retrieved from whatis.com: https://whatis.techtarget.com/definition/disruptive-technology

Scott, G. (2021, January 4). *Black Swan Event.* Retrieved from www.investopedia.com: https://www.investopedia.com/terms/b/blackswan.asp#:~:text=A%20black%20swan%20is%20an,they%20were%20obvious%20in%20hindsight.

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

Wiki. (2021, January 4). *Emerging_technologies definition.* Retrieved from https://en.wikipedia.org/wiki/Emerging_technologies#: https://en.wikipedia.org/wiki/Emerging_technologies#:~:text=Emerging%20technologies%20are%20technologies%20whose,background%20of%20nonexistence%20or%20obscurity.

[1] A Black Swan is an unpredictable event that is beyond what is normally expected of a situation and has potentially severe consequences. Black swan events are characterized by their extreme rarity, severe impact, and the widespread insistence they were obvious in hindsight. (Scott, 2021)

Acknowledgements

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

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

Shappee, Director, KSUP Library; Beth Drescher, Grant Specialist KSUP; Charlene Simser, prior Professor and Coordinator of Electronic Publishing at New Prairie Press and Pressbooks,[my mentor in the publishing gig]; Dr. Emily Finch and Ryan Otto at NPP; Chad Bailey, Instructor SIS KSUP, Aris Theocharis, our terrific editor; and especially Joel Anderson, KSU OVPR and Research Director.

We had some wonderful outside SMEs to bounce ideas off and get our heads straight. They include Dr. Donald Rebovich, Professor Emeritus and SME in Fraud and Identity Theft; Professor of Practice and Cybersecurity Director, Joe Giordano, Utica College; Professor Harold B. Massey, Executive Director of UAS Drone Port, UAS Pilot and Dr Amit K Maitra, Chairman and Founder of Borders and Beyond, Inc.; Dr. Bartosz Wojszczyk, President and CEO Decision Point Global; and Dr. Jeff Bardin, President of Treadstone 71, a superior intelligence firm.

We owe a special thank you for the permissions and expertise of Gregory Wrightstone, author of *Inconvenient Facts: The Science that Al Gore doesn't want you to know*. (Wrightstone, 2017) Chapter 7 drew heavily on its facts and wisdom as a counterpoint to thew views of Pierre Coutu's *Global Megatrends and Aviation the Path to Future-Wise Organizations*. (Coutu, 2019)

Next comes our expanded writing team: Dr Suzanne Sincavage, Executive Director for the Institute for Biodefense Research (IBR). IBR is a nonprofit devoted to advancing the science of microbial forensics; Dr Julie J. C. H. Ryan, CEO, Wyndrose Technical Group, is hands down the best subject matter expert (SME) in the Information Security field. Dr. Hans C. Mumm is an expert in leadership and UAS weapons – a lethal combination. Dr. Wayne C. Lonstein, Esq., a previous Dragon (Nichols' student) has gained recognition (licenses and certifications) in both law and cybersecurity as well as heads up his own legal firm. Professor Candice C. Carter, a Dragoness who is the creator of a cybersecurity program at Wilmington University and travels globally closing specialized cybersecurity breaches in major corporations. Capt. John Paul Hood, US Army, (our military adviser and previous Dragon) joined us to help us understand the intricacies of military C-UAS (non-classified) applications. Randall Mai, Research Technologist for KSU, a Dragon convert, with years of experience in UAS filed operations; Dr Mark Jackson, SME in UUV, naval architecture, and nanotechnologies, Sgt Jeremy Shay, Dragon student, COVID-19 expert, RET USAF, Fabrication Production Manager, Spirit AeroSystems; Joel Coulter, President, Mobile Sciences Consortium, LLC; and Bart Shields, Inventor and CTO of Olympus Sky, Inc. Special shoutout to NSWC PCD and Robert Leasko, PI for the NSWC PVD 2011 Demonstration and Report on UUVs and MCM Sensors.

Last, Professor Randall K. Nichols is managing editor / author / co-author of ten prior books and developer of six Masters and Certificate programs in Cybersecurity at Utica College and Kansas State University. He has five decades of Cybersecurity experience.

Finally, Montine Nichols deserves a commendation for her help on the final drafts and copy edit work for our book (and living with a real Dragon). Several KSUP UAS pilot – students helped with the "student view," and made valid suggestions for improvement, Vincent Salerno, Senior Airman in Kansas Air National Guard, John Boesen, (our handwriting expert); Diana K. Nichols, UAS Pilot; Josh Jacobs, Jorge Silva, Sr. UAS Safety Engineer, and Jordan McDonald. Special thanks go Kira C. Miller who professionally developed (more like "nailed") our cover art.[1]

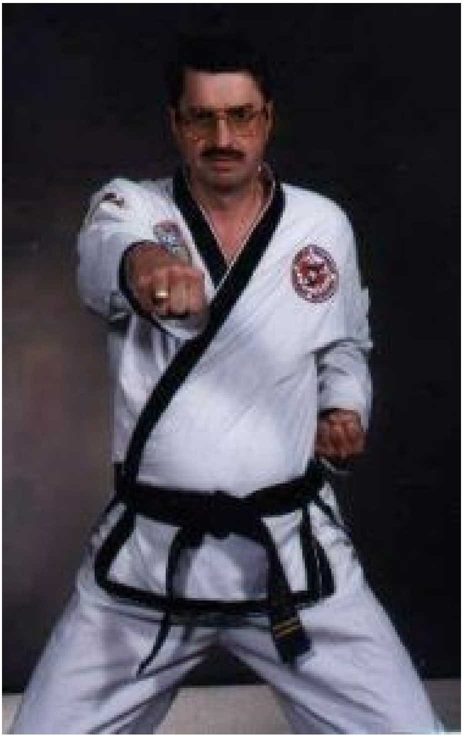
The team especially thanks Assistant Professors Ryan W. Otto, and Emily Finch Scholarly Communication Librarians, for their expert assistance with the NPP final efforts.

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

[1] Kira on October 27, 2020 will be Kira Nichols, marrying my youngest son.

List of Contributors

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



Randall K. Nichols is Professor of Practice in Unmanned Aircraft Systems (UAS) – Cybersecurity at Kansas State University Polytechnic (KSUP) in Salina, Kansas. Nichols serves as Director, graduate UAS- Cybersecurity Certificate program at KSUP. Nichols is internationally respected, with 50 years of experience in leadership roles in cryptography, counterintelligence, INFOSEC, and sensitive computer applications. Throughout his career, Nichols has published *ten* 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 Counterterrorism, Counterespionage, and Information Security Countermeasures to support its 1700 commercial, educational and U.S. government clients.

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

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

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

This is Professor Nichols eleventh published book. ***Disruptive Technologieswith Applications in Airline, Marine, Defense*** **is Nichols' 5th textbook as managing editor / contributor in the series on UAS /CUAS / UUV / special technologies all published by New Prairie Press. Others include:**

Unmanned Vehicle Systems & Operations on Air, Sea, Land
New Prairie Press (published on October 2, 2020)
Available as free eBook at: https://www.newprairiepress.org/ebooks/35/

Counter Unmanned Aircraft Systems Technologies and Operations
New Prairie Press (published on February 1, 2020)
Available as free eBook at: https://www.newprairiepress.org/ebooks/31/

Unmanned Aircraft Systems (UAS) in Cyber Domain: Protecting USA's Advanced Air Assets,
New Prairie Press (*NPP 2nd Edition* published on July 26, 2019)
Available as free eBook at: https://www.newprairiepress.org/ebooks/27

Areas of Expertise / Research Interests

- Counterterrorism / Counter- Intelligence /Counterespionage / Computer Security
- Countermeasures Asymmetric Warfare and Attack / Defense Scenarios against National Critical Infrastructure
- Computer Forensics and Cryptography SME & Federal Expert Witness (Federal Criminal Cases: Treason / Espionage)
- Risk Assessment / Threat Analysis / Vulnerabilities Analysis / Countermeasures
- Cybersecurity / Surveillance Technologies: Aerial, Infrared, Visual, Ultraviolet, Radio, Radar & Sonar
- SCADA – Advanced Cyber-weapons Creation / Deployment /

Deployment / Defense

- UAS- Integrating Unmanned Aircraft Systems into National Airspace System
- Designing Acoustic Countermeasures against hostile -actor UAS SWARMS & developing dual purpose IFF sound libraries.

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

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

Dr. Hans C. Mumm (Co-Author)

Dr. Hans C. Mumm holds a Doctor of Management with a concentration in Homeland Security from Colorado Technical University (CTU) and an MS in Strategic Intelligence from American Military University (AMU). He gained notoriety during Operation Iraqi Freedom as the officer in charge of the “Iraqi Regime Playing Cards; CENTCOM’S Top 55 Most Wanted List” which was touted by the Defense Intelligence Agency (DIA) as one the most successful

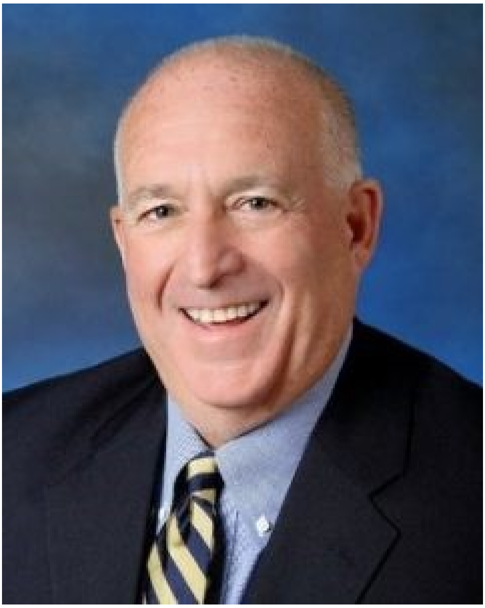
Information Operations (IO) in the history of Defense Intelligence Agency (DIA). Dr. Mumm is the former Division Chief for Cyber Security at the Office of The Director of National Intelligence (ODNI) programming and executing a budget of over $140M. Dr. Mumm has earned twenty-three personal military ribbons/medals including six military unit medals/citations, and two Directors Awards, from the DIA. In 2016 he was awarded the People of Distinction Humanitarian Award as well as being granted a US Patent and Trademark for How to Harmonize the Speed of Innovation and Change with the Human Spirit's Need for Leadership. In 2005, Dr. Mumm was recognized as one of the "Ten Outstanding Young Americans," and in 2003 he was awarded the National Defense PAC "American Patriot Ingenuity Award" for his service during "Operation Iraqi Freedom."

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

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

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

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



Wayne Lonstein holds a Bachelor of Arts Degree in Political Science from Wilkes University, a Bachelor of Science Degree in Cyber Forensics and Information Security from Syracuse University – Utica Collage, A Master of Science Degree in Homeland Security with a concentration in Information Security from The Pennsylvania State University and a Juris Doctor Degree from Pace University School of Law. Additionally, he holds a CISSP Certification from The Pennsylvania State University. He is a member of the state bars of New York, New Jersey, Massachusetts, and Pennsylvania as well as being admitted to over 30 United States District Court Bars, The Court of Veterans Appeals, United States Tax Court and the bar of the United States Court of Appeals of the 2nd, 3rd, and 5th Circuits.

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

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

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

Dr. Julie J.C.H. Ryan, D.Sc. (Co-Author Books 1-4 in Series)/ Foreword Disruptive Technologies Book 5)

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

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

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

Professor Candice M. Carter (Co-Author)

Ms. Candice Carter is a cybersecurity expert with over 15 years of hands-on experience in the areas of counterterrorism, counterintelligence, and criminal cyber investigations. She conducts Classified/Unclassified briefings in the areas of Terroristic Cyber Capabilities using Social Media and Counterterrorism for the Intelligence Community (IC). Ms. Carter conducts research and constructs Asymmetric Warfare and Attack / Defense Scenarios against National Critical Infrastructure. She is the Team Lead and for NASA Aeronautics Research Institute for *Transformative Vertical Flight (TVF) Commercial Intra-City On-Demand* VTOL group. Ms. Carter is an invited speaker for key organizations including BSides London and (ISC)2 Security Congress. She is an Assistant Professor/Chair MSc Cybersecurity program at the Wilmington University. Ms. Carter holds a MSc Cybersecurity Forensics and Intelligence from Utica College, Utica , NY and a PMT Cybersecurity UAS from Kansas State University.

Aris Theocharis (Co-Editor)

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

Kurt Barnhart, Ph.D. (Associate Dean & Foreword to 1st Edition)

Dr. Barnhart is Professor and currently the Associate Dean of

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

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

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

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

CPT John-Paul Hood USA (Co-Author)

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

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

Dr. Starkey is a Professor and currently serves as the CEO and Dean for the Kansas State University Polytechnic Campus. As Dean, she oversees the College of Technology and Aviation academic programs and campus research centers. Dr. Starkey holds an A.A. in Social Work from Colby Community College, a B.S. in Psychology from Fort Hays State University, a M.L.S. from University of North Texas, and a Ph.D. in Curriculum and Instruction from Kansas State University. Joining Kansas State Polytechnic in June 2002 as a technical services/automation coordinator and assistant professor, Starkey was promoted to library director and associate professor in 2007, and to assistant dean of continuous improvement and distance education in 2010. She was named associate dean of academics and promoted to full professor in 2014. She gained the additional duties of interim CEO and Dean in June 2018 and continues in that capacity today.

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

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

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

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

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

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

Dr. Mark J. Jackson (Co-Author)

Doctor Mark James Jackson is the McCune and Middlekauff Endowed Professor and University Faculty Fellow at Kansas State University. Born in Widnes, Lancashire, England, in 1967, Doctor Jackson began his engineering career in 1983 when he studied O.N.C. part I examinations and first-year apprenticeship-training course in mechanical engineering. After gaining an Ordinary National Diploma in Engineering with distinctions and I.C.I. prize for achievement, he studied a degree in mechanical and manufacturing engineering at Liverpool Polytechnic and spent periods in industry working for I.C.I. Pharmaceuticals, Unilever Industries, Anglo Blackwells, Unicorn International and Saint-Gobain Corporation. After graduating with the Master of Engineering (M. Eng.) degree with Distinction under the supervision of Professor Jack Schofield, M.B.E., Doctor Jackson subsequently conducted research for the Doctor of Philosophy (Ph. D.) degree at Liverpool in the field of materials engineering focusing primarily on microstructure-property relationships in vitreous-bonded abrasive materials under the supervision of Professors Benjamin Mills and H. Peter Jost, C.B.E., Hon. F.R.Eng.. He was subsequently employed by Unicorn Abrasives' Central Research & Development Laboratory (Saint-Gobain Abrasives' Group) as materials technologist, then technical manager, responsible for product and new business development in Europe, and university liaison projects concerned with abrasive process development. Doctor Jackson then became research fellow at the Cavendish Laboratory, University of Cambridge, working with Professor John Field, O.B.E., F.R.S., and Professor David Tabor, F.R.S., on condensed matter physics and tribology before becoming a lecturer in engineering at the University of Liverpool in 1998. At Liverpool, he attracted a number of research grants concerned with developing innovative manufacturing processes for which he was jointly awarded an Innovative Manufacturing Technology Centre from the Engineering and Physical Sciences Research Council in November 2001. In 2002, he became associate professor of mechanical engineering and faculty associate in the Centre for Manufacturing Research, Centre for Electric Power, and Centre for Water Resources and Utilization at Tennessee Technological University (an associated university of Oak Ridge National Laboratory), and a faculty associate at Oak Ridge National Laboratory. Dr. Jackson was the academic adviser to the Formula SAE Team at Tennessee Technological University. At Tennessee Technological University, Dr. Jackson established the NSF Geometric Design and Manufacturing Integration Laboratory. Dr. Jackson collaborated with Nobel Laureate Professor Sir Harold Kroto, F.R.S., editing a book on 'Surface Engineering of Surgical Tools and Medical Devices' and a special issue of the International Journal of Nanomanufacturing on 'Nanofabrication of Novel Carbon Nanostructures and Nanocomposite Films'. Dr. Jackson was appointed member of the United Nations Education, Scientific and Cultural Organization's (UNESCO) International Commission for the Development of the 'Encyclopedia of Life Support Systems' Theme on 'Nanoscience and Nanotechnologies', (http://m-press.ru/English/nano/index.html), and still serves in this capacity. The first edition of the encyclopedia was published 2009 and second edition published 2018. In March 2017, the degree of Doctor of Science (D. Sc.) in mechanical engineering was conferred upon Dr. Jackson in absentia by congregation for sustained contributions made in the area of mechanical engineering and advanced manufacturing over a period of twenty years.

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

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

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

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

Kurt J. Carraway, Col, USAF (Ret) [Foreword to Book 4]

After serving 25 years with the United States Air Force, retired Colonel Kurt J. Carraway is the Unmanned Aircraft Systems (UAS) Department Head and Executive Director of the Applied Aviation Research Center (AARC) at Kansas State University's Polytechnic Campus. As Department Head, Carraway leads UAS faculty in the university's UAS program, which includes a Bachelor of Science in Aviation Technology program, a UAS Minor and a UAS Certificate program. He also serves as a member of the graduate faculty on the campus. As Executive Director, Carraway provides strategic leadership in advancing Kansas State University's UAS program goals. He directs the execution of research activities involving UAS through the AARC. Carraway also directs flight operations development and maturation of the UAS training program through direct supervision of the Flight Operations staff. He manages highly skilled UAS professionals that perform hundreds of UAS flights per year in civil airspace. He sets policies and procedures for unmanned flight operations. He serves as Principal Investigator (PI) on UAS activities through the AARC and is the University PI representative to ASSURE, the FAA's UAS Center of Excellence.

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

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

Bart Shields (Co-Author)

Bart Shields, BS in Computer Science-Scientific Option, MS in Computer Science-Thesis Option, Chief Technology Officer, Inventor, Co-founder

Bart Shields is serial entrepreneur, long-time innovator, deeply technical product architect, with over 25+ years of technical and engineering management. He has designed systems from concept to deployment for a wide variety of verticals, but has focused mainly on data communication, with multiple wireless communication products to his credit ranging from commercial wireless broadband routers to tactical radios for the U.S. government.

Bart is a highly innovative, technology expert, having created designed multiple MAC layer protocols, including the design and implementation of a Wi-Max like protocol (WCOPP) in the late 90's and more recently, a Sensor Node MESH network MAC based upon Distributed Queuing. Bart has five patents to his credit, two for Wireless MACs based on Distributed Queuing and three for his recent cybersecurity protocol and cryptographic key management system, Autonomous Key Management (AKM).

Bart has built multiple engineering teams and entire departments from scratch, and overseen all aspects of engineering, including fabless ASIC design, communication systems algorithm development, and RF transceiver design and development.

Bart is an expert in embedded development and has spent his entire career in the design and development of embedded systems, including both mission and safety critical systems. Bart has focused the past six years entirely on cybersecurity and solving many of issues plaguing security today, with simple and elegant solutions built around his highly innovative technology, AKM.

Dr. Suzanne Sincavage (Co-Author)

Executive Summary

On May 3rd , 2020 Dr Suzanne Sincavage was named Executive Director for the Institute for Biodefense Research (IBR). IBR is a nonprofit devoted to advancing the science of microbial forensics.

Dr Sincavage, a PhD in public health epidemiology, with a focus on biological terrorism preparedness and response, has led her own consultancy, IDIQ Inc. since 2008, focusing on CBRNE Subject Matter Expertise in facilitating and integrating innovative technologies that counter biological terrorism.

Dr Sincavage received her PhD in Public Health, Epidemiology with specialization in Biological Terrorism from Union Institute & University. Dr. Sincavage's career encompasses 16 years of experience in the biotechnology and pharmaceutical industry serving as a field scientist supporting R & D, medical and regulatory affairs, and commercial operations covering therapeutic areas of infectious disease, virology, oncology, hematology, urology, and immunology.

Dr Sincavage is SME for the National Reconnaissance Office (NRO), Intelligence and National Security Alliance (INSA) and DHS. She has held senior management positions in Watson Pharmaceuticals, Department of Medical & Regulatory Affairs; Wyeth-Ayerst Laboratories, G.D. Searle; Hoffman-La Roche Laboratories; Sacred Heart Medical Center and for fun the La Jolla Symphony & Chorus.

Dr Sincavage holds certifications:
SAM (CCR); SBA 8 (m)
DD 2345 Military Critical Technical Data Agreement
DTIC
DTIC STINFO Manager
Counterterrorism
InfraGuard – Infrastructure Liaison Officer
ONR – Counterterrorism

Committees:
NDIA Legislative Committee
NDIA National Small Business Conference
NRO ASP Industry Working Group
INSA Acquisition Management Council
USGIF Small Business Working Group
WOSB 8(m) Working Group, SPAWAR HQ, San Diego

Abbreviations and Acronyms

ABBREVIATIONS: ACRONYMS [REV 91A] 01232021 C1 – C10

The following terms are common to the UAS / UUV industries, defense / airline / marine industries / general literature, conferences on UAS/UAV/Drone/UUV systems and / or specific to Professor Nichols' five (5) textbooks in the series on UAS / drones / UAV / UUVs.

A-STAR	Heuristic search algorithm discussed in chapter 9.
A2 / AD	Anti-access / Area Denial
A /Aref	Amplitudes of source and reference points, see Eq-20-6,7.
AA	Anti-aircraft / Adaptive Antennas
AAA	Anti-aircraft artillery
AAIB	Air Accidents Investigation Board
AAM	Air-to-air missile
AAV	Autonomous air vehicle
ABI	Aviation Block Infrastructure
ABMS	Advanced battle management system
ABS	American Bureau of Shipping
A/C	Aircraft
ACAS	Airborne collision avoidance system / Assistant Chief of the Air Staff
ACL	Agent communication language / Autonomous control levels
ACOUSTIC	Detects drones by recognizing unique sounds produced by their motors.
ACRP	Airport Cooperative Research Project
ACS	Airbome (defense) control station (system)
ACTD	Advanced Concept Technology Demonstration
AD	Air Defense / Ansar Dine terrorist group.
A/D	Attack / Defense Scenario Analysis

ADAC	Automated Dynamic Airspace Controller
ADAPs	Adaptive compute acceleration platforms
ADC	Air data computer
ADCP	Acoustic Doppler Current Profiler
ADF	Automatic direction finder/finding.
ADMS	Air defense missile (radar) system
ADS	Air Defense System (USA)
ADS-B	Automatic Dependent Surveillance – Broadcast systems
ADT	Air Data Terminal
AE	Artificial Employee
AESA	Active electronically scanned array
AEW	Airbome early warning
AF	Adaptive Filtering
AFCS	Automatic flight control system
AFRICOM	US Africa Command
AGL	Above ground level
AGM	Air- to- surface missile
AGARD	Advisory Group for Aerospace Research and Development (NATO)
AGM-65	Maverick (USA) is an air-to-surface missile (AGM) designed for close air support. It is the most widely produced precision-guided missile in the Western world, and is effective against a wide range of tactical targets, including armor, air defenses, ships, ground transportation and fuel storage facilities.
AGV	Autonomous Guard Vehicle
AHA	Autopilot Hardware Attack
AHD	Analog high definition
AHRS	Attitude and heading reference system
AI	Artificial intelligence: “1. a branch of computer science dealing with the simulation of intelligent behavior in computers and 2: the capability of a machine to imitate intelligent human behavior.” (Merriam-Webster, 2020)

AIAA	American Institute of Aeronautics and Aerospace
AIC	Aeronautical Information Circular
AIP	Aeronautical Information Publication
AIS	Automated Identification System for Collision Avoidance
AJ	Anti-Jam
AKM	Autonomous Key Management
ALB	Air Land Battle
ALERT	Advanced Low-observable Embedded Reconnaissance Targeting system.
AM	Amplitude Modulation / al-Mourabitoun terrorist group
AMB	Agile Multi-Beam
AMRAAM	Advanced Medium-Range Air-to-Air Missile
ANSP	Air Navigation Service Provider
ANO	Air Navigation Order (UK)
AO	Area of Operations
AoA	Angle of Attack
APEC	Asia Pacific Economic Cooperation
APG	Asia-Pacific Gateway
APKWS	Advanced precision kill weapon system
AQ	Al-Qaida Terrorist Group – “the Base”
AOA	Aircraft operating authority
AQIM	al-Qaeda in the Islamic Maghreb
Ar	Receive antenna effective area, m2
AR	Aspect ratio
AR drone	AR stands for “Augmented Reality” in AR *drone*. AR *Drone* can perform tasks like object recognition and following, gesture following.
ARM	Anti-Radiation Munitions
ARS	Airborne Remote Sensing
ART	Autonomous Rail Transport
ARW	Anti-radiation weapons
AS	Airborne Sensing Systems
ASB	Advisory Service Bulletin / Air Sea Battle

ASBM	Anti-ship ballistic missile
ASCM	Anti-ship cruise missile
ASEA	Active electronically scanned arrays
ASEAN	Association of Southeastern Asian Nations
ASC	ALEXA /SIRI /CORTANA
ASICs	Application specific integrated Circuits & circuit boards
ASL	Airborne Systems Laboratory
ASMS	Automated Separation Management System
ASR	Chinese Air Silk Road
ASOS	Automated surface weather observation system
ASTM	American Society of Testing and Materials (ASTM)
ASTER	Agency for Science, Technology and Research
ASuW	Anti-surface unit warfare
ASW	Anti-submarine warfare
AT	Aerial target
ATC	Air Traffic Control
ATHENA	Lockheed Martin Advanced Test High Energy Asset
ATM	Air Traffic Management
ATN	Aids to Navigation (aka ATON)
ATR	Automatic Target Recognition
ATS	Air Traffic Service
AUDS	Anti-UAV Defense System
AUV	Autonomous Underwater Vehicle
Avionics	Aviation electronics in manned or unmanned aircraft
AUVSI	Association for Unmanned Vehicle Systems International
AV	Air Vehicle
AWB	Application White Boxing
AWOS	Automated weather observation system
AWSAS	All Weather Sense and Avoid System
B	IF equivalent bandwidth, Hz
Backhauling	Intermediate links between core network or internet backbone and small subnets at the edge of the network

BA Bacterial agent

BAMS Broad Area maritime surveillance

BATS Bermuda Atlantic Time-series Study

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

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

BDA Battle Damage assessment

BER Bit error rate

Black Swan Black Swan Event- A black swan is an unpredictable event that is beyond what is.

normally expected of a situation and has potentially severe consequences. Black

swan events are characterized by their extreme rarity, severe impact, and the

widespread insistence they were obvious in hindsight.

(Black Swan Definition, 2020)

BLOS Beyond line-of-sight

BMI Buried Mine Identification

BNF Bind and Fly – with custom transmitter.

BOSS Buried Object Scanning Sonar

BPAUV Battlespace preparation autonomous underwater vehicle

BRI Chinese Belt and Road Initiative

BR&T Boeing Research and Technology

BT Biological toxins

BTA Biological Threat Agent

BSR Bilinear Signal Representation

BSs Base Stations

BVR Beyond visual range

BW Biological weapons

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

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

C Combined methods of CR

C2 / C2W Command and control / Command and Control Warfare

C3I Command, control, communications, and Intelligence

C4 Command, control, communications, and computers

C4I Command, control, communications and computers, intelligence

C4ISR Command, control, communications, computers, intelligence, surveillance & reconnaissance

C4ISTAR Command, control, communications, computers, intelligence, surveillance, target

acquisition and reconnaissance

CA Collision Avoidance / Clear Acquisition (GPS) / *Cyber Assault (aka Cy*A)

C/A Civilian acquisition code for GPS

CAA Control Acquisition cyber attack

CAS Close Air Support / Common situational awareness

CASA Civil Aviation Safety Authority

CASIC China Aerospace Science and Industry Corporation

C of A Certificate of Airworthiness

CAP Civil Air Publication

CAT Collision Avoidance Threshold /Connectivity & automation in transport

CC / CyC Cyber Crime

CCCI/II Classical Cryptography Course Volume I/II (Nichols R. K., Classical Cryptography Course Volume I / II, 1996)

CCE Cyber Counter Espionage

CCI Command control interface / *Cyber Counterintelligence*

CCMCPS	Cooperative Cognitive Maritime Cyber Physical System
CCS	Cyber Counter Sabotage
CCT	Cyber Counter Terrorism
CC-UAS	Counter-Counter Unmanned Aircraft Systems
CD	Conflict Detection
CDL	Common datalink
CDMA	code division multiple access
CDN	Content Distribution Network
CDR	Collision detection and resolution systems (automated SAA in UAS)
CEA	Cyber electromagnetic activities (Cyber, EW, Spectrum warfare)
CEO	Chief Executive Officer
CETC	Chinese Electronics Technology Group
CF	Computer Forensics
CFTA	Continental Free Trade Area
CFT	Certificate of flight trials / Cross-functional teams
CHIMERA	Counter-electronic HPM Extended range base air defense
CI / CyI	Cyber Infiltration
CIA	Confidentiality, Integrity, Availability / Central Intelligence Agency
CIAD	Cyber- Multi-layered Integrated Air Defense Systems
CIED	Computer improvised explosive device.
CIN	Common Information Network
CIR	Color Infrared – artificial standard where NIR bands shifted so that humans can see the infrared reflectance.
CISA	Cybersecurity & Infrastructure Security Agency
CLE	Airport code for Cleveland
C/N	Carrier to Noise ratio in HAPS, => C/ N0
C/NA	Communication / Navigation Aid
CM / CyM	*Countermeasure* / Cyber Manipulation
CN3	Communications / navigation network node

CNI	Critical National Infrastructure
CNKI	China-North Korea-Iran technical weapons cooperation agreements
CNO	Chief Naval Operations
CNPC	Control and non-payload links
CO2	Carbon dioxide emissions
COA	Certificate of Waiver or Authorization
COB	Chief of the Boat
COMINT	Communications intelligence
COMJAM	Communications Jamming
COMSEC	Communications Security
CONOP(S)	Concepts of Operations
CONUS	Continental United States
COOP	Cooperative Observer Program
COS	Continued Operational Safety
COTS	Commercial off-the-shelf
CPA	Closest Point of Approach
CPA Spoof	CPA spoof involves faking a possible collision with a target ship.
CPL	Commercial pilot's license
CPNI	Center for Protection of National Infrastructure (UK)
CPRC	Communist Party of the Republic of China
CPS	Cyber-physical systems
CR	Conflict Resolution / Close range / Cyber Raid (aka CyR)
CRH	Coaxial rotor helicopter
CRX	Received Signal Power, watts
CS	Control station
CSDP	Common Security and Defense Policy missions (EU)
CSR	Compact Surveillance Radar
CSfC	Commercial Solutions for Classified Program
CSIRO	Commonwealth Scientific and Industrial Research Organization
CT	Counter Terrorism / Counter Terrorism Mission

CTOL	Conventional take-off and landing
C-UAS	Counter Unmanned Aircraft Systems (defenses / countermeasures)
CUAS	CSIRO Unmanned Aircraft Systems
CV	Collision Volume
CW / CyW	Cyber Warfare
D-STAR	Variation of A-STAR algorithm suitable for solving path planning problems in unknown environments
D	distance from transmitter in Range equation (Adamy D. -0., 2015)
DA	Danger area
Danger Close	
Definition	www.benning.army.mil/infantry/magazine/issues/2013/May-June/Myer.html Nov 14, 2013 – 1) danger close is included in the "method-of-engagement" line of a call-for-fire request to indicate that friendly forces are close to the target. … Danger close is a term that is exclusive from risk estimate distance (RED) although the RED for 0.1 percent PI is used to define danger close for aircraft delivery. Pi = Probability of incapacitation. 2) Definition of "danger close" (US DoD) In close air support, artillery, mortar, and naval gunfire support fires, it is the term included in the method of engagement segment of a call for fire which indicates that friendly forces are within close proximity of the target.
DARO	Defense Airborne Reconnaissance Office
DARPA	Defense Advanced Research Projects Agency
DAS	Detection by Acoustical Signature
dB	decibels
DC	Direct Current
DCL	Drone Champions League
DCPA	Distance between vessels approaching CPA.
DDD	Dull, dangerous, and dirty
DDOS	Distributed Denial of Service cyber attack
DE	Directed Energy

DEF CON DEF CON is the world’s longest running and largest underground hacking conference.

DE / EP Directed energy / Electromagnetic pulse.

DEM Digital elevation model

DEW Directed energy weapons.

DF Direction finding

DFCS Digital Flight Control System

DHS Department of Homeland Security

DIME Diplomatic, information, military, and economy

DIRCM Directed Infrared Countermeasures

DIY Do-it-yourself (amateur built drones or modified racing drones)

D j Jammer location – to-target receiver location distance, in km, FM 34-40-7

DJ Data Jamming / Drone Jammer

DJI Popular and functional Chinese made drone series: Mavic, Phantom, Ryze, Matrix, Spark, Enterprise, Inspire, Tello {However, banned by USA Army} (Newman, 2017)

DL Downlink in HAPS

DLA Date last accessed (usually a web reference)

DLI Datalink interface

DME di-methyl ether

DNA Deoxyribonucleic acid

DoD Department of Defense

DOF Degrees of Freedom

DOS Denial of Service cyber attack

DOT Department of Transportation

DPM Direct power management / Dynamic Power Management

DPRK Democratic People’s Republic of Korea

D-R-O-N-E FAA Guidance: Direct, Report, Observe, Notice &Execute

DROV Remote operating vehicle

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

DSR Chinese Digital Silk Road

DSS	Decision Support System
DSSS	Direct sequence spread spectrum.
D t	Enemy transmitter location -to- target receiver location, in km, FM 34-40-7
DT	Directional transmission / Department of Transport (UK)
DTDMA	Distributed Time Division Multiple Access (DTDMA) network radio system
DTED	Digital terrain evaluation data
DTF	Drug Task Force
DTH	Direct-To-Home
DTI	Direct Track & Identify
DTRA	Defense Threat Reduction Agency
DUO	Designated UAS operator
DVL	Doppler Velocity Log
EA	Electronic Attack
EARSC	European Association of Remote Sensing Companies
EAS	Equivalent airspeed
EAU	East Africa union comprising of Israel and six East African states, Kenya, Ethiopia, Tanzania, Uganda, Rwanda, and South Sudan
(Eb / No)	Thermal noise power spectral density ratio
ECCM / EP	Electronic counter-countermeasures / Electronic Protection
ECM	Electronic countermeasures
ECR	Electronic combat reconnaissance
EDC	Estimated Date of Completion
EDEW	Effects of Directed Energy Weapons
EEDI	Energy efficiency design index
EEZP	Exclusive economic Zone protection
EFF	Electronic Frontier Foundation
EHS	Enhanced surveillance
EIRP	Effective isotopic radiated power
Electrolaser	Electroshock weapon that is also a DEW. Uses lasers to form electrically conductive laser-induced plasma charge.

ELINT	Electronic Intelligence
ELT	Emergency locator transmitter
ECM	Electromagnetic compatibility
EM	Electromagnetic
EMC	Electromagnetic compatibility
EME	Electromagnetic environment
EMI	Electromagnetic interference
EMO	Electromagnetic operations
EMP	Electromagnetic pulse
EMR	Electromagnetic Radiation
EMS	Electromagnetic Spectrum
EMSVIS	Electromagnetic Spectrum Visible Light
EMW	Electromagnetic Waves
EO	Electro-optical (sensing) / Earth Observation
EOI	Electro-Optical Imager
EOTS	Electro-optical targeting system
EPIRB	Emergency Positioning -Indicating Radio Beacon
EQUAS	Explainable question answering system.
ERPJ	Effective radiated power of the jammer, in dBm
ERPS	Effective radiated power of the desired signal transmitter, in dBm
ESC	Electronic still camera
ESM / ES	Electronic support measures / Electronic warfare support / Earth station & ESM Electronic Signal Monitoring
EU	European Union
EUNAVFOR	European Union Naval Force's anti-piracy naval mission
EUTM	Somalia Military training mission in Somalia
EVTOL	Electric Vertical Take-off and Landing
EW	Electronic warfare, see 9-15 & footnotes.
F	Field theory methods of CR
F	F*undamental frequency* is defined as the lowest frequency of a periodic waveform
f	Frequency, cycles / second RRE)

Fo Resonant frequency of string, Hz see Eq. 20-5

F Frequency in MHz, FM 34-40-7

FAA Federal Aviation Administration

FACE Future Airborne Capability Environment

FAME Fatty acid methyl esters

FAR False Alarm Rates

FB Facebook©

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

FBW Fly-by-wire

FCC Federal Communications Commission

FCS Flight control systems / Flight Control Station

FDF Frequency Domain Filtering

FDM frequency division multiplexing

FHSS Frequency hopping spread spectrum.

FIIP Floating Integrated Information Platforms

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

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

FL Flight Level

FLIR Forward-looking infrared

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

Floats Floating sensors (USN)

FMS Flexible manufacturing system

Follow-Me UAS autopilot automatically follows operator.

Fom HAPS Figure of merit in upload /download link

FoV Field of view

FFOV Forward Field of View

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

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

FPGA Field programmable gate array

FS	Fixed service
FSS	Fixed satellite service
FW	Fixed wing
FY	Fiscal year
G	Geometric methods of CR
G5S	G5 Sahel (G5S) Joint Force, has membership of five states: Burkina Faso, Mali, Mauritania, Niger, and Chad
GAO	General Accounting Office USA
gAR	Receiving Antenna Gain as a Factor
GBU	Guided Bomb Unit
GCHQ	Government Communications Headquarters (Britain)
GCS	Ground control station
GDP	Gross Domestic Product (USA)
GDPR	European Union's (EU) General Data Protection Regulation
GDT	Ground data terminal
GENie	General Electric Network for Information Exchange
GEO	Geostationary Earth orbit satellite
GEOINT	Geospatial-Intelligence
GeoFence	A geo-fence is a virtual perimeter for a real-world geographic area
GIGO	Garbage in, garbage out
GLOW	Gross lift-off weight for a missile / rocket
GLONASS	Global Satellite Navigational System
GNL	Galveston National Laboratory
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
GSAA	Government Services Administration – audit division
GSE	Ground support equipment
GSHM	Ground Station Handover Method
GSM	Global System for Mobile Communications
GT	Game Theory methods of CR
G/T	ratio of the receive antenna gain to system noise temperature.
(G /Ts) dB	Represents the figure of merit of the HAPS receiver, in dB.
GT	Gain of the transmit antenna, dB.
GTA	Ground -to -Air Defense
Hard damage	DEW complete vaporization of a target
Harmonic	Frequency, which is an integer multiple of the fundamental frequency.
H	Elevation of the jammer location above sea level, feet, FM 34-40-7
HAE	High altitude endurance
HALE	High altitude – long endurance
HAPS	High Altitude Platforms (generally for wireless communications enhancements)
HAPS UAVs	UAVs dedicated to HAPS service (example to communicate via CNPC links)
HCE	Highly contested environment
HEAT	High-explosive anti-tank warhead
HELWS	High energy laser weapon system
HITL	Human in-the-loop
HMI	Human machine interface
HO	Home Office (UK)
HPA	High power amplifier
HPL	High powered laser weapon
HPM	High powered microwave defense
HSM	Hardware Security Module

H t Elevation of enemy transmitter location above sea level, in feet, FM 34-40-7

HUD Heads-up display

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

Humanoids "a humanoid being: a nonhuman creature or being with characteristics (such as the ability to walk upright) resembling those of a human."

HUMINT Human intelligence (spy's)

HVT High value target (generally, for assassination)

I Sound intensity, W x m-2 [Source strength S / 4πr2] (Uni-Wuppertal, 2019)

IA *Information Assurance* / Intentional cyber warfare attack

I-actors Intentional Cyber Actors

IACS Industrial automation and control systems

IADS Multi-layered integrated air defense systems

IAI Israeli Aerospace Industries

IAS Indicated airspeed

IBM International Business Machines

ICAO International Civil Aviation Organization

I.C.B.C International Center for Boundary Cooperation (China)

ICBM Intercontinental Ballistic Missiles

ICGs Information centers of gravity

ICS Internet Connection Sharing / Industrial control systems

ICT Information & Communications Technology

ID Information Dominance / Inspection and Identification /Identification

IEC 62443 International standard for industrial automation and control systems

IEDs Improvised Explosive Devices

IEEE Institute of Electrical and Electronics Engineers

IETM	Interactive Electronic Maintenance Manuals
IEWS	Intelligence, electronic warfare, and sensors
IFF	Identification, friend, or foe
IFR	Instrument flight rules
I&I	Interchangeability and Interoperability
IIT	Intentional Insider Threats
Imaging Sensors	ARS sensors that build images
IL	Intensity level of sound measured, dB, Eq. 20-2
IMINT	Imagery intelligence
IMM/IM&M	Interacting-multiple-models tracker / Integrity Management & Monitoring
IMO	International Maritime Organization
IMU	Inertial Measurement Unit
INS	Inertial navigation system
INFOSEC	*Information Security*
IO	Information Operations, see Figure 9-11 & footnotes.
IOB	Internet of bodies
IOC	Intergovernmental Oceanographic Commission
IOR	India Ocean Region
IoT	Internet of things
IIoT	Industrial Internet of things
IPL	Insitu Pacific Limited
IR	Infrared Sensors
IRST	Infrared search and tracking
IS	Information Superiority
ISCS	Integrated shipboard control systems
ISIS	*Islamic State of Iraq and al Sham* (ISIS)
ISR	Intelligence, Reconnaissance and Surveillance UAS Platform
ISTAR	Intelligence, surveillance, target acquisition and reconnaissance
IT/OT	Information Technology/ Operational Technology
ITU	International Telecommunications Union – Standards Organization

ITU-R International Telecommunications Union – Radio Sector

IW Information Warfare

JADC2 Joint all-domain command & control

JADO Joint all-domain operations (Thatcher, 2020)

JAGM Joint-Air-to-Ground Missile

JAUS Joint architecture for UAS

JDAM Joint direct attack munitions

JFO Joint fires observer

JP Joint Publication – followed by military identifier.

JDAM Joint Direct Attack Munition

JNIM Jama'at Nusrat al-Islam wal-Muslimin

JOAC Joint Operational Access Concept

JOPES Joint Operation and Planning System / Execution System

JP Joint Publication

J / S = the ratio of the jammer power to the desired signal power at the input to the receiver being jammed in dB

JST Japan Time zone

JTAC Joint Terminal Attack Controller.

JTIDS Joint Tactical Information Distribution System (JTIDS) is an L band DTDMA.

K Boltzmann's constant (Noise component, RRE) (1.38 x 10 -23 J/K), Kelvin

K 2 for jamming frequency modulated receivers (jamming tuner accuracy), FM 34-40-7

KAMIKAZI Means "Divine Wind," Tactic best known for Japanese suicide A/C attacks on Allied Capital Vessels in WWII. UAS TEAMS or SWARMS could be directed in the same way.

KE Kinetic energy

KEW Kinetic energy weapons

KM Katiba Macina Groups

KMS Key Management System

KSU Kansas State University

L λ / 2 in Eq. 20-5

LAANC Low Altitude Authorization and Notification Capability

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

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

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

LGWs Laser-guided weapons

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

LCAC Landing Craft Air Cushion Facility

LCDR Lieutenant Commander

L/D Lift to drag ratio.

LDCM Low Duty cycle methods

LEO Low Earth Orbit Satellite / Law Enforcement Officer

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

LGTF Liptako-Gourma task force (LGTF) established by Burkina Faso, Mali, and Niger to secure their shared border region.

LIDAR	Light (Imaging) Detection and Ranging
LFS	Free- Space Loss as a Factor
LIPC	laser-induced plasma channel
LJ	Propagation loss from jammer to receiver, in dBi
LMADIS	Light Marine Air Defense Integrated System (family of C-UAS systems)
LMM	Lightweight Multi-role Missile (by Thales)
LNG	Liquid natural gas
LORAN-C	Long Range Navigation, Revision C
LOS	Line-of-sight / Loss of Signal / Loss of Separation
LOSAS	Low-cost Scout UAV Acoustic System
LPA	Log periodic array
LPI	Low Probability of Intercept
LR	Long range
LRA	Long range artillery
LRAD	Long Range Acoustical 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
LSG	Real-time Tracking Laser Scalar Gradiometer
LST	Laser spot trackers
LTA	Lighter than Air (airship) /Low noise amplifier
LTE /LTE+	Long Term Evolution – refers to mobile telecommunications coverage.
LUSV	Large Unmanned Surface Vehicles
LWIR	Long wave Infrared (sensor or camera)
M	Mass in Eq. 20-5
MA	Multi-agent methods of CR
MAC	Unique Media access control address assigned to a

network interface controller (NIC) for use as a network address in communication with a network segment.

MAD	Magnetic anomaly detection
MADIS	Marine Air Defense Integrated System
MAE	Medium-altitude endurance
MAGTF	Marine air-ground task force
MALDRONE	Malware injected into critical SAA for UAS.
MALE	Medium-altitude, long endurance UAS
MALE-T	Medium altitude long endurance – tactical UAS
MAME	Medium altitude, medium endurance
MARIN	Maritime Research Institute Netherlands
MARPOL	Marine pollution (prevention of)
MAS	Mayflower autonomous system
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
MBES	Multi-beam Echo Sounder
MCE	Mission control element
MCM	Mine countermeasures
MCU	Master Control Unit
MCVs	Mesoscale convective vortices
MDR	Missed Detection Rates
Mesonet	network of automated weather and environmental monitoring stations designed to observe mesoscale meteorological phenomena.
MEB	Marine expeditionary brigade (14,500 marines and sailors).
MEMS	Micro-electromechanical systems
MEO	Medium Earth Orbit satellite
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
MIT	Massachusetts Institute of Technology
ML	Machine learning techniques
MLRS	Multi launch rocket systems.
MLU	Mid-life upgrade
MMI	Man-machine interface
MORS	Military Operations Research Society
Modulation	Signal Modulation is the process of varying one or more properties of a periodic waveform, called the *carrier signal*, with a modulating signal that typically contains information to be transmitted
MPA	Maritime patrol aircraft
MPI	Message-passing interface
MPC	Model-based predictive control
MPO	Mission payload operator
MR	Medium range / Maritime Reconnaissance
MRE	Medium-range endurance
MS	Mobile service
MSL / AGL	MSL altitudes are measured from a standard datum, which is roughly equal to the average altitude of the ocean. So, an aircraft traveling 5,000 feet directly above a mountain that's 3,000 feet tall would have an altitude of 5,000 feet Above Ground Level (AGL) and 8,000 feet MSL.
MSR	Maritime Silk Road (China)
MSSM	Multi-step optimization method to achieve re-planning for stealth UAV penetration of ADS.
MTCR	missile Technology Control Regime
MTI	Moving target indication*
MTOM	Maximum take-off mass
MTOW	Maximum takeoff weight of an aircraft at which the pilot can attempt to take off, due to structural or other limits.
MTS	Multi Spectral Targeting System /Maritime Transportation Systems / Sector

MTTR	Multitarget tracking radar/Mean time to repair.
MUAV	Mini-UAV or maritime UAV
MUJAO	Movement for Unity and Jihad in West Africa
MUM	Manned-unmanned teaming.
MUSV	Medium Unmanned Surface Vehicles
MW	Microwave
MWIR	Midwave Infrared
MW	microwave towers
N	Available Noise power, watts for HAPS
N	Terrain and ground conductivity factor, FM 34-40-7

5 = very rough terrain with poor ground conductivity

4 = moderately rough terrain with fair to good ground conductivity

3 = Farmland terrain with good ground conductivity

2 = Level terrain with good ground conductivity[1]

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

NAC	Network Access Control
NACA	National Advisory Committee on Aeronautics
NAS	National Airspace (USA)
NASAMS II	National Advanced Surface to Air Missile System
NATO	North Atlantic Treaty Organization
NAV	Nano-air vehicle / NAV data message for GPS systems
NAVSEAS	Naval Sea Systems Command
NBC	Nuclear, biological, and chemical warfare
NCO	Network-centric operations
NCW	Network Centric Warfare
NDRC	National Development and Reform Commission (China)
NEC	Network enabled capability
NEMESIS	Netted Emulation of Multi-Element Signature against integrated Sensors (USN)

NGA	National Geospatial Intelligence Agency
NGO	Non-Governmental Organization
NIEM	National Information Exchange Model
NIR	near Infrared
NLOS	Non-line-of-sight
NM	Nautical Miles
NMAC	A NMAC is defined as an incident associated with the operation of an aircraft in which a possibility of collision occurs as a result of proximity of less than 500 feet to another aircraft, or a report is received from a pilot or a flight crewmember stating that a collision hazard existed between two or more aircraft.
NMLA	the National Movement for Liberation of Azawad (Tuareg Rebellion)
NO	Numerical Optimization methods of CR
NOAA	National Oceanographic and Atmospheric Administration
NOLO	No onboard live operator (USN)
NOTAM	Notice to airmen
NOx	Nitrogen emissions
NPD	Near Peer Doctrine
NPS	National Park Service
NSA	National Security Agency (US)
NSRL	New Silk Road Sea / Land routes (Chinese)
NSWC	Naval Surface Warfare Center
NSWC PCD	Naval Surface Warfare Center Panama City Division
NTIA	National Telecommunications and Information Administration
NTM/NTOM	Notice to mariners
NTSB	National Transportation Safety Board
NTT	Non-Threat Traffic
NULLO	Not using live operator (USAF)
NUSSRC	National Unmanned Systems Shared Resource Center
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
OoT	Ocean of Things (USN) (DARPA)
ONR	Office of Naval Research
OPA	Optionally piloted aircraft
OPAV	Optionally piloted air vehicle (aka OPV)
OPSEC	Operations Security
OSI	Open systems interconnection
OSS	Office of Strategic Services (now CIA)
OT	Operational technology
OTH	Over- the- horizon
OVPR	Office of the Vice President of Research , KSU
P	Isotropic source of an electromagnetic pulse of peak power, Mw
PACE	Primary; Alternative; Contingency; Emergency
PANCAS	Passive Acoustic Non-Cooperative Collision Alert System
PAR	Photosynthetically Active Radiation Sensor
PB	Particle Beams, Particle beams are large numbers of atomic or sub-atomic. particles moving at relativistic velocities.
PBL	Planetary boundary layer
PCAS	Persistent close air support
PCS	Personal Communication Services
PDV	Parameter Data Vector
PEIRP	Transmitter's effective isotropic radiated power, watts
PFMS	Predictive Flight Management System
PEMSIA	Partnership in Environmental Management of the Seas of East Asia
PGB	Precision guided bomb
PGM	Precision guided missile
PHOTINT	Photographic intelligence (usually sky – ground)
PHX	Airport code for Phoenix

PI	Probability of Incapacitation
PID	Proportional-Integral- Derivative
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
PKI	Public Key Infrastructure
PL	Power level, dB, Eq. 20-1
PLA	Chinese People's Liberation Army
PLAN	Peoples Liberation Army Navy (China)
PLC	Programmable Logic Controllers
PLOCAN	Research facility Oceanic Platform of the Canary Islands
PMA	Post Mission Analysis
PMIAA	Permissions Management: Identification, Authentication and Authorization
PNF	Plug and Fly with custom transmitter, receiver, battery, and charger.
PNT	Reliable communications; positioning, navigation, and timing
PO	Psychological Operations / Performance Objectives
POS	Position and Orientation System
POV	Point of View
PPP	Precise Point Positioning
PPS	Precise positioning service (GPS)
PRC	Peoples Republic of China (China)
Primum Non Nocere – First Do No Harm (Latin)	
PSD	Power Spectral Density
PREACT	*Partnership for Regional East Africa Counterterrorism* (PREACT)
PRF	Pulse repetition frequency codes
PRM	Precision Runway Monitor
PS	Pressure sensor

PSH	Plan-symmetric helicopter
PSR	Primary Surveillance Radar
P t	Power output of the enemy drone, in watts, FM 34-40-7
PW/PSYWAR	Psychological Warfare
PWO	Principal Warfare officer
P(Y)	Precise Signal (GPS)for military positioning
QOS	Quality of Service in HAPs
QR	QR code is a type of matrix barcode which is machine or phone readable.
QUAS	QUT UAS
QUT	Queensland University of Technology
R	1 /Tb is the bit rate (b/s) in link equation
R&D	Research & Development
R4	Energy density received at detected target range, R, nm.
RA	Resolution Advisory
RAC	Range air controller
RACC	Social media RACC Threat Matrix: Removal, Authenticity; Censorship, Collusion
RADAR	Radio Detection and Ranging
RADINT	Radar intelligence
RAM	Radar absorbing materials.
RAS	Radar absorbing structure.
RAST	Recovery, assist, and traverse.
RB	Rule-based methods (Conflict Resolution)
RBW	Red- breasted Woodpecker
RCE	Remote Code Execution
RCO	Remote-control operator
RCS	Radar cross-section
RCTA	Surf Radio Technical Commission for Aeronautics
RDT& E	Research, Development, Test & Evaluation
RED	Risk Estimate Distance
Remote ID	Remote ID has two meanings in this textbook. It is used as an information /

technology device to identify people from a UAV. This term is used in the UAS.

industry and the FAA as a mechanism for identifying an aircraft type and the

registrant from the ground, essentially a digital license plate and registration.

RES	Radio electronic systems
RF	Radio Frequency
RGB	Red Green Blue for VIS camera
RGT	Remote ground terminal
RIAS	Research Institute for Autonomous Systems -University of North Dakota
Rician PDF	Rician probability density function
RIMPAC	Rim of the Pacific Exercise – Maritime
RL	Ramp launched
RMS	Reconnaissance management system /Root-mean-square
RN	Ryan-Nichols Qualitative Risk Assessment Equations 17-2, 17-3
RNRA	Ryan – Nichols Attack / Defense Scenario Risk Assessment for Cyber cases
ROA	Remotely operated aircraft
ROC	Republic of China (Taiwan) / Regional Operations Center (USA)
ROV/ROUV	Remote operating vehicle / Remotely operated underwater vehicle
RPA	Remotely piloted aircraft
RPH	Remotely piloted helicopter
RPV	Remotely piloted vehicle
RR	Radio regulations
RRE	Radar Range Equation
RSA	RSA (Rivest–Shamir–Adelman) -authors of early public –key cryptographic system
RSTA	Reconnaissance, surveillance, and target acquisition
RTA	Dubai Roads and Transport Authority

RTF	Off- the- shelf, Ready -to -Fly
RTG	Real time Gradiometer
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
S&T	Science & Technology
SA	Situational Awareness
SAA	Sense and Avoid &
SAA	*Sense and Act Systems*; replaces *See and Avoid function* of a human pilot.
SAASM	Selective Availability Anti-Spoofing Module
SAE	Society of Automotive Engineers
SAHRV	Semi-autonomous Hydrographic Reconnaissance vehicle
SAM	Surface to Air Missile
SAMPLE	Survivable autonomous mobile platform, long-endurance
SAP	Systems Applications and Products also the name of a company
SAR	Synthetic aperture radar / Search and rescue-especially using helicopters.
SAS	Safety Assurance System
SATCOM	Satellite communications
SBP	Sub Bottom Profiler
SCADA	Supervisory Control and Data Acquisition systems
SCHEMA	Security Incident Identification
SCIF	Sensitive Compartmented Information Facility
SCS	Shipboard control system (or station) / Stereo Camera System / South China Sea
SE	Synthetic environment
SEA	Airport code for Seattle

SEAD Suppression of Enemy Air Defenses

SECDEF Secretary of Defense

Shadowing Airframe shadowing – UAV- Ground signal degradation during maneuver

SEZ Special economic zones

SHM Simple harmonic motion – represented by sign wave.

SHORAD Short Range Air Defense systems

SIGINT Signals Intelligence

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

SINS Ships inertial navigation systems.

SJM Salafi-Jihad Movement

SKASaC Seeking airborne surveillance and control.

SKYNET Fictional artificial intelligence system that becomes self-aware

SLAM Simultaneous localization and mapping

SLAMRAAM Surface launched AMRAAM

SM Separation Management

SMC Single moving camera

SME Subject matter expert

SMR Single main rotor

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

SOA Static Obstacle – Avoidance system

Soft damage DEW disruption to a UAS computer

SOLAS Safety of Life at Sea (International Maritime Convention) [safety conventions]

SONAR Sound Navigation and Ranging

Sox Sulfur emissions

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

SPS Standard position service (GPS)

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

Spot sensors ARS sensors that measure single locations without image library

SPURV Special purpose underwater research vehicle

SQL SQL Injection – common malevolent code injection technique

SR Short range

SRBM Short range ballistic missile, ex SCUD missile

SRL Systems readiness level

SSA Static Sense-and -Act

SSBN Ballistic missile submarine force

SSP Smart Skies Project

SSR Secondary Surveillance Radar

SST Self – Separation Threshold

ST&T Submarine Track and Trail

STANAG 4856 Standard interfaces of UAV Control System for NATO UAV

STCW Standards of training and certification

STK Satellite toolkit

STOL Short take-off and landing

sUAS Small Unmanned Aircraft System

SubT Subterranean Challenge Urban Circuit

SUAVE Small UAV engine

SWARM High level, dangerous collaboration of UAS, UUV, or unmanned boats

SWAT Special Weapons and Tactics (police / paramilitary)

SWAP Size, weight, and power

SWIR Shortwave infrared, 1400-3000 nm, 1.4 -3.0 um wavelength range

SZ **Safety Zone** is defined as the horizontal and vertical separation criteria which form a cylindrical airspace volume around the UAS. In figure 3-2 that volume is defined by 1000 ft. radius and 200 ft. height. It is assumed that initially the UAS is in the center with 100 ft above and below the A/C.

T In Range equation & environment, strength of a received signal, function of square or fourth power of distance, d, from transmitter (Adamy D. -0., 2015)

T Time, sec (RRE)

T Tension in Eq.20-5

TA Traffic Advisory

TAC Target air controller

TACAN Tactical air navigation

TAR Antenna noise temperature, Kelvin

TAS True airspeed

TBO Time between overhauls

TC Type certificate

TCAS Traffic alert and collision avoidance system

TCPA Time to reach Closest Point of Approach

Te Effective input noise temperature, Kelvin,

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

TETRA Terrestrial Trunked Radio for terrestrial terminals / services

Thermobaric Metal augmented charge

THOR Tactical high-power operational responder

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

TL Team Leader

TLS Transport Layer Security

TO take-off

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

TP Trajectory Prediction

TRANSCOM U.S. Transportation Command networks

TRL Technology readiness level: Technology readiness levels are a rating method.

developed by NASA to describe where a technology is in terms of its development. The lowest levels (1 – 3) are technologies that are being.

researched, the middle levels (4 – 6) are technologies that are being prototyped.

and tested, and the highest levels (7 – 9) are technologies that are being.

demonstrated and used. (NASA, 2017)

TS Measured noise temperature, Kelvin units above absolute zero.

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

TT & C Telemetry, tracking and command.

TUAV Tactical UAV

UA Unmanned Aircraft (non-cooperative and potential intruder)

U-Actors Unintentional Cyber Actors

UAE United Arab Emirates

UAM Urban Air Mobility (vehicle)

UAPO Unmanned Aircraft Program Office

UAS Unmanned aircraft system

UASCdr Unmanned aircraft system commander

UASIPP UAS Integration Pilot Program

UAS-p UAS pilot

UAV Unmanned aerial vehicle / Unmanned autonomous vehicle.

UAV-p UAV pilot

UBR Uplink bit rate, Mb/s

UCAR Unmanned combat armed rotorcraft

UCARS UAV common automated recovery system

UCAV Unmanned combat air vehicle

UCWA / UA Unintentional cyber warfare attack

UG Underwater glider (USN)

UGCS Unmanned Ground Control Station

UGS Unmanned ground-based station

UGT	Unmanned ground transportation
UGV	Unmanned ground vehicle
UHF	Ultra High Frequency, 300 MHz – 3 GHz
UIT	Unintentional Insider Threats
UK	United Kingdom
UL	Upload link
ULC	Uniform Law Commission
ULPCG	University of Las Palmas de Gran Canaria
UMTS	Universal Mobile Telecommunications System
U.N.	United Nations
UND	University of North Dakota
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNICEF	United Nations Children's Fund
US	United States
USAMRIID	U.S. Army Medical Research Institute of Infectious Diseases
USBL	Responder for Surface Ultra Short Baseline
USCG	United States Coast Guard
USCGA	United States Coast Guard Auxiliary
USD	Unmanned surveillance drone / United States Dollar
USMC	United States Marine Corp
USS	Undersea Search and Survey
USV	Unmanned surface vehicle [Boat]
UTM	Unmanned Traffic Management / Safe Uniform Traffic Management
UTV	Unmanned target vehicle
UUV	Unmanned underwater / undersea vehicle.
UV	Unmanned Vehicle
UUNs/DUNSs	Urgent / deliberate universal needs statements
UXO	Unexploded Ordinance
V	Visible
VCR	Video Camera Recorder
VFR	Visual flight rules

VHS	Very High Frequency Radio
VIKI	Virtual Interactive Kinetic Intelligence
VLA	Very light aircraft
VLJ	Very Light Jet
VLAR	Vertical launch and recovery
VLOS	Visual Line of Sight
VMC	Visual Meteorological Conditions
VNIR	Visible light and near infrared 400 – 1400 nm, 0.4 – 1.4 um wavelength range
VOA	Voice of America
Voloport	Landing site for Volcopter.
VTC	Vessel traffic control
VTM	Vessel traffic management
VTOL	Vertical take-off and landing
VTUAV	Vertical take-off UAV
WABN	wide available broadband networks
WARM	identify war reserve mode emissions.
WEF	World Economic Forum
WEZ	Weapon Engagement Zone
WMD	Weapons of Mass Destruction /Weapons of Mass Disruption
WMDD	Weapons of Mass Destruction Directorate
WRC	World Radio Conference Standards Organization
XLUUV	Extra-large unmanned undersea vehicle
XO	Executive Officer of Naval vessel
ZIGBEE or KILLERBEE	Sniffing / penetration tools specific to UAS.

Greek / Mathematical Symbols

λ	Wavelength in Hz, c / f where c= speed of light 344 m/s and f = frequency, Hz.
Σ	Radar Cross Sectional Area, m2
υ	UAV velocity vector and UAV speed (ms -1)
θ	Horizontal angle in inertial axes (rad)
Ψ	Vertical angle in inertial axes (rad)

x,y,z Inertial position coordinates (m)

κ Curvature (m-1)

τ Torsion, (m-1)

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

h Path length (m)

e Basis axes vector set.

$P(x, y, z, \theta, \Psi)$ UAV pose where: where x, y, z, is the UAV location or waypoint and (θ, Ψ) are.

the horizontal and vertical angles , respectively

Ps Starting pose for UAV moving to

Pf Finish pose

Ц Path constraint in (9.4)

a lateral acceleration proportional to curvature k

∞ vector operator in (9.6)

f(n) Path cost function in (9.9)

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

h(n) Heuristic function which estimates the distance from the next node n on the path.

to goal in (9.9)

h(X) represents actual journey cost from goal X.

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

stealth UAV in (9.10)

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

W length of the control domain in (9.11)

qi Output prediction error

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

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

3-D three dimensional

Special Definitions

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

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

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

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

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

Alford, L. D., Jr., USAF, Lt. Col. (2000) Cyber Warfare: Protecting Military Systems *Acquisition Review Quarterly*, spring 2000, V.7, No. 2, P, 105, (Nielsen, 2012)

Nichols, Randall K.; Mumm, Hans C.; Lonstein, Wayne D.; Ryan,

Julie J.C.H.; Carter, Candice; and Hood, John-Paul, "Unmanned Aircraft Systems in the Cyber Domain" (2019). *NPP eBooks*. 27. https://newprairiepress.org/ebooks/27

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

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

and (Gelfand S. A., 2009)

A majority of the technical abbreviations come from (Nichols R. K., et al., Unmanned Aircraft Systems in the Cyber Domain, 2019) and (Nichols, et al., Counter Unmanned Aircraft Systems Technologies and Operations, 2020) (Nichols & et.al, 2020) (Nichols, et al., Unmanned Aircraft Systems (UAS) in Cyber Domain: Protecting USA's Advanced Air Assets, 2nd Edition, 2019) Nichols, R. K., Ryan, J., Mumm, H., Lonstein, W., Carter, C., Hood, J., . . . & Jackson, M. (2020). *Unmanned Vehicle Systems & Operations on Air, Sea, Land*. Manhattan, KS: New Prairie Press #35. Nichols, R. K., Sincavage, S., Mumm, H., Lonstein, W., Carter, C., Hood, J., . . . & Shields, B. (2021). *Disruptive Technologies With Applications In Airline, Marine, Defense Industries*. Manhattan, KS: New Prairie Press, #TBA.

Other definitions from the following references:

References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Austin, R. (2010). "*Design for Stealth*", *Unmanned Aircraft Systems*

UAVS Design Development and Deployment. New York: John Wiley and Sons.

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

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

Bernstein, R. A. (29 June 2012). *MUNITIONS DETECTION USING UNMANNED UNDERWATER VEHICLES EQUIPPED WITH ADVANCED SENSORS.* Panama City, FL: NSWC PCD ESTCP Project Number MR-201103 Ver 7a.

Black Swan Definition. (2020, December 16). Retrieved from https://www.investopedia.com/terms: https://www.investopedia.com/terms/b/blackswan.asp#:~:text=A%20black%20swan%20is%20an,they%20were%20obvious%20in%20hindsight.

Bluefin Robotics. (2020, December 15). Retrieved from gdmissionsystems.com/underwater-vehicles/bluefin-robotics: https://gdmissionsystems.com/underwater-vehicles/bluefin-robotics

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

Crouch, T. (2014, March). *history-of-flight/wright-brothers-first-flight-photo.* Retrieved from www.airspacemag.com: https://www.airspacemag.com/history-of-flight/wright-brothers-first-flight-photo-annotated-180949489/

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

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

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

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

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

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

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

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

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

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

DoD-01. (2018). *JP 1-02.* Retrieved from Department of Defense

Dictionary of Military and Associated Terms: www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

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

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

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

DTRA. (2019, October 18). Private Communication re Aviation Vulnerabilities. (Nichols, Interviewer) Retrieved from https://www.dtra.mil/

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

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

EIA. (2019, June 20). *The Strait of Hormuz is the world's most important oil transit chokepoint.* Retrieved from EIA – US Energy Information Administration: https://www.eia.gov/todayinenergy/detail.php?id=39932

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

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

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

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

FAA. (2018, February 1). *Part 107 Rule for sUAS.* Retrieved from Fly under the Special Rule for Model Aircraft: https://www.faa.gov/uas/getting_started/model_aircraft/

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

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

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

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

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

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

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

1. Sulzberger, J. B. (2009). *Hunting Sea Mines with UUV-Based Magnetic and Electro-Optic Sensors.* Retrieved from algebra.sci.csueastbay.edu/: http://algebra.sci.csueastbay.edu/~grewe/pubs/DistSensorNetworkBook2011/Atmosphere/UnderWaterSeaMineHunt.pdf

Gallagher, S. (2019, September 16). *Missiles and drones that hit Saudi* *oil fields: Made in Iran, but fired by whom?* Retrieved from Arstechnica.com: https://arstechnica.com/tech-policy/2019/09/missiles-and-drones-that-hit-saudi-oil-fields-made-in-iran-but-fired-by-whom/

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

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

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

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

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

Hartman, K. a. (2013). The Vulnerability of UAVs to Cyber Attacks – An Approach to the Risk Assessment. *2013 5th International Conference on Cyber Conflict* . Tallin: NATO CCD COE Publications.

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

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

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

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

Howard, C. (2019, June 21). *What is the Strait of Hormuz, where Iran shot down US Navy drone?* Retrieved from Fox News:

https://www.foxnews.com/world/whats-the-strait-of-hormuz-iran-shot-us-navy-drone

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

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

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

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

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

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

Kania, E. (2017, July 6). Swarms at War: Chinese Advances in Swarm Intelligence. China Brief Volume: 17 Issue 9. *China Brief Volume: 17 Issue 9*.

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

Kaye, T. a. (2001, September 30). ACHIEVING INFORMATION DOMINANCE:. Retrieved from DODCCRP-Space and Naval Warfare Systems Center San Diego: http://www.dodccrp.org/events/2002_CCRTS/Tracks/pdf/026.PDF

Kim, A. G. (2012, June). *Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles.* Retrieved from Infotech@Aerospace.com: https://www.researchgate.net/publication/268571174_Cyber_Attack_Vulnerabilities_Analysis_for_Unmanned_Aerial_Vehicles

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

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

Kovacs, T. (1998). *Micromachined Transducers Sourcebook.* NYC: McGraw-Hill.

Leasko, R. (2014). *Munitions Detection Using Unmanned Underwater Vehicles Equipped with Advanced Sensors.* Scotts Valley, CA: CreateSpace Independent Publishing Platform (Amazon Media on Demand).

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

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

Lister, T. (2019, September 16). *Attack is a game-changer in Gulf confrontation.* Retrieved from CNN: https://www.cnn.com/middleeast/live-news/saudi-oil-attack-dle-intl/h_3e647100fa720927c962d7643472b12d

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Moir, I. a. (2006). *Military Avionics Systems.* New York: Wiley Aerospace Series.

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

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

Myer, G. (2013, May-June). *Danger Close Definition.* Retrieved from US Army Magazine: www.benning.army.mil/infantry/magazine/issues/2013/May-June/Myer.html

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

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

NASA. (2018). *Unmanned Aircraft Systems* (UAS) *Integration in the National Airspace System* (NAS) *Project.* Retrieved from NASA: https://www.nasa.gov/feature/autonomous-systems

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

Naval Mines. (2020, December 16). Retrieved from en.wikipedia.org: https://en.wikipedia.org/wiki/Naval_mine#cite_note-minewar-83

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

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

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

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

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

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

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

Nichols, R. K. (2019, October 15). *Randall Nichols (October 15, 2019) Implications from Attack by Iran on Saudi Arabian Oil Fields (implications-from-attack-iran-saudi-Arabian-oil-fields-Nichols.* Retrieved from www.linkedin.com/pulse/: https://www.linkedin.com/pulse/implications-from-attack-iran-saudi-arabian-oil-fields-nichols/

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

Nichols, R. K., & et.al. (2020). *Unmanned Vehicle Systems & Operations on Air, Sea, Land.* Manhattan, KS: NPP #35.

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

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

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

Nichols, R. K., Mumm, H. C., Lonstein, W. D., Ryan, J. J., Carter, C., & and Hood, J.-P. (2019). *Unmanned Aircraft Systems in the Cyber Domain, 2nd Edition.* Manhattan, KS: NPP eBooks. 27. Retrieved from www.newprairiepress.org/ebooks/27

Nichols, R. (Nov 28-30, 2006). Cyber Terrorism, Critical

Infrastructure, & SCADA Presentation. In R. Nichols (Ed.), *Defense Threat Reduction Agency Conference.* Shirlington VA: Utica College, Utica NY.

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

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

Nichols, R.-0. (2016, March 29). NCIE UAS SAA Final Rev 4. 2016 INFOWARCON *conference presentation April* 4-7, Nichols, R.K. et. al. (3-29-2016) Presentation to INFOWARCON April 4-7 on NCIE UAS SAA Final Rev 4, presented to 2016 INFOWARCON conference, Memphis TN. Available as PPTx presentation download from author or in CANVAS. Memphis, TN, USA: INFOWARCON16.

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

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

NSWC. (2020, December 15). *Warfare Centers* NSWC *Panama City.* Retrieved from www.navsea.navy.mil: https://www.navsea.navy.mil/Home/Warfare-Centers/NSWC-Panama-City/What-We-Do/

Ocean Studies Board, N. R. (2012). *Oceanography and Mine Warfare.* Washington, DC: Ocean Studies Board, National Research Council ISBN 0-309-51587-4.

Osborn, K. (2019, October 15). *Swarm Hell: Can the U.S. Army Stop Hundreds of Drones Armed with Explosives*? Retrieved from National Interest: https://nationalinterest.org/blog/buzz/swarm-hell-can-us-army-stop-hundreds-drones-armed-explosives-88206

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

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

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

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

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

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

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

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

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

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

Randall K. Nichols, D. (2018). Chapter 20 Acoustic CM & IFF Libraries V SWARMS Rev 1 05142019. In R. K. Nichols, H. C. Mumm, W. D. Lonstein, & J. S. Hood, *Unmanned Aircraft Systems* (*UAS*) *in the Cyber Domain: Protecting* USA's *Advanced Air Assets, 2nd ed.* 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, D. J. (2000). *Defending Your Digital Assets against Hackers, Crackers, Spies and Thieves.* New York: RSA Press.

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

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

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

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

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

REMUS -1. (2020, December 15). *REMUS 100 Technical Brochure (2017).* Retrieved from www.hydroid.com: https://www.hydroid.com/sites/default/files/product_pages/ New_Generation_REMUS_100_%20Brochure_2017.pdf

REMUS -2. (2020, December 15). *REMUS 600 Technical Data.* Retrieved from www.hydroid.com/remus-600-defense-applications: https://www.hydroid.com/remus-600-defense-applications

REMUS. (2020, December 15). *REMUS 100 for Defense Applications Data Sheet.* Retrieved from https://www.hydroid.com/new-generation-remus-100-defense-applications: https://www.hydroid.com/new-generation-remus-100-defense-applications

REMUS -3. (2020, December 15). *REMUS 600 Technical Data Sheet.* Retrieved from www.hydroid.com/: https://www.hydroid.com/ sites/default/files/product_pages/ REMUS_600_Brochure_2017_0.pdf

REMUS -4. (2020, December 15). *REMUS 6000* . Retrieved from www.hydroid.com/: https://www.hydroid.com/sites/default/files/product_pages/REMUS_6000_Brochure_2017.pdf

REMUS -5. (2020, December 15). *REMUS 6000 Brochure*. Retrieved from www.hydroid.com/: https://www.hydroid.com/sites/default/files/product_pages/REMUS_6000_Brochure_2017.pdf

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

Roland, A. (1977). Bushnell's Submarine: American Original or European Import? *Technology and Culture: The Johns Hopkins University Press*, Vol. 18, No. 2 (Apr., 1977), pp. 157-174 (18 pages).

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

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

SERDP-ESTCP. (2012). *Munitions-Response/Munitions-Underwater/MR-201103-IR*. https://www.serdp-estcp.org/Program-Areas/Munitions-Response/Munitions-Underwater/MR-201103: NSWC PCD.

Sheena McKenzie, M. W. (2019, September 17). *Saudi attacks send oil prices soaring*. Retrieved from CNN: https://www.cnn.com/middleeast/live-news/saudi-oil-attack-dle-intl/h_1ab7e8469e98525f887c3a4e588dde8a

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Stratfor. (2019, October 20). *strait-of-Hurmuz-chokepoints.* Retrieved from https://www.stratfor.com: https://www.stratfor.com/sites/default/files/styles/wv_small/public/strait-of-hormuz-chokepoints.jpg?itok=xSgx6Hhi

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

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

Sun, W. M. (June 2015). Unmanned Aircraft Systems: Air-Ground 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.*

Teledynemarine. (2020, December 16). *Q-Boat_1250.* Retrieved from www.teledynemarine.com: http://www.teledynemarine.com/Q-Boat_1250?BrandID=13

Teledynemarine-1. (2020, December 16). *Z-Boat1800T_Trimble.* Retrieved from www.teledynemarine.com: http://www.teledynemarine.com/Z-Boat1800T_Trimble?BrandID=13

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

Thatcher, M. K. (2020, August 9). *Integrated Joint All-Domain Operations Full Spectrum Operations.* Retrieved from www.lockheedmartin.com: https://www.lockheedmartin.com/

content/dam/lockheed-martin/aero/documents/mdo/ Integrated_JADO_Solution_Whitepaper.pdf

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Wiley, R. G. (1993). *Electronic Intelligence: The Analysis of Radar Signals, 2nd ed.* Norwood, MA: Artech House.

Wilson, M. (2012). The Use of Low-Cost Mobile Radar Systems for Small UAS Sense and Avoid. *Sense and Avoid in UAS Research and Applications.*

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

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

Wright, T. (2017, August 11). *You've Been Warned: Keep Your Drones*

Away From Military Bases. Retrieved from Air & Space, Smithsonian: https://www.airspacemag.com/daily-planet/keep-your-drones-away-military-base-180964451/

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

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

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

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

Yu, X. &. (2015). Sense and avoid technologies with applications to unmanned aircraft systems: Review and prospects. *Progress in Aerospace Sciences*, 74, 152-166.

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

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

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

[1] FM 34-40-7

Table of Contents (Detailed)

Table of Figures

1: Propulsion and Fuels: Disruptive Technologies for Submersible Craft Including UUVs [Jackson]

2. Automation & Human-Machine Symbiosis [Mumm]

3. UAS Regulation / Innovation / Safety 2020 / Privacy and Beyond [Hood]

4. UUVs, Advanced Sensors, Munitions Detection, USVs [Nichols]

7. Failure of Climate Change [Nichols]

8. Nightmare Technologies [Nichols]

9. Social Media – The Next Battleground in Information Warfare [Lonstein]

Table of Tables

Table of Equations

1: Propulsion and Fuels: Disruptive Technologies for Submersible Craft Including UUVs [Jackson]

The length of the aft hull-section (Laft) is (Eq. 1.1):

(1.1)

$L_{aft} = 100 - (L_{fwd} + L_{mid})$

The radius of the forward hull-section, Rfwd, for a given axial coordinate, x, is defined as a modified semi-ellipsoid (Eq. 1.2):

(1.2)

$R_{fwd} = (D /2) \{ [1 - (x- L_{fwd} / x)^{2}]^{n} \}$

The radius of the aft hull-section, Raft, is defined as (Eq. 1.3):

(1.3)

$R_{aft} = (D /2) - \{ [(3D/2L_{aft}{}^{2} - \tan \alpha / L_{aft}) (x - L_{fwd} - L_{aft})^{2}] \}$

6 Future Proof Security [Shields]

(6.1) Asset Authentication = Asset Identity Validation + Asset Identity Verification

1. Propulsion and Fuels: Disruptive Technologies for Submersible Craft Including UUVs [Jackson]

Student Learning Objectives – The student will understand disruptive technologies associated with submersible craft including unmanned underwater vehicles (UUVs).

The student will be able to:

- Understand the drivers for change that leads to the adoption of disruptive technologies.
- Appreciate the need for international regulations to manage the disruption.
- Explain the current and future disruptive technologies that drive the need to change fuels for use in new propulsion systems.
- Understand the role of naval architects in developing submersible craft including UUVs that adopt disruptive technologies.

Introduction

Drivers for Change

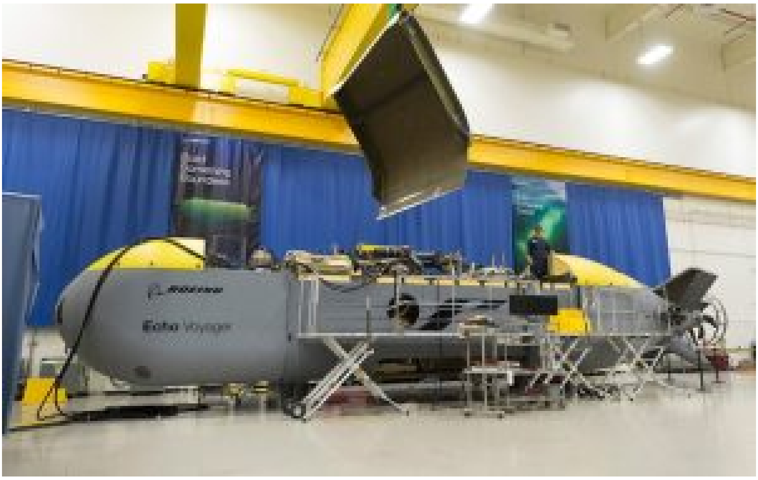
The major disruptors in terms of propulsor's and associated fuels for UUVs (Button, 2009) are driven by three areas: introduction of carbon taxes, rising cost of fuel and environmental regulations. In terms of carbon emissions, Article 2.2 of the Kyoto Protocol limits carbon emissions and is governed by the International Maritime

Organization (IMO) for all seafaring craft (American Bureau of Shipping, 2019). Failure to reach such an agreement globally means that individual nations is responsible for its own reductions and the IMO developed the Energy Efficiency Design Index (EEDI) to support nations who are proactive at reducing carbon emissions. At best, nations monitor reductions, and the naval architect develops procedures aimed at reducing the carbon footprint of the craft.

The rising price of oil is a way of reducing carbon emissions from an economic viewpoint. As it is a finite resource, there will be a point when the price of oil will force operators of submersibles including UUVs to use an alternate fuel and its finite volume is seen as a significant disruptor that will force naval architects to design craft that will use renewable sources of energy (Department of the Navy, 2004), (Department of Defense, 2011), (Department of Defense, 2012). Extra-large UUVs (XLUUVs) is set to become the dominant UUV for the US Navy starting 2023 (US_Congress, 2020). The US navy defines XLUUVs as greater than 48 inches in diameter and can only be launched from a pier rather than a manned submarine.

A typical XLUUV is shown in Figure 1.1 and is known at the Boeing Echo Voyager XLUUV. The Echo Voyager is 51 feet in length and has a rectangular cross section of 8.5 feet x 8.5 feet, a weight in air of 50 tons, and a range of 6,500 nautical miles. It can accommodate a modular payload section up to 34 feet in length and provides 2,000 cubic feet of internal payload volume.

Figure 1.1 Boeing Echo Voyager XLUUV. Courtesy of Boeing (https://www.boeing.com/defense/autonomous-systems/echo-voyager/index.page)



International Regulations

The regulatory authority that serves the international maritime community is known as the 'International Maritime Organization' and is an arm of the United Nations (UN). The UN has a secretariat of flag states where regulations and conventions are debated and agreed. The IMO provides rules that follow the regulations and are adopted across all territorial and international waters. There are a number of regulations that cover UUVs and are associated with the prevention of marine pollution (MARPOL), standards of training and certification (STCW) and safety conventions (SOLAS). MARPOL applies to the protection of the marine environment from the craft itself, STCW provides a competency framework for operators of UUVs and SOLAS applies to structural integrity of UUVs and other seafaring craft, manned or unmanned (American Bureau of Shipping, 2019). Emissions control under MARPOL Annex VI restricts the emissions of nitrogen (NOX) and sulfur (SOX) pollutants during the combustion of diesel in prime movers. However, restrictions in ozone, particulates and greenhouse gases are included in subsequent amendments of Annex VI.

The standards are arranged in three tiers I, II, and III. Tier I was established in 1997 and ratified in 2004, whereas Tiers II and III were established in 2008 and ratified in 2010. NOX limits apply globally, whereas SOX limits apply regionally. Large seafaring vessels typically produce relative CO2 emissions between 1 – 3, whereas airplanes emit 398 relative units of CO2, small goods vehicles emit 226 relative units of CO2, large articulated trucks emit 49 relative units of CO2, while railway wagons emit 6 relative units of CO2. Therefore, ships and submersibles have a low carbon footprint than other forms of global transport.

Fuels and Propulsion: Current Disruptive Technologies

Diesel Fuels

Diesel engines have improved significantly since the 1980s with advances associated with increased bore/stroke ratio, slow- and medium-speed engines, improved peak pressures and significant fuel reductions in two-stroke engines. Turbocharging efficiency and fuel injection technology have contributed to further reductions in consumption in four-stroke engines. However, since the mid-1990s, the design of diesel engines changed due to the reduction of NOX and SOX emissions without changing fuel efficiency requirements. Marine engine design has changed since the mid-1990s and include changes such as: low NOX combustions with adjustable camshafts, variable inlet valve controls, high boost pressures and better combustion chamber design, greater mechanical strength of engines, two-stage turbocharging, exhaust gas recirculation, waste gate technology, sequential turbocharging, variable turbine geometry, humidification of inlet air, use of selective catalytic reduction systems, exhaust gas scrubbing, and the emulsification of fuels (MAN Energy Solutions, 2018).

The disruptive technologies used for improving NOX emissions in diesel engines are focused on reducing peak temperatures and duration of the combustion cycle and the use of Miller cycle inlet valve timings and higher-pressure turbochargers. It has been discovered that using the Miller cycle instead of the Diesel cycle during combustion reduces NOX emissions by reducing the cycle temperature at constant high pressure, hence the use and further development of high-pressure turbocharging using two-stage turbochargers.

Biofuels

Collections of cells and proteins and the conditions under which these natural living systems grow and replicate created the first biofuels. The first generation of biofuels consisted of biodiesel and bioethanol. Biodiesel is manufactured from vegetable oils (coconut, palm, rape seed, soybean, and tallow) and animal fats. They are classed as fatty acid methyl esters (FAME) and are manufactured when vegetable oils and animal fats react with alcohol such as methanol. Bioethanol is manufactured by fermenting renewables based on sugar or starch. These ingredients are typically cassava, corn, sorghum, sugar beets, sugar cane and wheat. The variability in FAME stability in various conditions is due to the type of ingredients used in their formulation and their ability to absorb water and hold in suspension, which causes hydrolytic reactions that causes FAME to revert to fatty acids. If water is dissociated microbiological growth can clog filters and corrosion of engine parts can occur.

Disruptors that may enhance and increase the use of biofuels focus on producing synthetic fuels based on branch-chain higher alcohols, E-coli, microorganisms such as yeast and algae-based fuels. Other types of fuels that may be used in the future could be based on di-methyl ether (DME) that can be produced from biomass, natural coal and gas and oil residues. It is condensed when pressured above 0.5 MPa, is non-toxic and environmentally benign and is not dissimilar to liquid natural gas (LNG). It has a high cetane number and is high in oxygen content when mixed in air achieving smokeless combustion and very low formation of particulates. However, it has a lower density than other fuels and lower combustion enthalpy. It requires lubricity and corrosive inhibiting additives, but despite the issues of lubricity and corrosion, it has high thermal efficiency, low noise, low NOX emissions and is low in particulates (low soot formation) (MAN Energy Solutions, 2018).

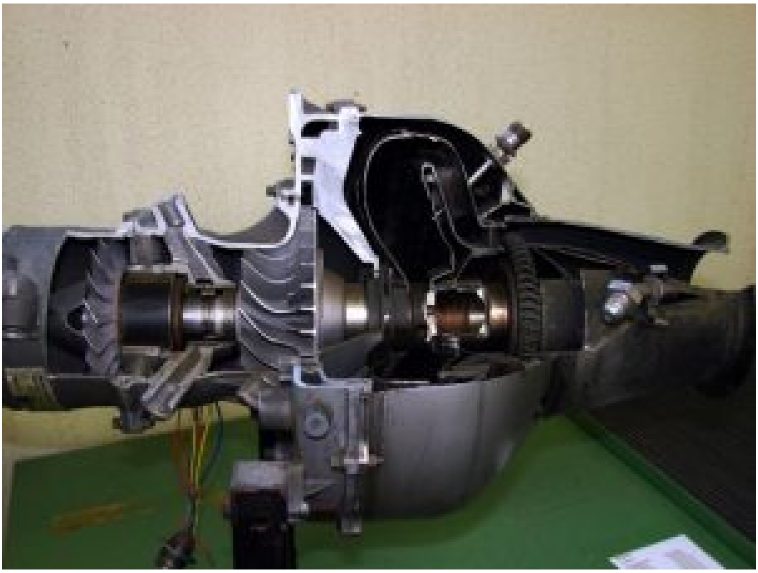
Liquid Natural Gas (LNG) Fuels

The principal constituent of LNG is CH4, which reduces CO2 emissions by 25%. Also, NOX production is 85% less due to compression ratio and combustion temperature differences. Since sulfur is absent from the fuel, SOX emissions are non-existent. The advantages of using LNG are described as low emissions, existing marine engines burn LNG, LNG is cheaper than most fuels, and fueling technology is well established. The disadvantages associated with LNG are associated with methane slip and that LNG requires a heat source to evaporate it to form a gas used for combustion.

Gas Turbine Propulsion

Gas turbines are used for direct propulsion or can be used to generate electricity to electric motors when not used for propulsion. Figure 1.2 shows a typical cross-section of a gas turbine. This allows them to be used for hybrid operations coupled to diesel engines or diesel generators. Gas turbines have the advantage of low weight compared to standard prime movers and aero-derivative turbines burn distillate fuels that satisfy current regulations on emissions and smoke generation. However, distillate fuels are more expensive than standard marine fuels, and are very powerful when turbines are heat recovery turbines are coupled to use the exhaust gases to increase thermal efficiency for electricity generation. Indeed, gas turbines can be used for propulsion and for providing electricity to secondary propulsion units. The advantages of using gas turbines lies in the fact that they are high power density prime movers and are low weight and small size. NOX emissions are low and SOX emissions are negligible due to use of high-grade fuels. However, distillate fuels are expensive, turbines are less efficient as ambient temperature increases and thermal efficiencies are lower compared to diesel engines (MAN Energy Solutions, 2018).

Figure 1.2 Cross section of a typical gas turbine engine. Courtesy of Tilyudai and reused under license CC BY-NC-SA 2.0. To view a copy of this license, visit https://creativecommons.org/licenses/by-nc-sa/2.0/.



Nuclear Propulsion

Energy generation and storage usually relies on breaking chemical bonds between atoms. Nuclear power relies on converting large and heavy nuclei into smaller fission products by controlled chain reactions. A large amount of heat is generated that is converted to usable power via an appropriate thermodynamic cycle. Nuclear propulsion is CO2 free and is quite disruptive in terms of using it as a propulsion source. Molten salt thorium reactors are considered to be disruptors to using diesel and turbine power units owing to the abundance of thorium compared to uranium and using molten salts of fluorides and chlorides to act as coolants operating at temperatures in the range of 650OC to 700 OC. Such reactors are in development and the use on seafaring craft is governed by the IMO's Code of Safety for Nuclear Ships, Resolution A.491 (XII), 1981. However, they have not been used on UUVs and small submersibles so experience and knowledge of operation from larger submarines may have to be transferred to the naval architect responsible for using them in UUVs. The advantages of using them include no emissions generated, the design of reactors is well established so could easily be adapted for UUVs, they can be small and modular in design, the cost of fuel is paid at the beginning of use and is not subjected to price fluctuations. The disadvantages of this technology are associated with knowledge of safety and the lack of systems engineering knowledge in personnel that would prevent wider adoption, design of UUVs may be constrained because of the technology, regulatory standards would need to be created for use in UUVs, support systems and planned response to misuse would need to be developed and for use a new and controversial technology, proof of concept and the management of public perception will need to be managed (MAN Energy Solutions, 2018).

Battery Technology

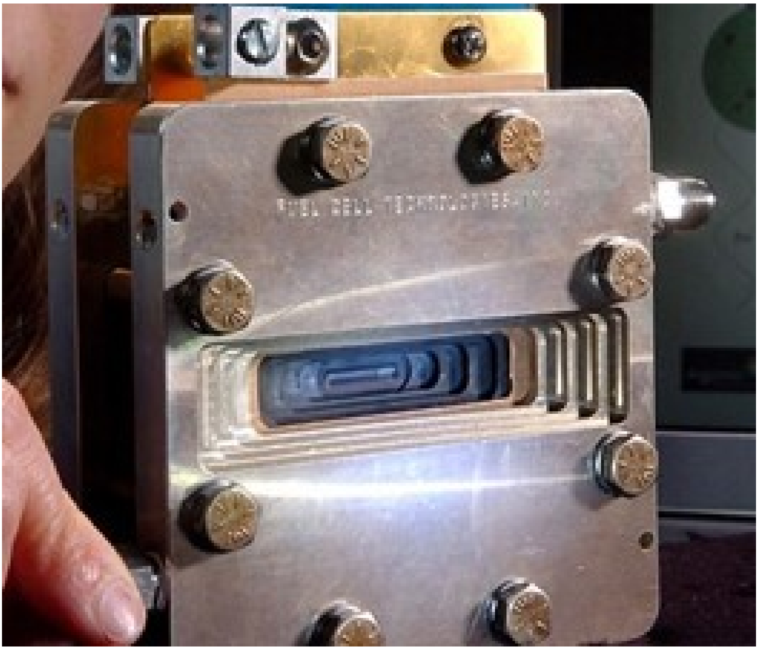
Battery technology is very well advanced and documented. New battery chemistries are fundamental and constitute the most disruptive technology associated with their wider use on UUVs. Metal-sulfur is typical, but metal-air is becoming more widespread such as lithium-air being the leading couple due to its ability to provide the highest amount of energy per density of metal. However, post lithium-air battery technology is being developed due to the limited supply of lithium. The use of magnesium-air batteries is being considered and the technology developed because magnesium can be harvested from salt water. However, energy storage is thought to be the key to the future for UUVs, so the development of supercapacitors to store charge is a key disruptor for many areas of transport, not least UUVs. The advantages of batteries on UUVs are focused on non-generation of emissions, continuous development means that they will get smaller and more powerful and that batteries can be used as hybrid power generators with combinations of other modes of propulsion (MAN Energy Solutions, 2018). Disadvantages include size and the fact that they need to be recharged/replaced when the UUV is being used in service. A submarine battery cell is shown in Figure 1.3.

Figure 1.3 Submarine battery cell. Courtesy of Jamie Sanford and used with permission under license CC BY-NC 2.0. To view a copy of this license, visit https://creativecommons.org/licenses/by-nc/2.0/.

Fuel Cells

Fuel cells were invented in 1838 but not widely adopted until recently due to their low mass, the emission of the fuel cell is water, and because materials technology has advanced so much in recent years that fuel cells may be widely used. They are electrochemical and require support plant such as pumps and fans and rely on hydrogen and oxygen combining to release energy. The reactants consumed by the fuel cell is stored externally rather than internally (batteries) and can be renewed continuously rather than depleted (battery). Therefore, it produces power all the time as long at the reactants are supplied to it. There are certain drawbacks to their use such as hydrogen supply issues at sea and they have lower specific power and density compared to diesel engines. They also provide direct current output that is not compatible with coupling to mechanical transmission systems (MAN Energy Solutions, 2018). However, they can be used for auxiliary power sources, methanol can be used as a substitute fuel, they are quiet (no moving parts), and they require clean fuels that do not emit SOX or NOX due to low temperature operation. Figure 1.4 shows a fuel cell developed by the Argonne National Laboratory, USA.

Figure 1.4 Fuel cell. Courtesy of Argonne National Laboratory (license CC BY-NC-SA 2.0). To view a copy of this license, visit https://creativecommons.org/licenses/by-nc-sa/2.0/.



Hydrogen Fuel

Hydrogen is a potential disruptive fuel for use on UUVs and can come from sources such as wind, hydro-electric, nuclear or as a conventional fuel used in fuel cells. The advantages of using liquid hydrogen are that it does not produce CO2 or SOX emissions, it uses land-based sources of power for creation, it can be used in fuel cells and in internal combustion engines and burning it produces a large amount of fresh water (MAN Energy Solutions, 2018). However, it is unknown in the marine sector, has some safety issues and a supply infrastructure would be needed for use in UUVs.

Future Disruptive Technologies for Propulsion and Fuels

Hybrid Propulsion

Hybrid propulsion is an option where different modes of power can be used to optimize the operation of the UUV. The reasons for selecting hybrid propulsion systems are focused on reduced fuel consumption, reduced impact of CO2 and other pollutants, variable future fuel costs and supply, insurance against increasing environmental legislation, noise reduction, operating in zero emission mode, and lower amount of maintenance.

Further disruptive technologies associated with propulsion include the use of propellers such as fixed pitch, controllable pitch propellers and ducted propellers. The type of propeller used for UUVs is determined by operational conditions. Typically, for small high-speed UUVs both rotational speed and propeller advance can be high and it can be difficult to control the effects of cavitation. Therefore, developments in the use of ducted and podded propellers will need to be made to apply this disruptive technology to UUVs. Other types of propeller to be considered for use on UUVs include contra-rotating propellers, and cycloidal propellers. The naval architect should maximize the diameter of the propeller so that torque, thrust, and propeller efficiency are maximized. The propeller can be approximated to a Wageningen B-screw series using open water design data. This is well characterized in most texts concerned with naval architecture (Lewis, 1988). Other disruptive technologies to consider for propulsion is waterjet propulsion and magneto hydrodynamic propulsion for small UUVs.

Energy Saving Devices

Energy saving devices associated with hydrodynamic flow are considered in three sections of the hull: before the propeller, at the propeller and after the propeller. There are some overlapping areas but mostly operate at the boundary layer and in the wake of the UUV. Devices placed on the flow of the propeller include wake equalizing ducts, asymmetric stern, Grothuis spoilers, partial stern tunnels, Mewis ducts, reaction fins, Zozen nozzles, and integrated ducted propellers.

Disruptive technologies applied to the propeller area include low speed propellers, propellers with end plates, Kappel propellers and propeller boss cap fins. For energy saving behind the propeller, grim vane wheels, rudder thrusting fins and rubber bulb fins are adopted depending on the mode of operation (Hughes, 2010).

Hull Design (Appendages and Coatings)

The efficiency of the hull is governed by the form of the hull and its dimensions (Nicholls, 2020). The hull envelope for submersibles is described by the Jackson hull-form (Figure 1.5) (Hughes, 2010). However, the stern of the UUV can be improved by using the Myring hull-form with its axisymmetric geometry. The Myring hull-form is a function of five variables: forward length of hull-section (Lfwd), parallel mid-body length (Lmid), forward curvature index (n), tail semi-angle (α), and maximum hull-form diameter (D).

The length of the aft hull-section (Laft) is (Eq. 1.1):

(1.1)

$$L_{aft} = 100 - (L_{fwd} + L_{mid})$$

The radius of the forward hull-section, Rfwd, for a given axial coordinate, x, is defined as a modified semi-ellipsoid (Eq. 1.2):

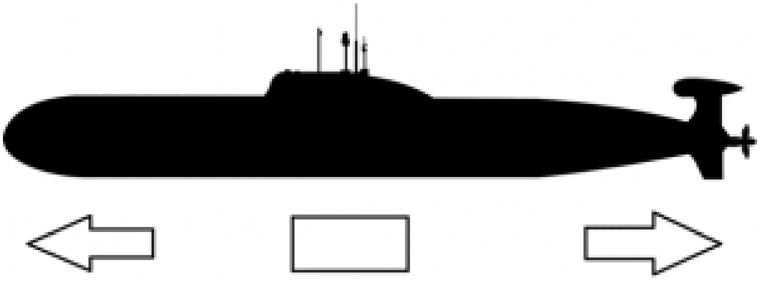
(1.2)

$$R_{fwd} = (D / 2) \{ [1 - (x - L_{fwd} / x)^{2}]^{n} \}$$

The radius of the aft hull-section, Raft, is defined as (Eq. 1.3):

(1.3)

$$R_{aft} = (D / 2) - \{ [(3D/2L_{aft}{}^{2} - \tan \alpha / L_{aft}) (x - L_{fwd} - L_{aft})^{2}] \}$$



FORWARD-BODY MID-
BODY AFT-BODY

Figure 1.5 Jackson hull-form geometry. [Adapted from Open Clipart Vectors by pixabay (Public Domain Image)]

The Myring hull-form is similar to the Jackson hull-form. However, the semi-angle of the aft section provides the naval architect with the ability to account for stern flows effects due to the geometry of the hull-section. The use of coatings on the Myring hull-form has yet to be investigated as a potential disruptive technology that could changes the characteristics of skin friction resistance and reduced biofouling.

Hull coatings and roughness is significant when considering the motion of UUVs. Hull coatings minimize the skin friction component of resistance and prevent fouling of the surface. Tin-based coatings have been used regularly in marine applications to prevent fouling but are detrimental to the environment. Therefore, disruptive technologies are focused on providing environmentally-friendly coatings such as electrochemically active coatings that allow the injection of boundary interfaces with bubbles so that an air cushion can be activated under certain conditions to reduce friction and disrupt the fouling process. Investigations into the texture of coating/hull surfaces will need to be conducted to emulate the skin of marine mammals so that friction and fouling is minimized or eliminated completely.

Superconducting Electric Motors

Electric motors are very efficient, but superconducting electric motors are highly efficient (~ 99%). This allows them to reduce operating costs of UUVs and reduce emissions. Superconducting motors are smaller in size, typically developing power per weight in the region of 30 kW/kg compared to standard electric motors ~ 5 kW/kg. High temperature superconductors discovered in 1986 are useful for developing this technology, but the discovery of magnesium diboride as a superconducting material in 2001 means that its lower critical temperature and sensitivity to magnetic fields will need to be adapted for use in rotating electrical machinery. The potential advantages of this disruptive technology include very low losses in electrical machines such as motors and the size and weight of the motor compared to traditional electric motors is much lower. However, the technology is yet to be proven at sea.

Conclusions: Naval Architect’s Role

The role of the naval architect is becoming increasingly complex and broad especially when one considers the effects of extreme weather and the minimization of using the earth’s scarce resources (Lewis, 1988). The future naval architect will need to work with natural scientists, such as marine biologists, in order to design vessels that work with nature to minimize the impact on the natural world (Hughes, 2010). The role will continue to work with engineers from other disciplines, project managers and business administrators and we may see the development of new academic courses that blend the principles of naval architecture with business studies that includes the commercial aspects of UUVs such as ‘naval systems architecture’ or ‘marine systems engineering’ (MAN Energy

Solutions, 2018). The UUV must be considered as a system in order to design an environmentally beneficial craft. This means that the design, operation, and maintenance of the UUV is an integrated system, and that the naval architect needs to fully understand the operational and engineering principles that form the systems architecture of UUVs. The potential integration of disruptive technologies into the design of UUVs provides opportunities to further advance the field of underwater systems especially in the current political and economic climate.

Questions

- What are the drivers for change in terms of using new fuels for propulsion units in UUVs?
- Name and explain the key international regulations that support the design and operation of submersibles and other forms of UUVs.
- Describe the disruptive technology driving the development of diesel engines and explain why the Miller thermodynamic cycle better than the Diesel cycle in the context of disruptive technologies applied to diesel engines?
- Discuss and describe the current disruptive technologies that affect the design, maintenance, and operations of UUVs.
- The choice of fuel is dependent on the type of prime mover used in a UUV. What are the environmental benefits of using biofuels, LNG, and hydrogen?
- What is hybrid propulsion? Name its advantages and disadvantages.
- Comment on the design a the UUV’s hull section and the naval architect’s role in designing UUVs subjected to future disruptive technologies.
- What are the advantages and disadvantages of using superconducting electric motors in UUVs?

References

American Bureau of Shipping. (2019). *ABS Rules for Building and Classifying Underwater Vehicles, Systems and Hyperbaric Facilities*. Houston, Texas: American Bureau of Shipping.

Button, R. W. (2009). *A Survey of Missions for Unmanned Undersea Vehicles*. Santa Monica, California, USA: RAND Corporation.

Department of Defense. (2011). *Unmanned Systems Integration Roadmap*: 2011 – 2036. Washington DC, USA: US Government.

Department of Defense. (2012). *Sustaining US Global Leadership: Priorities for the 21st Century Defense*. Washington DC, USA: US Government.

Department of the Navy. (2004). *The Nay Unmanned Undersea Vehicle Master Plan*. Washington DC, USA: US Government.

Hughes, O. F. (2010). *Ship Structural Analysis and Design*. New York, USA: Society of Naval Architects and Marine Engineers.

Lewis, E. V. (1988). *Principles of Naval Architecture: Volumes I, II and III*. New York, USA: Society of Naval Architects and Marine Engineers.

MAN Energy Solutions. (2018). *Basics of Ship Propulsion*. Berlin, Germany: MAN.

Nichols, R. K. (2020). *Unmanned Vehicle Systems and Operation on Air, Sea and Land* (Vol. IV). Manhattan: New Prairie Press.

US_Congress. (2020). *Navy Large Unmanned Surface and Undersea Vehicles: Background and Issues for Congress (Report* 45757). Washington DC: US Congress.

2. Automation & Human-Machine Symbiosis [Mumm]

Student Learning Objectives – The student will gain knowledge of the concepts and framework as it relates to the symbiosis of humans and machines and how this once futuristic idea is now a reality.

A Look Back at the Machine and Human Symbiosis Evolution

The idea that humans and machines would someday become interdependent upon one another was once considered science fiction and useful material for Hollywood films; however, it was not a scenario based on reality. This has all changed, and the interdependence of the human race on machines is becoming an integration that we can no longer ignore.

The Biology Dictionary lists the definition of symbiosis as "an evolved interaction or close living relationship between organisms from different species, usually with benefits to one or both of the individuals involved". (Symbiosis Definition, 2020). See Figure 2.1.

Figure 2.1 Robot and Human Connecting (Middleton, 2018)

For this discussion, the humans are creating the autonomous systems (robots) for the benefit of the human race, which is deemed as an obligation in symbiosis in "which case the relationship between the two species is so interdependent, that each of the organisms is unable to survive without the other" (Symbiosis Definition, 2020). The case for an obligated symbiotic relationship can be made here as a 'facultative' relationship is based in the ability of the connection to be created by choice, because one entity can live without the other. In the year 2020 and beyond, it is clear humans have created a world where machines are essential to human survival. This survival is seen in many forms from daily activities, healthcare to national security and warfare as discussed in November of 2020 by the head of the British Army, General Sir

Nick Carter, as he is forecasting “Thirty thousand “robot soldiers” could be fighting alongside humans in the near future as the British Army is forced to modernize” (Duncan, 2020). This would include small drones, unmanned ground vehicles, and unmanned underwater vehicles.

A look at how the human race is becoming more of a cyborg or a cyber organism is discussed from the lens of this being an endosymbiosis relationship “occurring when one of the symbiotic partners lives within the body of the other” (Symbiosis Definition, 2020).

The study of organic life and how it evolves is steeped in history, scientific theories, and documentation. This is in stark contrast to the very recent evolution of artificial intelligence and artificial life. In order to achieve full symbiosis between humans and machines

“may require that truly human-like characteristics be developed in intelligent machines. Such machines not only should be capable of human-like thinking, reasoning, and problem solving, but also should be capable of displaying human-like motivation, emotion, and personality, among other things.

Little is known about how a system will evolve over time and how this evolution will act and react in human settings such as the workplace and our overall society” (Sun, 2020).

The Fifth Industrial Revolution

Changes take time, resources, and evolutionary reasoning towards the betterment of humanity or a radical shift in our daily lives introduced in small measures. This pace of change is speeding up, and the time between shifts is shrinking, yet the effects of the change are magnified without a clear understanding of the consequences of actions and the reactions they cause. The fifth revolution will “take away mundane and repetitive tasks; it opens the way to curiosity, creativity, empathy, and judgment, ensuring a balance between people and technology” (Joseph, 2020). The rate of change will dwarf that of the past as the definition of the new revolution will herald that in “the Fifth Industrial Revolution, humans and machines will dance together, metaphorically” (Gauri, 2019). In a September 2020 article of *The National*, Patrick Noack states:

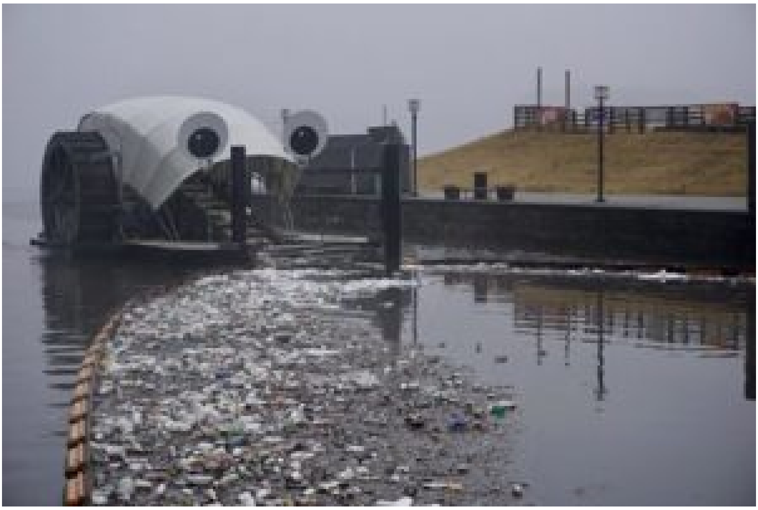
The speed of this revolution is unprecedented, and the impact is relevant to more and more people in increasingly diverse ways…the first of the revolutions lasted about 200 years. The second lasted 100, while the third about 50. It is easy to see the pattern here…during the fourth (revolution) we are hyperconnected through our smart devices to most of the planet. The fifth revolution will make that connection closer and seamless and will feel unmediated. The smart device on which we tap and into which we speak will disappear. Brain-computer interfaces will replace them. (Noack, 2020).

The aviation and maritime industries are steep in the history of humans and machine as the industrialization of our societies spread across the world. It was first the naval industry and later the aviation industry that allowed commerce to blossom and affordable travel to take hold. The change seen in these industries drove innovation, yet profit was the goal; this hallmark is what defines the shift as humanity "needs a Fifth Industrial Revolution to flower like a new Renaissance Age. It will be marked by creativity and common purpose, as we together work to bend progress and profits toward purpose and inclusivity" (Gauri, 2019).

Consider the motivations of innovations such as "Mr. Trash Wheel" as seen in Figure 2-2, as it depicts human-like qualities even though it is a sustainably powered trash interceptor invented in Baltimore, Maryland.

"Mr. Trash Wheel helps to connect the dots and helps residents understand the impact of their actions," said Rebecca Woods, executive director of Baltimore's Environmental Control Board. "Mr. Trash Wheel provides a point of education for upstream efforts in helping residents understand what happens to trash that enters streets and then storm drains. Woods said. "Mr. Trash Wheel (Figure 2.2) is that friendly face that provides my son comfort that trash will be blocked from entering the harbor. To my son, Mr. Trash Wheel is a hero" (Kossakovski, 2018).

Figure 2.2 Mr. Trash Wheel (Kossakovski, 2018)



The project offered a purpose greater than profit, as the amount of trash that is in harbors, docks, and even the open ocean is staggering. "Plastic, tires and other trash routinely flow into the harbor through the city's storm sewers". This innovation allows for more than just environmental cleanup; and it provides for profits towards a purpose of inclusivity as Mr. Trash Wheel "has collected more than 1.5 million pounds of trash since May 2014. It is powered by the harbor's current and solar panels" (Kossakovski, 2018).

The fifth industrial revolution is poised to push the fourth revolution into the history books and take over sooner than one might think. Our preferred mode of communications moves from cell phones to brain waves, our data collection from the internet of things to 3-D sensor collection, allowing artificial intelligence freedom to roam far past our understanding. We might "check-in at the airport using a mind-reading bracelet or do our mind-supported shopping to guarantee our safety from infectious viruses... our use of these technologies will lay the foundations for yet a new revolution. What might the Sixth Industrial Revolution hold?" (Noack, 2020)

.

Human and Machine Joined – Cyborg or Evolutionary Inevitability?

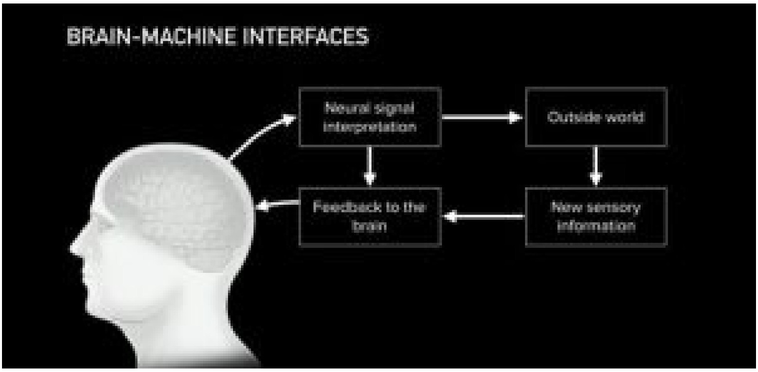
Who would have ever thought that the television program "The Six Million Dollar Man" would not only become reality, but it would also be looked at as rudimentary in our evolution of integrating machines into humankind to improve our quality of life and ultimately extend our lives? The definition of a cyborg is "a person whose physiological functioning is aided by or dependent upon a mechanical or electronic device" (Cyborg, 2020) or basically a bionic human or animal. Now the real question becomes, do machines evolve past humankind, becoming not only more intelligent but also self-aware and more like humankind?

Will robots continue to learn and study humans and their evolution for the purpose of evolving past humanity? What is not apparent is the pace at which authorities, responsibilities, strategic plans, and policies must change and evolve in order to help organizations understand their role in shaping a positive, proactive future.

The threat of unchecked technology, unmanned architecture development, and the ability to weaponize unmanned systems continues to evolve. Unmanned architecture technology advancements have offered more sophisticated abilities with cost-effective designs that have reduced the entry barrier for consumers, businesses, enemy states, and terrorist organizations. (Nichols, et al., 2019).

Elon Musk's company, Neuralink, is working on creating a brain to machine interface which will allow for an integrated brain-machine symbiosis with thousands of channels to take advantage of the power of artificial intelligence. Musk has described it as a "Fitbit for your brain" and is envisioning that a robot will do the entire surgery to fit this coin-sized device into your brain. Musk admits that the ethical and safety issues will drive some of the early public's adoption.

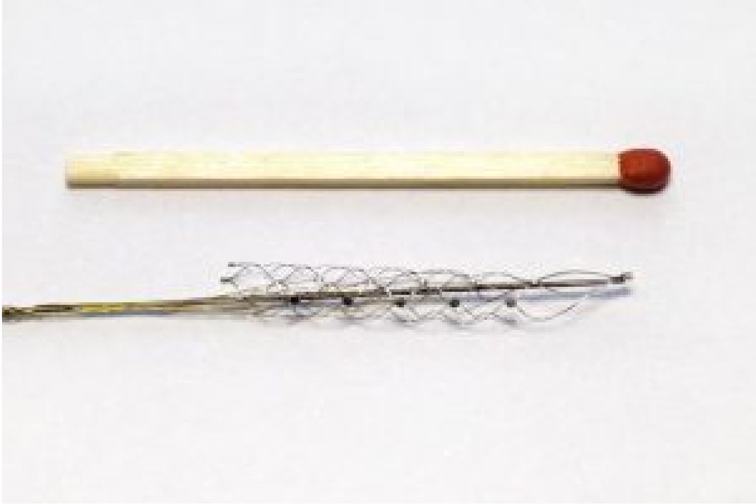
Figure 2.3 Neuralink Interface Process (Gilbert, 2019)



The device would read your brain through the interface as it is "connecting electrodes throughout the brain and reading its neuron signals en masse. (Figure 2.3) Gathering huge amounts of data from the signals would eventually teach Neuralink's software how the brain uses them to communicate with the rest of the body" (Ioannou, 2020). Musk is quoted as stating, "It's not just a measure of computerizing your brain, but a measure of potentially fixing complex neurological problems. "I think there's an incredible amount we can do to solve brain disorders and damage" (Gilbert, 2019).

Reports published in the Journal of NeuroInterventional Surgery are hailing the first time a Stentrode device has allowed a human to control a computer by using their mind, without wires or machine intervention. The device is inserted into the brain via a small keyhole incision (Lavars, 2020). Figure 2.4 shows the device next to a matchstick. The patient, Phillip O'Keefe, has had a Stentrode device implanted and

Figure 2.4 Stentrode device compared to a matchstick (Lavars, 2020)



the implant records his brain activity and transmits it wirelessly to a small receiver worn on his chest, and onward to a computer that translates the signals into onscreen commands… to surf the internet, write emails, do part-time work in data entry, and check his online banking. By thinking about moving his left ankle, he is able to perform a mouse click (Lavars, 2020).

This incredible symbiosis offers us a glimpse into the idea that "technology will bend back towards the service of humanity, marked by creativity and a common purpose…empower(ing) us to close the historic gap and create a new socio-economic era" (Joseph, 2020).

Cyborgs and cyborg soldiers of all forms and fashion are featured in Hollywood movies and Sci-Fi novels. These cyborg soldiers are no longer characters in sci-fi thrillers. As depicted in Figure 2.5, the troops of the future will have computers embedded in their craniums. The Defense Advanced Research Projects Agency (DARPA)

Figure 2.5 Mind-Controlled Troops Connected to Weapons Systems (West, 2018)

is selecting teams to develop a "neural interface" that would both allow troops to connect to military systems using their brainwaves and let those systems transmit back information directly to users' brains. The Next-Generation Non-Surgical Neurotechnology, or N3, program aims to combine the speed and processing power of computers with humans' ability to adapt to complex situations, DARPA said. In other words, the technology would let people control, feel, and interact with a remote machine as though it were a part of their own body (West, 2018). (See Figure 2.6)

Figure 2.6 Mockup of U.S. SOCOM's TALOS suit (Rempfer, 2019)

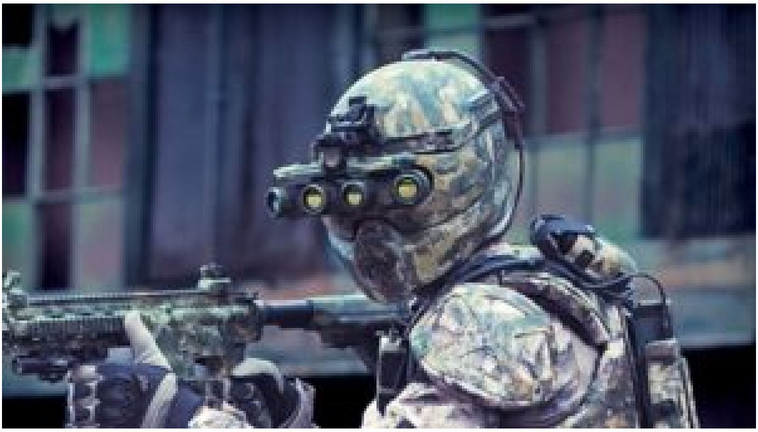
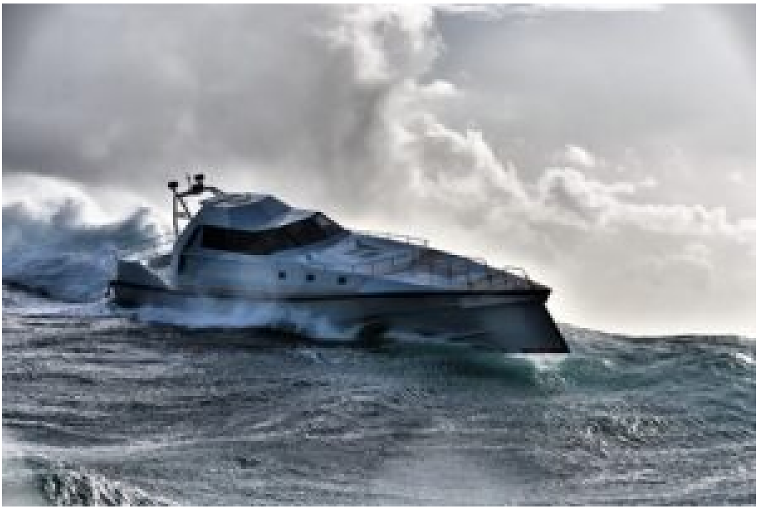


Figure 2-6 illustrates the future soldier with additional sensors to allow the soldier to autonomously send and receive information. The implications of a machine talking directly into a human mind in the middle of a high stress, highly emotional situation such as combat is not understood or even discussed within most available literature. The consequences to the human or to the battlefield are not known as "these interactions would allow warfighters direct communication with unmanned and autonomous systems, as well as with other humans, to optimize command and control systems and operations" (Rempfer, 2019). All of this is with a questionable ability to interject ethics and with minor regard as to what long term effects it will have on the human soldiers.

Traversing the Seas with New Autonomous Technologies

The seas are generally regarded as a very unforgiving place where a mix of factors from weather to technology combined with the operator's experience will determine success or failure in successful navigation or just surviving this environment. Future Defense USA in Alexandria, Virginia, is developing an optionally piloted advanced technology vessel known as the Thunderchild to the defense market and later to the civilian arena. The boat will be outfitted with complimentary autonomous systems based on the customers' requirements (DiDonato, 2020). (Figure 2.7)

Figure 2.7 The Thunderchild (Kowalski, 2020)

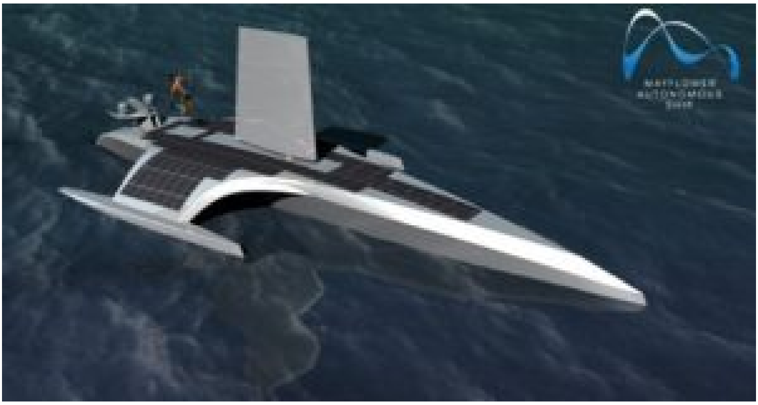


The Thunderchild already holds world records for speed in navigation, and with the ability to operate in sea state six, which encompasses wind speeds over 25 knots, and wave heights of over 3 meters, this capability allows the Thunderchild to operate where most of the worlds Coast Guards and Navies are not able to. This technology will have the ability to be optionally piloted, allowing for maximum flexibility for manned operations when required or unmanned operations to take advantage of the advances in communications, navigation, and a lower operating cost than currently available (DiDonato, 2020).

Surface vessels are quickly moving to full autonomy with the help of some large IT companies. IBM has invested in moving autonomy forward with its Mayflower Autonomous Ship (MAS). It is currently sailing and is slated to re-trace the original 1620 Mayflower sea route to commemorate the 400th anniversary of the Mayflower ocean voyage. MAS will use IBM's advances in AI and edge computing (Figure 2.8):

to sense, think and make decisions at sea, even with no human intervention… with no human captain or onboard crew, it will become one of the first full-sized, fully autonomous vessels to cross the Atlantic. The mission will further the development of commercial autonomous ships and help transform the future of marine research." (IBM News Room, 2020)

Figure 2.8 MAS (IBM News Room, 2020)

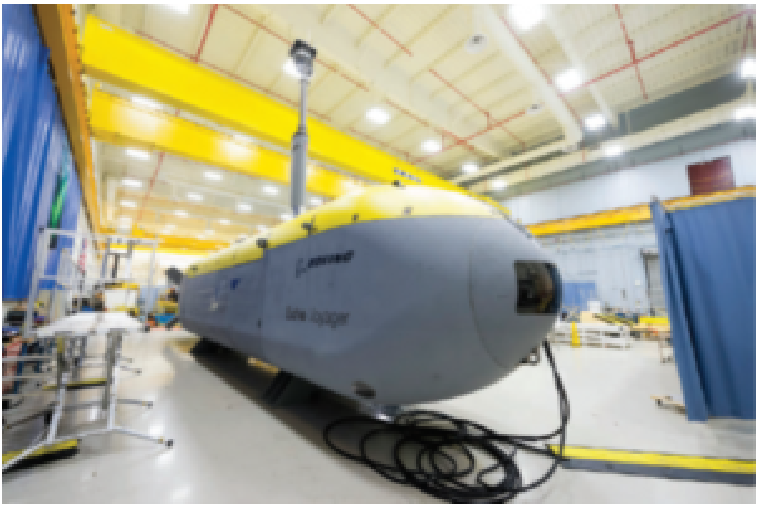


Unmanned underwater vehicles (UUVs) will be used for logistics, research, and offensive and defensive weapons. The US Navy is working quickly to increase its offensive undersea drone capabilities as

“The maritime domain has yet to see the kind of explosive innovation that UAVs have brought to land warfare… autonomous systems promise to bring to the undersea domain the kind of new capabilities and offensive punch, the Navy has yet to fully tap their potential” (Frandrup, 2019).

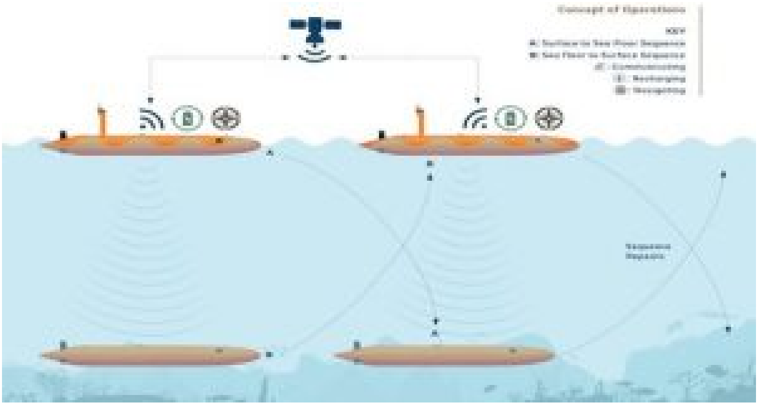
The new era of unmanned submarines and the implications of where the technology will lead humankind is under “The influence of massive spending on developing AI for undersea systems portends the greatest change in military sea power since the introduction of nuclear-powered vessels”. (Wilson, 2019) See Figure 2.9.

Figure 2.9 Boeing Echo Voyager Extra-Large Unmanned Underwater Vehicle (XLUUV) (Wilson, 2019)



The research missions of UUVs are countless, yet they have their limitations. Terradepth, a Texas company, is working on solving the power and longevity issues that plague many research missions. Terradepth is working on a tag-team design of an unmanned submersible they named AxV. (Figure 2.10)

Figure 2.10 Diagram illustrating the Terradepth system (Coxworth, 2020)

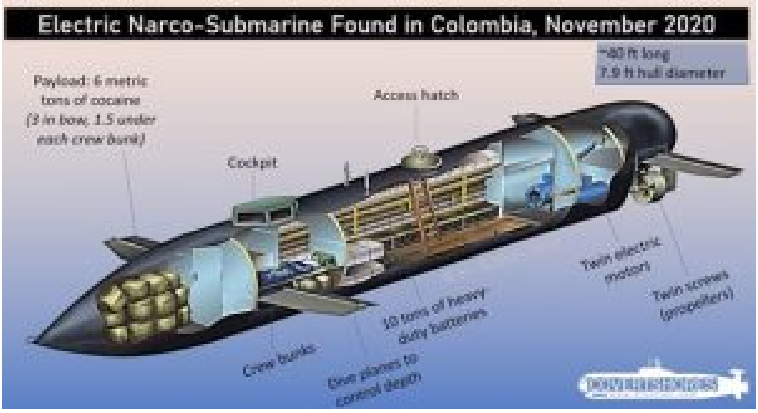


The submerged AxV likewise gathers *undersea* data, running purely on battery power. When that battery starts getting low, the vehicle automatically surfaces near its counterpart. It then fires up its generator and starts recharging its battery, while the AxV that *had* been traveling at the surface submerges to take its place underwater (Coxworth, 2020).

Terradepth has had such successful sea trials of the technology in November 2020 that they are continuing to expand the capabilities beyond the current depth of 6,000 meters. The next power solution set they are working to incorporate is an air-breathing hydrogen fuel cell system.

Technology can be used for good or evil; it just depends on how the technology is employed. In November 2020, the US Drug Enforcement Agency (DEA) captured a hard to detect narcotics carrying submarine near Choco, Colombia. (Figure 2.11)

Figure 2.11 Electric Narco-Submarine (Sutton, 2020)


Electric Narco-Submarine Found in Colombia, November 2020
~80 ft long
7.9 ft hull diameter
Payload: 6 metric tons of cocaine (3 in bow, 1.5 under each crew bunk)
Access hatch
Cockpit
Twin electric motors
Twin screws (propellers)
10 tons of heavy duty batteries
Crew bunks
Dive planes to control depth

This "fully submersible electric-powered submarine makes it very hard to trace. The vehicle was capable of carrying 6 tons of cocaine. The street value of such a huge amount stands at an estimated $120 million USD" (Kundu, 2020). Although not unmanned yet, it is clear to see that the narco-traffickers are working on undersea logistics to move their products. It will only be a matter of time before they add unmanned underwater vehicles to their fleet.

Advancement in unmanned submersibles is tied directly to the improvements in the AI field. AI vessels are not just being limited to nefarious uses; many governments are working on broadening mission sets for national defense. China has made "achievements in AI-enabled unmanned surface vessels, which it plans to use to patrol and bolster its territorial claims in the South China Sea. It has also tested unmanned tanks as part of research efforts to integrate AI into ground forces" (Tadjdeh, 2020).

It is clear that the symbiosis of human and machine to harness the power of the seas is quickly approaching; technology laws, policies, and governance still have a long way to go before man and machine can claim victory.

Human Symbiosis Disrupts the Aviation Industry

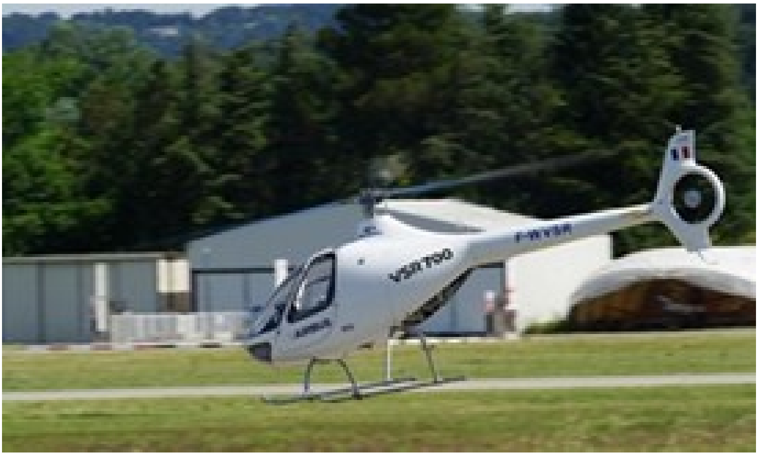
In examining the idea of human symbiosis and the aviation industry, most thoughts immediately go to UAVs or drone type aircraft. However, the optionally piloted aircraft/vehicle (OPV) allows for the symbiosis in a more trusting and understood manner. If an aircraft is only able to be flown by the computer itself, and no human intervention is possible when a fault occurs, humans quickly start to distrust the sensors, computers, and AI systems. Nowhere is this example clearer than that of the Lion Air and the Ethiopian Airline Boeing 737-Max 800 aircraft crashes that occurred respectively in 2018 and 2019.

A preliminary report from Indonesian investigators indicates that Lion Air 610 crashed because a faulty sensor erroneously reported that the airplane was stalling. The false report triggered an automated system known as the Maneuvering Characteristics Augmentation System, or MCAS. This system tried to point the aircraft's nose down so that it could gain enough speed to fly safely (Hawkins, 2019).

The sensors that were supposed to create a human symbiosis with the aircraft ended up creating confusion and causing the crash of two airliners, killing 346 persons, and grounding the entire fleet of aircraft. The cost to Boeing and the airline industry is in the billions, the FAA lifted the grounding order for the 737 Max as of December 3, 2020.

The ability to have an optionally piloted helicopter has been demonstrated by Airbus in 2017. Airbus has stated that the "The OPV (Figure 2.12) is able to autonomously take-off, hover and perform stabilized flight and maneuvers…VSR 700 flight control system is a fully-digital, multi-channel system with a very high level of redundancy. It takes advantage of Airbus Helicopters unique expertise in digital autopilots" (VSR700 demonstrator performs first autonomous flights, 2017).

Figure 2.12 VSR 700 OPV (VSR700 demonstrator performs first autonomous flights, 2017)



Boeing is working diligently in the arena of OPVs that handle passenger traffic (Figure 2.13). In January of 2019, Boeing's unmanned passenger aircraft completed its first flight as it "tested the prototype's autonomous functions and ground control systems, according to Boeing. Subsequent test flights will check forward and wing-borne flight and the transition between vertical and forward flight modes" (Abel, 2019).

Figure 2.13 Boeing Unmanned Passenger Aircraft (Abel, 2019)

This OPV "was designed and developed in partnership with Boeing NeXt and Boeing subsidiary Aurora Flight Sciences. John Langford, president, and CEO of Aurora Flight Sciences, stated, "Certifiable autonomy is going to make quiet, clean and safe urban air mobility possible" (Abel, 2019). The next project for Boeing is reportedly an unmanned electric cargo aircraft that will carry up to 500 pounds.

Airbus is also working on a pilotless commercial jet. Airbus has been testing the aircraft and confirmed that "while completing alignment on the runway, waiting for clearance from air traffic control, we engaged the autopilot and the A350-1000 achieved eight automatic takeoffs over a period of four and a half hours" (Hardingham, 2020). See Figure 2.14.

Figure 2.14 A350-1000 Pilotless Commercial Aircraft (Hardingham, 2020)

Even without a fully pilotless aircraft, passenger jets are currently landing with the "assistance of on-board computers with pilots manually fly the aircraft for just a few minutes on average… Autonomous technologies are paramount to supporting pilots, enabling them to focus less on aircraft operation and more on strategic decision-making and mission management" (Hardingham, 2020).

Further into the future of aviation and human symbiosis is the promise of what is being called Ion Thrusters that allows flight without a liquid type fuel. See Figure 2.15.

Figure 2.15 Ion Thruster Rendering (IFL Science, 2020)

This technology is being created by a team led by Steven Barrett from the Massachusetts Institute of Technology (MIT), the "so-called electro aerodynamic-powered plane, one that uses solid-state propulsion, meaning no propellers or jet engines with expendable fuel" (IFL Science, 2020)

The idea of humankind and flying machines working together in a symbiotic relationship is moving further toward reality. The technologies and public policies that regulate this technology must align better in the future in order for humans to trust the machines and the machines, understanding their role in serving humanity.

Integrating Artificial Employees-The Changing Horizon of Human Resources

There is an old saying that all problems are people problems, which gives rise to the issue of employees in the fifth revolution as "we are unprepared to meet the challenges ahead. According to a recent World Economic Forum Report, for example, 65% of children entering the school system today will end up in careers that don't exist yet" (Gauri, 2019).

The study of organic life and how it evolves is steeped in history, scientific theories, and documentation. This is in stark contrast to the very recent evolution of artificial intelligence and artificial life. Little is known about how a system will evolve over time and how this evolution will act and react in human settings such as the workplace and our overall society. Can a virtual or physical robot (autonomous system) truly understand the needs, emotions, and motivations of a human? If this is possible using AI, the autonomous systems "can anticipate what a human will need and will do, it can provide better assistance. Furthermore, if it can appreciate, for example, the frustration that a human feels, then it can help to find solutions" (Sun, 2020).

The potential risk for " loss to an organization from an Artificial Employee (AE) making autonomous decisions is enormous" (Brand, 2019). The Canadian Chief Scientific Officer of Kindred Biomedical states, "A subset of the artificial intelligence development in the next few decades will be very human-like. I believe these entities should have the same rights as humans…robots fundamentally have to make mistakes in order to learn" (Wong, 2017). The risk could potentially be every bit as great as that of human error. Research in this area tends to use the Grounded Theory as it lends itself well to organizations and human resource issues. The grounded theory research approach "presents promising possibilities for the development of theoretical frameworks that emerge from research situated in practice and enhance the Human Resource Development (HRD) theorist" (Egan, 2002). There appears to be very few organizations with a plan for increasingly autonomous machines capable of deep learning, as

"these machines are considered physical assets as opposed to intelligence assets" (Brand, 2019). Machines do not have the same issues as humans who have self-determined and intrinsic motivations and thus are capable of autonomous choice of action in accordance with these motivations…include not only power, achievement, and other individualistic tendencies, but also adherence to social norms, affiliation with other individuals, and other tendencies related to social cooperation and interdependence" (Sun, 2020).

Most corporations adopt risk management, ethics, or training and development plans for human employees. By contrast, machines with any level of intelligence are considered physical assets and are managed as such. However, a thinking machine is capable of choices, actions, and decision making, much like that of its human counterpart. If a machine can make an autonomous decision or action, "the behavior of the machine must be managed and responsible for outcomes assigned" (Brand, 2019). If so, training, monitoring, and development programs must be considered for managing the AEs in many of the same ways human employees are managed. On a deeper level, human and machine resources must be observed and managed in their interactions. The machines that will make thinking decisions could have much broader implications and the humans that interact with them will respond based on human needs and human concerns.

Any organization relying on a human to make an intelligent decision has some employee oversight system in place. An entire field of employment and research is dedicated to the complex task of managing humans and their decisions. The hypothesis is an equally in-depth system of management is called for when managing intelligent machines, with a focus on differences in the decision making and task completion methodology. In Ethical Dilemmas in the Age of AI, Abramson states, “In the distant future, some machines may have to make decisions for humans. In the case of empathy, imagine a robot having to decide if resuscitation attempts on a deceased human should be undertaken, and if so, for how long?” (Abramson, 2016).

In January 2017, and again in 2018, the European Union passed a motion adopting a report that calls for the development of “electronic personhood” – regulations for robots and AI systems “granting special legal status, or “electronic personalities,” to smart robots, specifically those which can learn, adapt, and act for themselves (Withers, 2018). Although this legislation has not passed yet, it appears that it will be approved in the next few years as countries and companies start to tackle the issue of leveraging Artificial Employees.

There are far too many issues and questions to address in this chapter, however, as a parting thought on this topic, consider what happens if a human goes on vacation – who monitors the AE? What is liability for a mistake by the AE? What about AE maintenance? How do you terminate an AE? Is it a loss to the company/ government, or is it employee replacement? What could a company potentially lose or be liable for?

Conclusions

Additional theoretical models and frameworks should be explored in this challenging environment with many complex issues that have yet to be discovered. Future research implementing these theoretical models and frameworks should be used to fill the knowledge gaps related to evolving approaches and innovative solutions that could complement the speed of human/machine progress. If a machine can make an autonomous decision or action, the behavior of the machine must be managed and responsible for the result.

The cyborg soldier of the future will “mentally link up with the various weapons systems at their disposal…this would also be a two-way system that could enable the systems to transmit information back to the soldier as well" (West, 2018). If so, training, monitoring, and development programs must be considered for managing the symbiosis of human and machines in many of the same ways we manage human employees. A broad range of cognitive architectures needs to be investigated as the human mind "needs to deal with all of its functionalities: perception, categorization, memory, decision-making, reasoning, problem-solving, communication, action, learning, metacognition, motivation, and so on" (Sun, 2020). The demand for AI and human symbiosis models capable of working with these broad functionalities needs to be better scoped for future research and integration if we are to hope for true human-machine symbiosis.

Time will tell if the human resources, maritime, and aviation industries can all successfully adjust into this new world. Human-machine symbiosis appears to be just over the horizon; it will also require guidance to incorporate the correct mix of policies and laws to support a complimentary partnership to this new reality instead of a hindrance.

Questions

1. What is the difference between symbiosis and the industrial revolution?
2. Do you think human evolution will migrate to us all being cyborgs? Why or Why not?
3. List three disruptive technologies in the aviation industry.
4. How would you to take advantage of the disruptive nature of the fifth industrial revolution and human symbiosis?
5. Name three ways that the maritime industry is benefiting from the fifth industrial revolution and the inclusion of human symbiosis in next-generation technologies.

References

Cyborg. (2020, December 8). *Cyborg.* Retrieved from https://www.dictionary.com/browse/cyborg: https://www.dictionary.com/browse/cyborg

IFL Science. (2020, December 10). *Scientists Have Created A Star Trek-Like Plane That Flies Using "Ion Thrusters" And No Fuel.* Retrieved from https://www.iflscience.com/technology/: https://www.iflscience.com/technology/scientists-have-created-a-star-treklike-plane-that-flies-using-ion-thrusters

Abel, K. (2019). *Boeing's Unmanned Passenger Aircraft Completes First Flight. South Sound Business.* Retrieved from https://southsoundbiz.com/: https://southsoundbiz.com/boeings-unmanned-passenger-aircraft-completes-first-flight/

Brand, K. (2019, December 7). *Research in Artificial Employee Management.* . Retrieved from www.kathrynbrand.com: www.kathrynbrand.com

Coxworth, B. (2020, December 10). *Place-trading* AUVs *designed for longer oceanographic missions.* Retrieved from https://newatlas.com/: https://newatlas.com/marine/terradepth-axv-auv/?utm_source=New+Atlas+Subscribers&utm_campaign=1a2437bb47-EMAIL_CAMPAIGN_2020_12_10_02

DiDonato, R. (2020, December 12). *Future Defense* USA *[Interview].* Retrieved from https://www.futuredefenseamd.com/: https://www.futuredefenseamd.com/

Duncan, C. (2020). *Thousands of 'robot soldiers' could be fighting in British army in near future*, UK *military chief says.* Retrieved from https://www.independent.co.uk/: https://www.independent.co.uk/news/uk/politics/robot-soldiers-british-army-nick-carter-https://www.independent.co.uk/news/uk/politics/robot-soldiers-british-army-nick-carter-b1705452.html

Egan, T. M. (2002). Grounded Theory Research and Theory

Building. *Advances in developing human resources* , pp. 4(3), 277-295. .

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

Gauri, P. &. (2019, May 5). *What the Fifth Industrial Revolution is and why it matters.* . Retrieved from https://europeansting.com/: https://europeansting.com/2019/05/16/what-the-fifth-industrial-revolution-is-and-why-it-matters/

Gilbert, B. (2019). *Elon Musk finally took the wraps off his new brain microchip company that plans to connect people's brains to the internet by next year.* Retrieved from https://www.businessinsider.com/: https://www.businessinsider.com/what-is-elon-musk-brain-chip-company-neuralink-2019-7

Hardingham, T. (2020). *Are we one step closer to pilotless commercial jets?* . Retrieved from https://www.cnn.com/: https://www.cnn.com/travel/article/airbus-pilotless-commercial-jets/index.html

Hawkins, A. (2019). *Everything you need to know about the Boeing 737 Max airplane crashes.* Retrieved from https://www.theverge.com: https://www.theverge.com/2019/3/22/18275736/boeing-737-max-plane-crashes-grounded-problems-info-details-explained-reasons

IBM News Room. (2020, December 12). *Sea-Trials-Begin-for-Mayflower-Autonomous-Ships-AI-Captain.* Retrieved from https://newsroom.ibm.com/: https://newsroom.ibm.com/2020-03-05-Sea-Trials-Begin-for-Mayflower-Autonomous-Ships-AI-Captain

Ioannou, L. (2020, Dec 7). *Elon Musk demonstrates brain-computer tech Neuralink in live pigs.* Retrieved from https://www.cnbc.com/: https://www.cnbc.com/2020/08/28/elon-musk-demonstrates-brain-computer-tech-neuralink-in-live-pigs.html

Joseph, T. (2020). *How the 5th Industrial Revolution is Advancing*

Humanity at Workplace. Retrieved from https://www.fingent.com/: https://www.fingent.com/blog/how-the-5th-industrial-revolution-is-advancing-humanity-at-workplace/

Kossakovski, F. (2018, December 6). *Mr. Trash Wheel cleans up Baltimore Harbor with a dash of humor.* Retrieved from https://www.pbs.org: https://www.pbs.org/newshour/science/mr-trash-wheel-cleans-up-baltimore-harbor-with-a-dash-of-humor

Kundu, A. (2020, November 24). *DEA catches stealthy narco submarine in Colombia.* Retrieved from https://www.fleetmon.com/maritime-news/: https://www.fleetmon.com/maritime-news/2020/31729/dea-catches-stealthy-narco-submarine-colombia/

Lavars, N. (2020, December 7). *Brain implant allows mind control of computers in first human trials.* Retrieved from https://newatlas.com/: https://newatlas.com/medical/stentrode-brain-implant-mind-control-first-trials/#:~:text=in%20the%20neck-,Stentrode%20was%20implant

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/

Nichols, R. K., Mumm, H. C., Lonstein, W. D., Ryan, J. J., Carter, C., & and Hood, J.-P. (2019). *Unmanned Aircraft Systems in the Cyber Domain.* Manahattan, KS: New Prairie Press. Retrieved from https://newprairiepress.org/ebooks/27/

Noack, P. (2020, December 9). *The Fifth Industrial Revolution: where mind meets machine.* Retrieved from https://www.thenationalnews.com/: Noack, P. (2020). The Fifth Industrial Revolution: where mind meets machine. The National News(August 9 2020). https://www.thenationalnews.com/opinion/comment/the-fifth-industrial-revolution-where-mind-meets-machine-1.1061280

Rempfer, K. (2019, November 27). *Cyborg warriors could be here* *by 2050, DoD study group says.* . Retrieved from https://www.armytimes.com/news/: https://www.armytimes.com/news/your-army/2019/11/27/cyborg-warriors-could-be-here-by-2050-dod-study-group-says/

Sun, R. (2020). Potential of full human–machine symbiosis through truly intelligent cognitive systems . *AI & Society*, pp. 35(1), 17-28. https://doi.org/10.1007/s00146-017-0775-7 .

Symbiosis Definition. (2020, November 18). Retrieved from https://biologydictionary.net/symbiosis/: https://biologydictionary.net/symbiosis/

Tadjdeh, Y. (2020, October 30). *China Threatens U.S. Primacy in Artificial Intelligence.* Retrieved from https://www.nationaldefensemagazine.org/: https://www.nationaldefensemagazine.org/Articles/2020/10/30/China%20Threatens%20US%20Primacy%20in%20Artificial%20Intelligence

VSR700 *demonstrator performs first autonomous flights.* (2017, December 17). Retrieved from https://www.airbus.com/newsroom/: https://www.airbus.com/newsroom/press-releases/en/2017/06/VSR700.html

West, N. (2018, December 8). *DARPA Researching Mind-Controlled Troops Connected to Weapons Systems.* Retrieved from https://www.thedailybell.com/: https://www.thedailybell.com/all-articles/news-analysis/darpa-researching-mind-controlled-troops-connected-to-weapons-systems

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

3. UAS Regulation / Innovation / Safety 2020 / Privacy and Beyond [Hood]

Student Learning Objectives

UAS Regulations keep changing. This chapter is designed to bring drone operators and enthusiasts up to date. This chapter is study only.

Two New FAA Rules That make a Difference

Two long awaited rules from the Federal Aviation Administration (FAA) regarding mandating remote identification (Remote ID) of drones and allow drone operators of “small” drones to fly over people and at night under certain conditions. The majority of following information was taken from the FAA Executive Summary and associated press release issued in December 2020.

As a parting gift to show that 2020 wasn’t all bad, the FAA released two long-awaited rules that will help push the drone industry into the future. The FAA’s ultimate goal is to enable routine drone operations in the same airspace as manned aircraft, but a lot of hurdles have to be cleared before that is possible. Like a game of Chutes and Ladders, many small moves and a couple of big ones are required to reach that goal, and along the way, there is an ever-present danger of sliding backwards. (Kiemen, 2021)

Figure 3.1. Embry-Riddle drone ready to fly by Scott Burgess, Embry-Riddle Aeronautical University. Source: Scott Burgess ERAU

These rules come at a time when drones represent the fastest-growing segment in the entire transportation sector – currently over 1.7 million drone registrations and 203,000 FAA-certified remote pilots. (Administration, 2020) See Figure 3.1

According to the FAA, Remote ID is a major step toward the full integration of drones into the national airspace system. Remote ID provides identification of drones in flight as well as location of their control stations, providing crucial information to our national security agencies and law enforcement partners, and other officials charged with ensuring public safety. Airspace awareness reduces risk of drone interference with other aircraft and people and property on the ground. (Administration, 2020)

Equipping drones with remote ID technology builds on previous steps taken by the FAA and the drone industry to integrate operations safety into the national airspace system. Part 107 of the federal aviation regulations currently prohibits covered drone operations over people and at night unless an operator obtains a waiver from the FAA. The new regulations jointly provide increased flexibility to conduct certain small UAS without obtaining a waiver. (Administration, 2020)

"The new rules make way for the further integration of drones into our airspace by addressing safety and security concerns," said FAA Administrator Steve Dickson. "They get closer to the day when we will more routinely see drone operations such as delivery of packages." (Administration, 2020)

As the rules are read and understood, it can be inferred which potential industries these new rules are aimed at effecting (or allowing) to move forward. Examples of such industries include delivery and transit services.

Remote ID

The remote ID Rule applies to all operators of drones that require FAA registrations. There are three ways to comply with the operational requirements:

1: Operate a standard Remote ID drone that broadcasts identification and location information of the drone and control station;

2: Operate a drone with a Remote ID broadcast module (may be separate device attached to the drone), which broadcasts identification, location, and take-off information; or

3: Operate a drone without Remote ID but at specific FAA-recognized identification areas.

(Administration, 2020)

Operations over People and at Night

This rule applies to Part 107 operators. The ability to fly over people and moving vehicles varies depending on the level of risk a small drone operation presents to people on the ground. Operations are permitted base on four categories

These Operations Categories consist of the following:

Category 1 eligible: small, unmanned aircraft must weigh less than 0.55, including everything on board or otherwise attached, and contain no exposed rotating parts that would lacerate human skin. No FAA-accepted Means of Compliance (MOC) or Declaration of Compliance (DOC) required.

Category 2 eligible: small, unmanned aircraft must not cause injury to a human being that is equivalent to or greater than the severity of injury caused by a transfer of 11 foot-pounds of kinetic energy upon impact from a rigid object, does not contain any exposed rotating parts that could lacerate human skin upon impact with a human being, and does not contain any safety defects. Requires FAA-accepted means of compliance and FAA-accepted declaration of compliance.

Category 3 eligible: small, unmanned aircraft must not cause injury to a human being that is equivalent to or greater than the severity of injury caused by a transfer of 25 foot-pounds of kinetic energy upon impact of a rigid object, does not contain any exposed rotating parts that could lacerate human skin upon impact with a human being, and does not contain any safety defects. Requires FAA-accepted means of compliance and FAA-accepted declaration of compliance.

Category 4 eligible: small, unmanned aircraft must have an airworthiness certificate issued under Part 21 of FAA regulations. Must be operated in accordance with the operating limitations specified in the approved Flight Manual or so otherwise specified by the Administrator. The operating limitations must not prohibit operations over human beings. Must have maintenance, preventive maintenance, alterations, or inspections performed in accordance with specific requirements in the final rule. (Administration, 2020)

Figure 3.2 EL PASO, TEXAS – NOVEMBER 20: DroneUp pilot Andrew Holbert prepares to launch a drone to deliver a COVID-19 self-collection test kit to a home, after being ordered from Walmart by a resident, amid a Covid-19 surge on November 20, 2020 in El Paso, Texas. Source: Photo by Mario Tama/Getty Images

Operating Rules

Operations at Night (See Figure 3.2)

- – Remote pilots in command who wish to conduct small, unmanned aircraft operations at night must complete either the updated initial test or the updated recurrent online training prior to conducting such operations.
- – Additionally, prior to conducting small, unmanned aircraft operations at night, the small, unmanned aircraft must be

equipped with anti-collision lights that can be seen for 3 statute miles and have a flash rate sufficient to avoid a collision. These anti-collision lights must be operational.

Operations Over People

- – **Category 1 eligible aircraft:**
  - o Small, unmanned aircraft must weigh less than 0.55, including everything on board or otherwise attached, and contain no exposed rotating parts that would lacerate human skin. Remote pilots are prohibited from operating a small, unmanned aircraft as a Category 1 operation in sustained flight over open-air assemblies unless the operation meets the requirements for standard remote identification or remote identification broadcast modules established in the Remote ID Rule.

(Administration, 2020)

- – **Category 2 eligible aircraft:**
  - o Remote pilots are prohibited from operating a small, unmanned aircraft as a Category 2 operation in sustained flight over open-air assemblies unless the operation meets the requirements for standard remote identification or remote identification broadcast modules established in the Remote ID Final Rule.
  - o Requires means of compliance and declaration of compliance by applicant.
- – **Category 3 eligible aircraft:**
  - o Must not operate the small, unmanned aircraft over open-air assemblies of human beings.
  - o May only operate the small, unmanned aircraft above any human being if operation meets one of the following conditions:

    - The operation is within or over a closed- or restricted-access site and all human beings located within the closed- or restricted-access site must be on notice that a small, unmanned aircraft may fly over them
    - The small, unmanned aircraft does not maintain sustained flight over any human being unless that human being is directly participating in the operation of the small, unmanned aircraft; or located under a covered structure or inside a stationary vehicle that can provide reasonable protection from a falling small, unmanned aircraft.
  - – **Category 4 eligible aircraft:**
    - o Must have an airworthiness certification issued under Part 21.
    - o Must be operated in accordance with the operating limitations specified in the approved Flight Manual or as otherwise specified by the Administrator. The operating limitations must not prohibit operations over human beings.
    - o Must have maintenance, preventative maintenance, alterations, or inspections performed in accordance with specific maintenance requirements detailed in the final rule.
    - o Remote pilots are prohibited from operating a small, unmanned aircraft as a Category 4 operation in sustained flight over open-air assemblies unless the operation meets the requirements of standard remote identification or remote identification broadcast modules established in the Remote ID Final Rule.

(Administration, 2020)

Figure 3.3 UAV and Drone Solutions monitoring aircraft
(Source: AOPA.org)

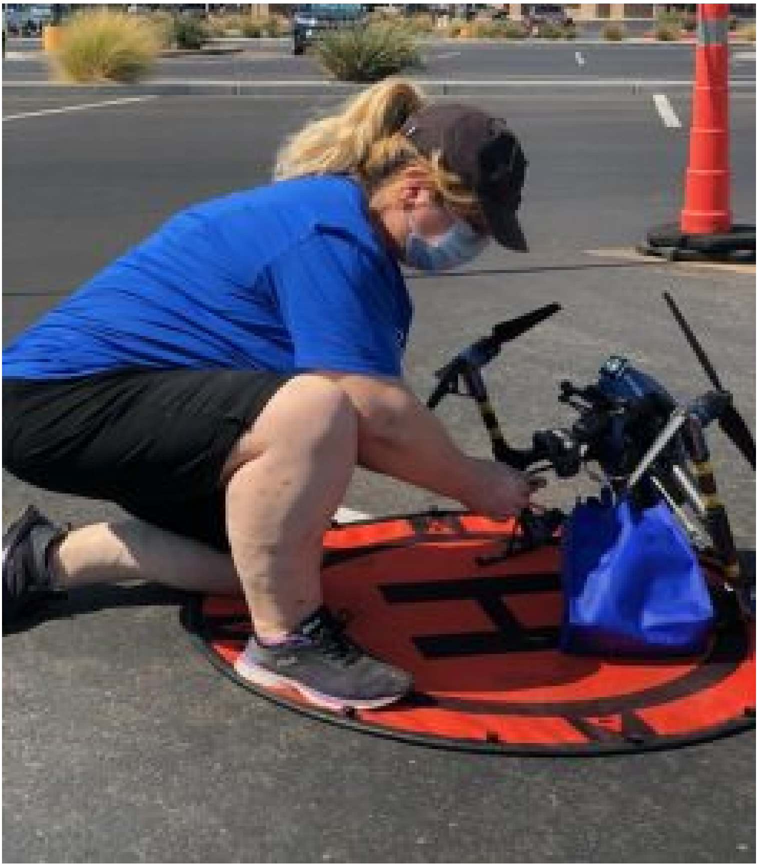
Operations over moving vehicles (See Figure 3.3)

- – Must be Category 1, Category 2, and Category 3, eligible to operate over people, may not maintain sustained flight over moving vehicles; transit operations only.
- – For an operation under Category 1, Category 2, or Category 3, the small, unmanned aircraft, throughout the operation –
    - o Must remain within or over closed- or restricted-access sites, and all human beings located inside a moving vehicle within the closed- or restricted-access site must be on notice that a small, unmanned aircraft may fly over them; or
    - o Must not maintain sustained flight over moving vehicles.
- – For a Category 4 operation, the small, unmanned aircraft must –
    - o Have an airworthiness certificate issued under part 21 of

this chapter.

- o Be operated in accordance with the operating limitations specified in the approved Flight Manual or as otherwise specified by the Administrator. The operating limitations must not prohibit operations over human beings located inside moving vehicles.

Figure 3.4. Las Vegas, NV, September 23, 2020. A DroneUp employee prepares a Covid-19 test kit for delivery. (Source: Joe Cerreta, Embry-Riddle Aeronautical University)



Remote Pilot Knowledge Test Changes (See Figure 3.4)

A remote pilot in command, owner, or person manipulating the flight controls of a small, unmanned aircraft system must:

- – Have in that person's physical possession and readily accessible the remote pilot certificate with a small UAS rating and identification when exercising the privileges of that remote pilot certificate.
- – Present his or her remote pilot certificate and identification upon request from the FAA, NTSB, TSA, or and Federal, state, or local law enforcement officer.
- – Make available, upon request, to the FAA and document, record, or report required to be kept under FAA regulations.
- – Upon request, must allow the FAA to test or inspect the small, unmanned aircraft system, the remote pilot in command, the person manipulating the flight controls of a small, unmanned aircraft system, and, if applicable, the visual observer to determine compliance with the rule. (Administration, 2020)

Design and production Rules for Manufacturers

- – Some existing Category 1 small, unmanned aircraft may meet the performance-based requirements to be eligible for Category 1 operations over people of this rule beginning the effective date of the rule (Those that have already been produced with propeller guards/shrouds that prevent the blades from causing laceration to human skin upon impact).
- – Manufacturers may bring to market retrofit propeller guards to install on existing small, unmanned aircraft to make them eligible for Category 1 operations over people beginning after effective date of this rule.

- – Some existing small, unmanned aircraft may meet the performance-based requirements to be eligible for Category 2 operations over people of this rule once FAA-accepted MOC and DOC are received.
- – Small, unmanned aircraft may meet the performance-based requirements for Category 2 of this rule upon FAA-Accepted MOC/DOC 9-12 months after the effective date of this rule.
- – Small, unmanned aircraft may meet the performance-based requirements for Category 3 of this rule upon FAA-Accepted MOC/DOC 9-12 months after the effective date of this rule.
- – Category 4 small, unmanned aircraft for operations over people may receive an airworthiness certificate beginning 6-12 months after the effective date of this rule.

Major Changes from Proposed Rule to the Final Rule

- – Category 1 small, unmanned aircraft cannot have any exposed rotating parts that would lacerate human skin.
- – Category 1, 2, and 4 remote pilots are prohibited from operating small, unmanned aircraft in sustained flight over open-air assemblies unless the operation meets the requirements of standard remote identification or remote identification broadcast modules established in the Remote ID Final Rule.
- – Added a Category 4 of small, unmanned aircraft that. Ay be eligible for operations over people and moving vehicles.
- – Allow operations over moving vehicles
- – Remote pilot, owner, or person manipulating the controls must have in their physical possession and readily available their remote pilot certificate.

(Administration, 2020)

What Do These Two Rules Really Mean and Why is it Important?

Some major players in the drone industry are not all that happy with the new rules as they currently stand. The following article excerpt from Sean Hollister has a much different take and makes some interesting points.

Alphabet's drone delivery company "Wing" still wants drones tracked — but differently

Internet-based tracking is exactly what the FAA had originally intended to do when it first

proposed the Remote ID rules back in December 2019, by the way — before it received a

laundry list of reasons from commenters why internet-based tracking might be problematic and

decided to abandon it. Here are just a few of the ones mentioned:

- The cost of adding a cellular modem to a drone to begin with
- The cost of paying for a monthly cellular data plan just to fly a drone
- The lack of reliable cellular coverage across the entirety of the US
- The cost of paying a third-party data broker to track and store that data
- The possibility of that third-party data broker getting breached
- The possibility of that data broker or network getting DDoS'd, grounding drones in the US

"Personally,[1] I think it's pretty ridiculous that the FAA felt it had to choose between "everyone has to broadcast their location to everyone within earshot" and "everyone has to pay gobs of money to private industry and trust some data broker with their location," but the reasons why we aren't going with internet-based tracking make some sense to me. (Hollister, 2021)

Most proponents of Remote ID technology, including Wing, like to explain that it's merely a "license plate" for the skies, perhaps nothing more intrusive than you'd already have on your car. Here's Wing (See Figure 3.5) on that:

This allows a drone to be identified as it flies over without necessarily sharing that drone's complete flight path or flight history, and that information, which can be more sensitive, is not displayed to the public and only available to law enforcement if they have proper credentials and a reason to need that information. (Hollister, 2021)

But the thing about license plates is, traditionally, you have to be within eyeshot to see them. You'd have to be physically following a car to track it. That's not necessarily true of a broadcasting transmitter, and it's potentially *far* less true of an internet-based solution like the one Wing seems to wish the FAA had offered instead. Naturally, it depends on who owns the internet-based solution and how much you trust them and their security. (Hollister, 2021)

Either way, it's going to be a while before we find out how secure or vulnerable, how broad or narrow these Remote ID broadcasts are truly going to be. That's because the FAA's final rule doesn't actually mandate what kind of broadcasting tech drones will be required to use: companies have the next year and half to figure that out, and they have to submit it to the FAA for approval. The FAA is also clear that broadcast Remote ID is just a first step, an "initial framework," suggesting that internet-based Remote ID might still be an option in the future. (Hollister, 2021)

Figure 3.5 Image: Wing. (Source: https://www.theverge.com/2021/1/1/22209558/google-wing-faa-drone-remote-id-broadcast-rule-privacy-security)

Drone Privacy Laws Around the World

The following sub sections are part of an in-depth survey from Surfshark regarding drone privacy laws around the world. The great thing about the study is that it drills down into a region-by-region analysis.

As the use of drones expands around the world — according to the Federal Aviation Administration, there are currently 1.7 million drones registered in the United States alone — lawmakers have been faced with new and complex regulatory challenges to protect the privacy of ordinary citizens. The increased prevalence of drones has raised the prospect of pervasive surveillance by governments, companies, and individuals, and lawmakers are struggling to keep up with the advancing technology. (SurfShark, 2021)

And while at least 143 countries have enacted some form of drone-related regulation, many experts contend that current drone regulation is insufficient to deal with the threat of widespread surveillance. Drone laws around the world range from outright bans of the technology to relatively unrestricted flight, but most legislation focuses on how the drone is being operated — and does not address nuances related to privacy. Many of the privacy threats that have lawmakers concerned are speculative and rely on the technology of tomorrow — making it difficult to pass privacy-specific legislation today. In the meantime, lawmakers have been able to pass laws concerning drone operation, which are a first step to "privacy by design" legislation, restricting where and how a drone can be flown to minimize opportunities to violate privacy in the first place. To support the effort to establish an international regulatory framework for drone legislation, we looked at drone operation laws in over 200 countries around the world. (SurfShark, 2021)

Lawmakers around the world have responded to the growing use of drones in various ways. While some countries, such as Cuba, Iraq, Iran, and Kuwait, have outright banned the use of unmanned aircraft, others have passed legislation allowing for more experimental use of the technology. (SurfShark, 2021)

On every continent, at least one country allows drones to fly what experts term "beyond visual line of sight", meaning the aircraft can fly to areas beyond the view of the pilot. In Finland, for example, where the home of FAI Drone Racing World Cup is held, pilots can obtain a permit allowing them to pilot drones outside of their view with special first-person view goggles. To see how drones are being regulated around the world, we compiled data on drone-related legislation for 210 countries. We looked at drone-related legislation for specific countries and analysis of drone-related legislation from sources such as UAV Coach, RAND Corporation, UAV Systems International, and the Library of Congress. (SurfShark, 2021)

We found that drone regulation in each country generally fell into one of seven categories:

- Outright ban
- Effective ban
- Restrictions Apply (such as drone registration or licensing, additional observers required, no commercial usage etc..)
- Visual line of sight required
- Experimental visual line of sight (experiments where drones fly beyond the line of sight are allowed)
- Unrestricted (when flying away from private property and airports, under 500 ft/150metres height and with drones weighing less than 250g)
- No drone-related legislation

We assigned each country a category status based on its legislation as of October 2020.

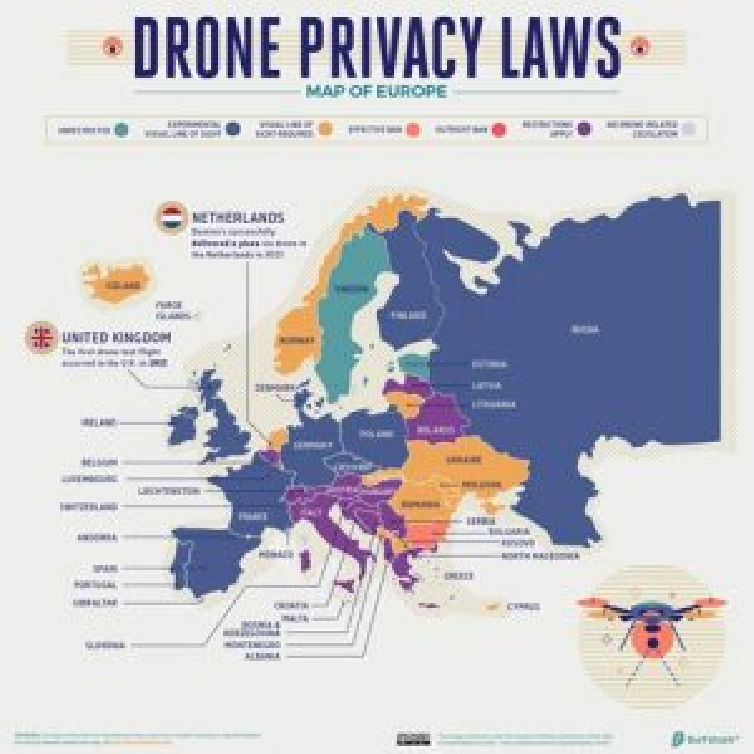
Europe

Europe currently has some of the most liberal drone regulation of any continent. Although many of the countries in the continent have some form of drone legislation restricting drone usage, these are often in the form of simple operational guidelines.

Drone pilots in Latvia, for example, are required to wear an identifying piece of clothing, such as a hat or a shirt. In Austria, pilots are required to get a license if the drone weighs more than about half a pound and flies above 98 feet. (SurfShark, 2021)

Figure 3.6 EUROPE: Drone Privacy Laws.

(https://surfshark.com/drone-privacy-laws)



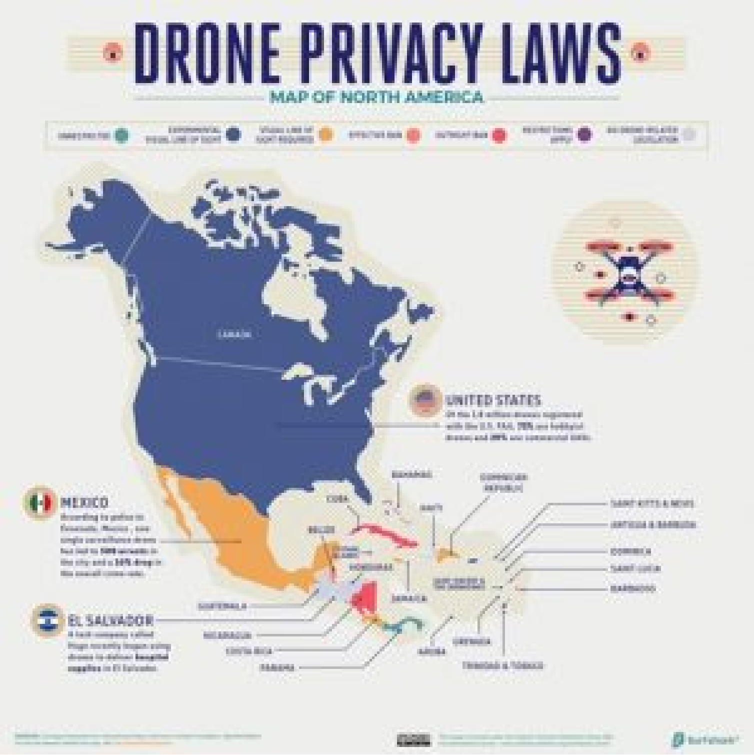
North America

While the bulk of countries around the world require drone pilots to be able to see the UAV at all times, 33% of countries in North America allow for experimental drone flights beyond the line of sight, the largest share of any continent and far above the 22% global average. The large number of countries allowing experimental drone flights may be related to the presence of tech companies like Amazon, Walmart, and DHL, which are researching ways to incorporate drones into their delivery infrastructure and developing methods to ship lightweight packages short distances. Countries with experimental drone legislation include Canada, the

United States, the Cayman Islands, Antigua and Barbuda, and other small Caribbean nations. (SurfShark, 2021)

Figure 3.7 NORTH AMERICA: Drone Privacy Laws.

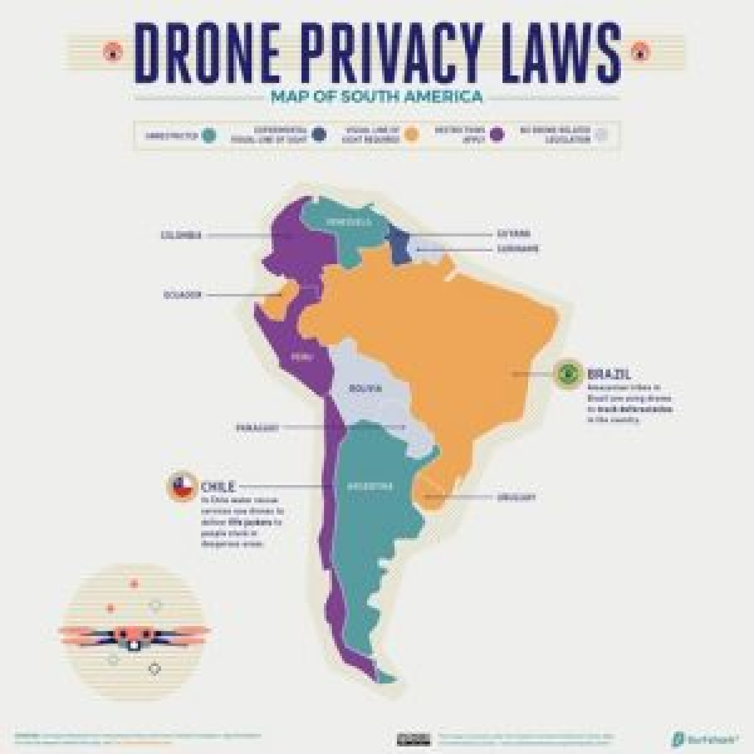
(https://surfshark.com/drone-privacy-laws)



South America

67% of countries with drone-related legislation in South America allow drones to be flown, as long as the aerial vehicle stays within the view of the pilot, the largest share of any continent. No countries in South America have outright or effective bans on drones. But while no countries ban drones, only one country, Guyana, has provisions that allow for flights beyond the line of sight — the fewest of any continent. Other countries in South America have specific drone rules geared towards safety and environmental conservation. In Peru, for example, drones' flights cannot last longer than an hour. In Ecuador, drones are completely banned on the Galapagos Islands save for approved scientific usage. (SurfShark, 2021)

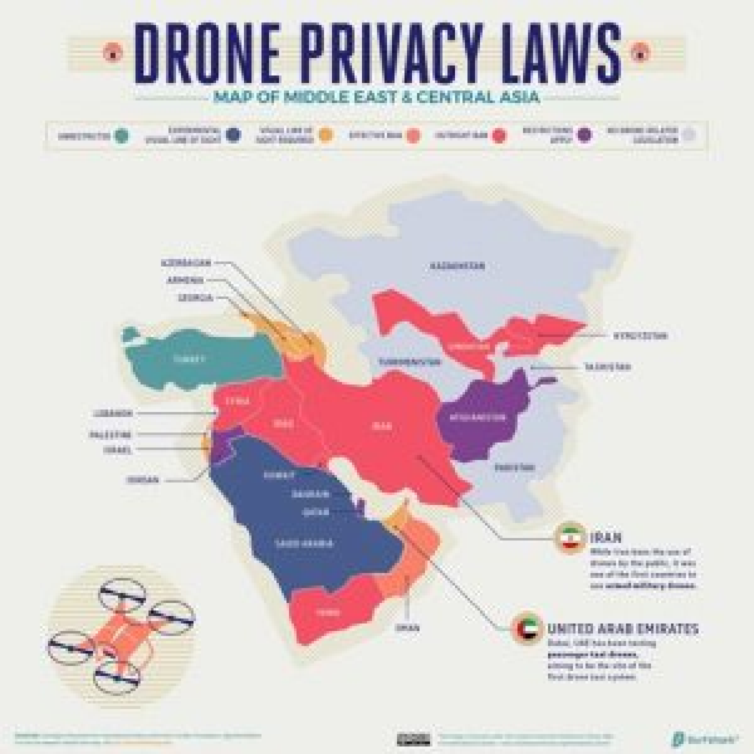
Figure 3.8 SOUTH AMERICA: Drone Privacy Laws.
(https://surfshark.com/drone-privacy-laws)



Middle East & Central Asia

21% of countries here with drone-related legislation have outright bans on drones, more than the 11% global share and the second largest share of any continent. Additionally, there are a number of countries with effective bans on drones. In Bhutan, for example, drone flight is only allowed by the government. Overall, 15% of countries in Asia have effective bans on drones, far more than the 8% global average and the largest share of any continent. A small number of countries, however, are beginning to allow for drone flights beyond the line of sight. Japan, for example, is currently developing a licensing system that will allow for drone flights beyond the visual line of sight for government deliveries. (SurfShark, 2021)

Figure 3.9 ME & CA: Drone Privacy Laws.
(https://surfshark.com/drone-privacy-laws)

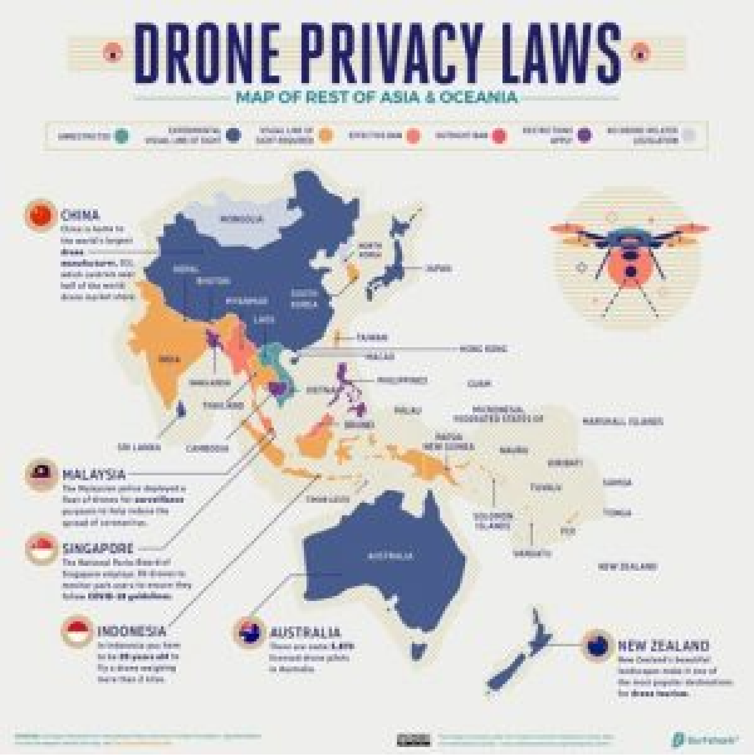

DRONE PRIVACY LAWS
MAP OF MIDDLE EAST & CENTRAL ASIA
UNRESTRICTED
EXPERIMENTAL VISUAL LINE OF SIGHT
VISUAL LINE OF SIGHT REQUIRED
EFFECTIVE BAN
OUTRIGHT BAN
RESTRICTIONS APPLY
NO DRONE-RELATED LEGISLATION
AZERBAIJAN
ARMENIA
GEORGIA
KAZAKHSTAN
KYRGYZSTAN
UZBEKISTAN
TURKMENISTAN
TAJIKISTAN
TURKEY
SYRIA
IRAQ
IRAN
AFGHANISTAN
PAKISTAN
LEBANON
PALESTINE
ISRAEL
JORDAN
KUWAIT
BAHRAIN
QATAR
SAUDI ARABIA
YEMEN
OMAN
IRAN
While Iran bans the use of drones by the public, it was one of the first countries to use armed military drones.
UNITED ARAB EMIRATES
Dubai, UAE has been testing passenger taxi drones, aiming to be the site of the first drone taxi system.
Surfshark

Rest of Asia and Oceania

56% of countries in Oceania have no drone-related legislation, the largest share of any continent. Of the countries that do have drone-related legislation, a majority allow drones as long as pilots stay within the visual line of sight of the drone. No countries have outright bans or effective bans of drones. In Australia and New Zealand, there are provisions for drones to fly beyond the visual line of sight of the pilot. Currently, licenses that permit drones to fly beyond the line of sight are limited among a few small aviation companies. According to the RAND Corporation, licenses for experimental flights beyond the line of sight are easier to obtain in Australia than in the United States. (SurfShark, 2021)

Figure 3.10 OCEANA: Drone Privacy Laws.

(https://surfshark.com/drone-privacy-laws)



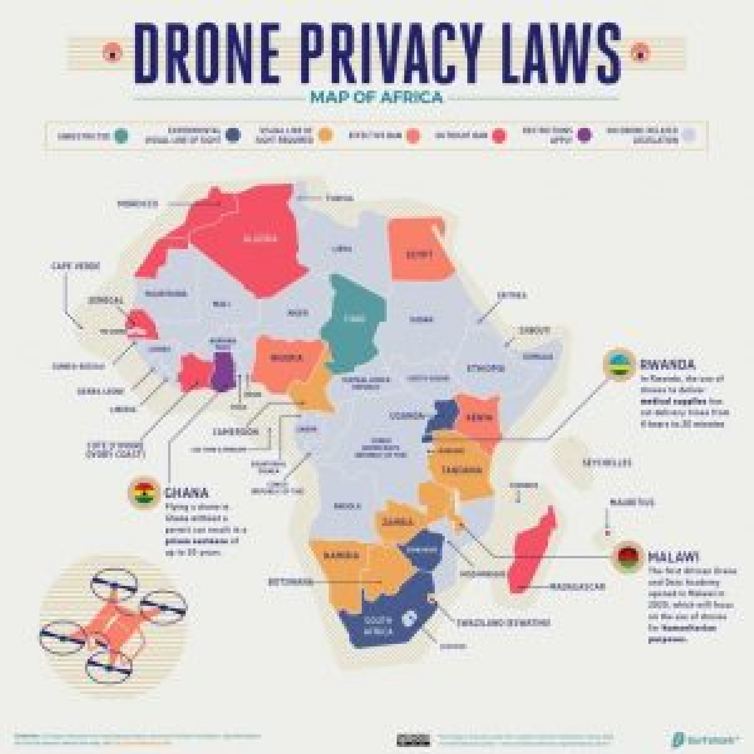
Africa

More than half of all countries in Africa have no drone-related legislation. Of the countries that do have drone-related legislation, 21% have an outright ban on the technology, the largest share of any continent. Another 13% of countries have an effective ban on the technology, the second largest share of any continent. In Egypt, for example, while drones are technically legal with permission from the Civil Aviation Authority, it is very difficult to obtain permission.

But while there are obstacles to drone flight in a number of African countries, there are also examples of innovation in the continent. In Ghana and Rwanda, for example, drones are allowed to fly beyond the line of sight to deliver medical supplies to remote villages. Other African countries that allow drones to fly beyond the line of sight include Uganda and Zimbabwe. (SurfShark, 2021)

Figure 3.11 AFRICA: Drone Privacy Laws.

(https://surfshark.com/drone-privacy-laws)



Demand for drone technology shows no signs of slowing down. According to the World Intellectual Property Organization, the number of patents for drone technology is increasing rapidly —

growing 34% from 7,076 in 2017 to 9,485 in 2018 alone. As commercial technology for unmanned aerial vehicles continues to advance, it is important for the legislation regulating them to keep up. And until there is some international standard or governing body for the usage of drones established, it's fascinating to see how the regulation of drones differs from country to country around the world. Keep scrolling down to see the full data from our study, and to check out the law where you live. (SurfShark, 2021)

Methodology & Sources

To see how drones are being regulated around the world, we looked at related legislation for specific countries using sources such as UAV Coach, RAND Corporation, UAV Systems International, and the Library of Congress. We found that drone regulation in each country fell into one of seven categories: outright ban, effective ban, visual line of sight required, experimental visual line of sight (experiments where drones fly beyond the line of sight are allowed), restrictions apply, unrestricted, and no drone-related legislation. We assigned each country a category status based on its legislation as of October 2020. (SurfShark, 2021)

References

Administration, F. A. (2020, December 28). *faa.gov*. Retrieved from Press Release – US Department of Transportation Issues Two Much Anticipated Drone Rules to Advance Safety and Innovation in the United States: www.faa.gov/news/press_release/news_story.cfm?newsld=25541

Hollister, S. (2021, January 1). *Google's Wing warns new drone laws 'may have unintended consequences for privacy*. Retrieved from theverge.com: https://www.theverge.com/2021/1/1/22209558/google-wing-faa-drone-remote-id-broadcast-rule-privacy-security

Kiemen, K. (2021, January 6). *Two New FAA Drone Rules That You*

Will Actually Want to Read About . Retrieved from forbes.com: https://www.forbes.com/sites/kristykiernan/2021/01/06/two-new-faa-drone-rules-that-you-will-actually-want-to-read-about/?sh=6156c4807e21

SurfShark. (2021, January 18). *License to Fly* . Retrieved from Drone Privacey Laws Around the World : https://surfshark.com/drone-privacy-laws

[1] Hollister' opinion, not chapter author.

4. UUVs, Advanced Sensors, Munitions Detection & USVs [Nichols]

Student Learning Objectives

- – To take a birds-eye view of UUVs in service of detecting, assessing, and classifying underwater munitions
- – To study the type of sensors and their performance objectives in underwater service
- – To focus on a specific UNCLASSIFIED NSWC PCD demonstration of three UUVs used for detection of munitions targets (both proud and buried)
- – To look at improvements in survey UUVs / on surface UVs for shallow water studies.
- – To see the future of this technology as a Black Swan event.[1]

What is the Advanced Weapons Problem that UUVs can solve?

There are underwater munitions sites around the world where the quantity and the type of munitions are either unknown or not well documented. These sites are unsafe and can't be used for any other purpose. The sites need to be surveyed and all the munitions identified and if necessary disarmed. (Leasko, 2014). Underwater munitions falls in the murky purview (CLASSIFIED) of the National Unmanned Systems Shared Resource Center (NUSSRC) located at the Naval Surface Warfare Center Panama City Division (NSWC PCD). It has multiple offices associated with the Office of Naval Research (ONR) Mine Countermeasure (MCM) UUV systems integrated with advanced sonar, magnetic and electro-optical sensors.[2] These systems provide capability for experimentation and demonstration of current Science and Technology (S&T) and Research and Development (R&D) program assets as they apply to the detection and classification of underwater mines to be used for detection, assessment, and characterization of underwater munitions. (Leasko, 2014)

NSWC PCD

The Naval Surface Warfare Center Panama City Division (NSWC PCD) is one of many naval installations conducting S&T research around the world. NSWC PCD is a particularly fascinating one and has a huge mission. NSWC PCD Our mission is to conduct research, development, test, and evaluation (RDT&E) and in-service support of the following core mission areas: Mine Warfare Systems, Naval Special Warfare Systems, Diving and Life Support Systems, Amphibious/Expeditionary Maneuver Warfare Systems and other missions that occur in the littoral, or coastal, regions. NSWC PCD's Technical Capabilities include: Air Cushion Vehicle Systems; Expeditionary Maneuver Warfare Systems Engineering and Integration; Special Warfare Maritime Mobility Mission Systems and Mission Support equipment; Mine Countermeasure Detect and Engage Systems; Modular Mission Packaging; Platform Integration and Handling; Littoral Mission Systems integration and Modular Mission Packages Certification; *Unmanned Systems Engineering and Integration*; Autonomous Diving and Diving Support Systems; and Surface Life Support Systems for Extreme Environments. Their major facilities include: Diving and Life Support Complex; Mine Warfare Complex; Special Warfare Research and Engineering Complex; Expeditionary Warfare Complex; Landing Craft Air Cushion (LCAC) Facility; LCAC Software Integration Laboratory; Human Systems Integration Usability Lab; USMC Amphibious Raids and Reconnaissance; Integration Facility; Coastal Test Range; Prototype Fabrication Facility; Additive Manufacturing or 3D printing for rapid prototyping; and 3D Expeditionary Laser Scanning. This is the purview of just one of the ten plus NSCW warfare centers. These are all part of the Naval Sea Systems Command (NSSC), “The force behind the fleet.” (NSWC, 2020)

Murky Waters

We can get a OPEN SOURCE peek into the use of NAVSEA’s MCM UUV assets to evaluate and demonstrate current technologies with advanced detection, assessment, and characterization sensor packages. NSWC PCD published a report (UNCLASSIFIED) on their Post Mission Analysis (PMA) of all sensor data relating to the performance of UUV technologies for the underwater munitions problem so identified. (Leasko, 2014) [3]

The PMA data collection / demonstration by NSWC PCD occurred in early 2011.

Technology

Three specific UUV assets in the NUSSRC inventory[4] that can address the detection and characterization of underwater munitions in an organic fashion are the Remote Environmental Measuring Units 100 (REMUS 100); the Blufin12 Buried Mine Identification (BMI) UUV systems and the REMUS 600 BMI UUV, with a separate magnetic sensor, the Real-time Tracking Laser Scalar Gradiometer (LSG) to collect data over the field too. (Leasko, 2014)

REMUS Group

REMUS makes four serious UUV products. REMUS 100, REMUS 300, REMUS 600 and the REMUS 6000. Figure 4.1 shows the REMUS 100/MK 18 Mod 1. The first two UUVs are described.

Source: (REMUS, 2020)

The REMUS 100 is a man-portable Unmanned Underwater Vehicle (UUV) designed for rapid deployment, it can be easily transported via helicopter and launched from a dock or any vessel of opportunity. With a maximum operating depth of 100 meters and a mission duration of up to 12 hours, it is ideal for rapid, low-logistics deployments. (REMUS, 2020). The UUV is 67” L x 7.5” D and weighs

80 lbs. It has a maximum depth of 328 ft and 6 hours operations time. It is equipped with the following: (REMUS -1., 2020)

Environmental Sensor
– Fluorometer/Backscatter Sensor
– Fast Response Conductivity

Temperature Sensor
– Oxygen Optode
– Turbidity Sensor
Imaging Hardware
– Bathymetric Side Scan Sonar
– Video Camera Recorder (VCR) Module
– Lightbar for VCR Module
– Gap-Filler Sonar
Communication/Navigation Equipment
– Precision GPS
– Military GPS
– Wi-Fi Communications
– Iridium Communications
– NavP Inertial Navigation System
with Payload Processor
Software
– Navlab Post Processing Software
– RECON Software
– Reflection Post-Mission Analysis Software

Figure 4.1 REMUS 100/MK 18 Mod 1

Source: (REMUS -1., 2020)

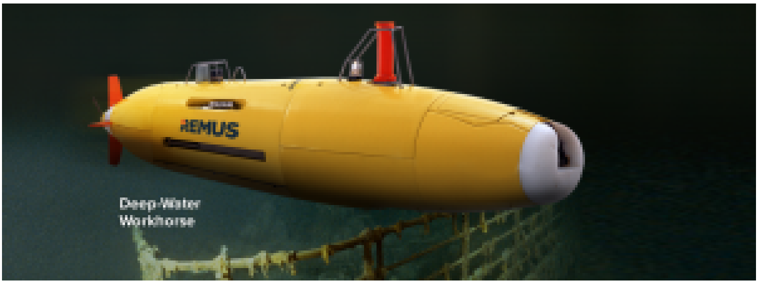
REMUS 600

The REMUS 600 is a midsized UUV designed for easy transport and maximum versatility, the REMUS 600 (the US Navy MK18 Mod 2 and LBS AUV Program vehicles) is a highly configurable vehicle with a maximum operating depth of 600 meters. Able to be deployed from vessels as small as an 11 meter RHIB and boasting a maximum mission duration of 24 hours, the REMUS 600 can be outfitted with a broad range of sensors to meet the requirements of nearly any mission. (REMUS -2., 2020) The REMUS 600 has the following specifications: Vehicle Diameter 12.75 in; diameter varies depending upon module (for 600 m depth configuration); Vehicle Length Min length ~9 ft to Max length ~18 ft; length varies depending upon module configuration; Max Weight in Air Min ~850 lbs where weight varies depending upon module configuration; Maximum Operating Depth 600 meters (1500 meter configuration available);Energy 5.4 kWh rechargeable Li-ion battery; (Second 5.4 kWh battery tray is optional), exchangeable battery option available; and Endurance Typical mission endurance is up to 24 hours in standard configuration; subject to speed, battery and sensor configurations. (REMUS -3., 2020) It is equipped with the following (See Figure 4.2) :

Standard System Configurations
– Doppler Velocity Log (DVL)
– Compass or Inertial Navigation System as
Standard Depending on Configuration
– Acoustic Modem (Low & High Frequency Options Available)
– Pressure Depth Sensor
– Conductivity & Temperature Sensor
– GPS/Wi-Fi/Iridium
– Emergency Recovery Equipment
– Terrain Avoidance Sonar
Optional Equipment
– Up to (2) Battery Trays
– Responder for Surface Ultra Short Baseline (USBL)
– Navigation Aiding
– NavP/HG 9900 INS with Payload Processor
– Obstacle Avoidance Sonar
Optional Sensors
– Dual Frequency Sidescan Sonar
– HiSAS 2040 Synthetic Aperture Sonar
– Dynamically Focused Sidescan Sonar
– Optical Environmental Characterization Sensors
– Video Camera
– Multi-Beam Echo Sounder (MBES)
– Electronic Still Camera (ESC)
– Sub-Bottom Profiler (SBP)
– Fish Finding Echo Sounders
– Oxygen Sensors
– Photosynthetically Active Radiation (PAR) Sensor
– LED Based Lights & Strobes for Cameras
– High Precision, Dual-Band GPS Receiver
– Terrain Avoidance Sonar (Obstacle Avoidance Sonar optional)
– Other Custom Sensor Options Available
Shipboard Devices
– Shipboard Communications Mast
– Power Box with Battery Charger/Conditioner

– Shipboard Communications System
(GPS, Iridium, Wi-Fi and Optional Freewave)
– Acoustic Communications Bottle
– Ranger Deck Box
– Acoustic Transducer Towfish
– Releasable Acoustic Transponders
– Portable Surface Communications Station

Figure 4.2 REMUS 600 UUV



"The REMUS 6000 AUV (Figure 4.3) was designed under a cooperative program involving the Naval Oceanographic Office, the Office of Naval Research and the Woods Hole Oceanographic Institution (WHOI) in support of deep-water autonomous operations. The REMUS 6000 AUV boasts the same proven software and electronic subsystems found in our highly successful REMUS 100 AUV, with a depth rating, endurance, and payload that allow for autonomous operations in up to 6000 meters of water." (REMUS -4, 2020) The REMUS 6000 has Vehicle Diameter 28 in by Vehicle Length 13 ft and weighs in Air 1900 lbs; works at Maximum Operating Depth 6000 meters (4000 meter configuration also available); Energy 12 kWh rechargeable Li-ion battery pack for two pressure housings; a second 12 kWh set can be purchased as an option with system permitting 2-hour turn around; charge time is typically 8 hours and the batteries are rechargeable up to 300 cycles or for 5 years under recommended storage conditions; and has Endurance Typical mission duration of 22 hours; subject to speed & sensor configuration. (REMUS -5., 2020) What makes the REMUS 6000 is "technical horsepower:"

Standard System Configurations
– Acoustic Doppler Current Profiler/Doppler
Velocity Log (ADCP/DVL)
– Acoustic Modem (Low Frequency)
– Inertial Navigation System (INS)
– Sidescan Sonar
– Depth Sensor
– Conductivity & Temperature Sensor
– GPS/Wi-Fi/Iridium
Optional Sensors
– Dual Frequency Sidescan Sonar
– ECO Sensors
– Multi-Beam Echo Sounder (MBES)
– Video Camera
– Electronic Still Camera (ESC) with
200 Watt-Sec Strobe Lighting
– Sub-Bottom Profiler (SBP)
– NavP/HG 9900 INS with Payload Processor
Deployment Options
– Launch & Recovery System
– Operations Van
– Side Launch Rotation Table
Shipboard Devices
– Shipboard Communications Console
– Power Box with Battery Charger
– Antenna Box
(GPS, Iridium, Wi-Fi and Optional Freewave)
– Acoustic Communications Bottle
– Ranger Deck Box
– Towfish

– Acoustic Transponders

– HiPAP USBL Capability

Vehicle Interface Program (VIP)

The REMUS 6000 uses essentially the same Vehicle Interface Program (VIP) as the proven REMUS 100 AUV. This highly intuitive VIP greatly simplifies vehicle maintenance, mission planning, vehicle checkout, and data analysis; and will run on any PC or laptop operating under Windows.® Communication between the vehicle and the host is conducted via a standard Ethernet connection. Among other features, the VIP includes:

– An integrated text editor for construction of the mission file.

– A map view that illustrates the planned mission for review.

– Automatic error checking performed on all aspects of the planned

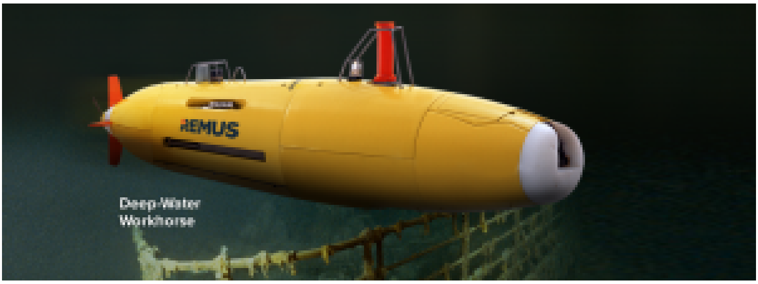
mission, with warning messages that appear if any mission

parameters are incorrect.

– A set of quick-look indicators display system status, where green

indicates OK, and red indicates a fault.

Figure 4.3 REMUS 6000



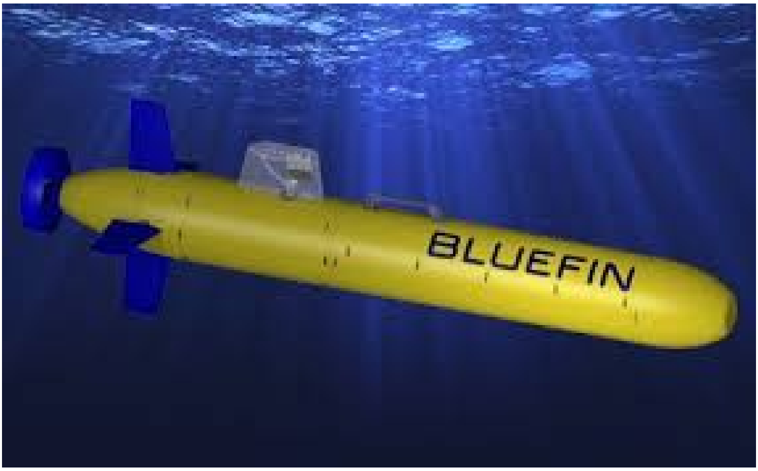
Source: (REMUS -5., 2020)

Bluefin 12 Buried Mine Identification (BMI) UUV System

In a paper by (G. Sulzberger, 2009) the Bluefin 12 BMI was abstracted as follows: "The Bluefin12 Buried Mine Identification (BMI) System is used as the platform to develop a capability for the identification of buried mines. This system houses the bottom looking sonar, the Real-time Tracking Gradiometer (RTG), and an Electro-Optic Imager (EOI).

The objective for the RTG is the enhancement of the processing that extracts target locations and magnetic moments from the raw RTG data. (G. Sulzberger, 2009) added the capability to conduct real-time processing capability to provide autonomous target classification and localization results soon after the UUV passes the target, while the system is still performing the mission. These results will be shared with the vehicle or other sensors for transmission back to a base station when the vehicle surfaces. The objectives for the EOI include additions to the control software and the development of a set of versatile image processing techniques. A significant goal is to develop the ability to make images viewable remotely over the vehicle's RF link. This allows for a quick review of contacts and improved flexibility in mission planning and execution. Image processing goals included the development of image enhancement algorithms that could be applied to all EOI data. The intent of the enhancement algorithms is to enhance image contrast and sharpness to better differentiate targets from background and increase target detail. The software will be used to batch process large amounts of raw EOI images and save them in a format so that the user can scroll through the images using a standard image viewer." (G. Sulzberger, 2009) (Figure 4.4)

Figure 4.4 Bluefin12 BMI

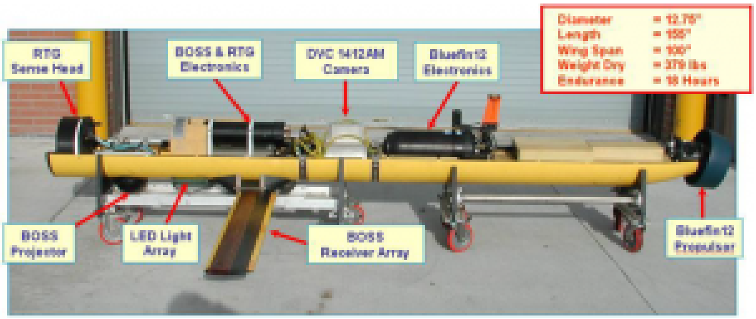


Source: (Bluefin Robotics, 2020)

Demonstration

The objective of the NSWC PCD MR-201103 project conducted in 2011 was to leverage the Office of Naval Research's (ONR) Mine Countermeasures (MCM) unmanned underwater vehicle (UUV) assets to evaluate and demonstrate the applicability of existing ONR MCM UUV technologies integrated with advanced sensor packages for facilitating detection, assessment, and characterization of underwater munitions.

Figure 4.5 Bluefin 12 Internals



Source: (Bernstein, 29 June 2012)

A number of sensors were employed in the demonstration. The BMI sensor suite consists of the Buried Object Scanning Sonar (BOSS) and the Realtime Tracking Gradiometer (RTG) fitted to the Bluefin-12 UUV. The REMUS100 system carries a dual frequency, 900/1800 kHz side scan sonar. (Figure 4.5) The REMUS system provided high resolution acoustic images of proud objects, while the BMI sensor suite on the Bluefin-12 UUV provided acoustic images of buried objects and the magnetic moments of targets or clusters within range of the RTG sensor. The combination of the data from both UUV systems was designed to enable detection of acoustically reflective targets and discrimination between proud and buried state, provide size and aspect information, and indicate which contain magnetic material of the level seen for munitions. (SERDP-ESTCP, 2012)

Demonstration Results

Quoting from the (SERDP-ESTCP, 2012) report, the Results were not without Implementation errors.

"A small underwater munitions test site was planted in the Davis Point area of St. Andrew Bay near Naval Surface Warfare Center-

Panama City Division (NSWC PCD). Five nominal 100-m-long target lines spaced 2 m apart were laid parallel to each other. The first two lines had individual targets spaced along the lines and aligned at random orientations relative to the target lines. One line had the targets proud and the other line had the targets flush buried. The third through fifth lines had two clusters of targets on each line. Lines one and two provided baseline measurement data for each individual target type. Lines three through five provided acoustic and magnetic data for clusters of munitions in different states of burial and orientation. The planted locations of the targets were determined by their drop locations from the surface vessel using plumb lines and a GPS system.

The BOSS sensor clearly demonstrated the capability of detecting and imaging unexploded ordnance (UXO) *targets of the class* M *targets in proud, partially buried, and fully buried configurations*. Discriminating between the different targets was accomplished by comparing the known target physical dimensions with the measured dimensions extracted from the BOSS imagery. However, discriminating multiple targets in a clustered configuration was difficult for the case of targets closely spaced together (target 16-CL1-M). This is due to the medium resolution of the BOSS sensor. The developer of the BOSS system has recommended increasing the transmit frequency to increase the resolution to enhance the imagery but funding for this effort has not been forthcoming.

The RTG experienced hardware failure during the data collection event at the end of June, leading to lost data. A likely candidate for this failure is the oil-filled cables that connect the sensor head to the electronics bottle. These cables and their connection points have failed in the past with similar effects on the data. A refurbishment and recalibration of the RTG system would be beneficial for future testing events and will be necessary to improve results." (SERDP-ESTCP, 2012)

Implementation Issues

The technologies encountered numerous problems during their deployment, including the failure of multiple channels in each sensor, not allowing much of the data to be recovered. The sensor suite used in the experiment was unique research and development equipment developed by the Navy for finding buried mines. As such, it cannot be procured commercially. Additional equipment would have to be custom-built.

Improvements in magnetic sensors have been made since the RTG sensor was constructed, and alternate sensor designs might be considered, including the LSG sensor. Collaboration between government and contractor subject matter experts would be required to develop a state-of-the-art gradiometer suitable for integration with the Bluefin-12 UUV and the BOSS sensor for regular use in munitions surveying. As a part of that effort, software for processing gradiometer and BOSS data would be streamlined to enable survey contractors to use the system with minimal additional training. (SERDP-ESTCP, 2012)

Success Criteria and Performance Objectives

Before we describe a selected sensors and findings, it is useful to know what the success criteria was for this demonstration. First we need to think in terms of Performance Objectives.

Performance Objectives (PO) Remote Environmental Measuring Units REMUS 100.

The performance objective (PO) for the REMUS 100 was to first provide a wide area search over the entire site areas with the 900 kHz side scan sonar. Once the wide area search was complete the sonar imagery from that search would provide information on the overall assessment of *proud* objects in the area and if any are contacts of interest. A follow-on lower altitude, small-area detailed survey and target reacquisition of the contact of interest would be performed operating the sonar at 1800 kHz. The 1800 kHz frequency provided with picture quality sonar imagery that enhances classification and identification of the proud contacts of interest. Along with sonar data camera imagery it would provide clear picture quality imageries of the contact of interest.

This PO was not accomplished because the REMUS camera was unavailable. The survey was performed on a clear water day with the EO sensors on board the REMUS 600.

Performance Objectives – Buried Object Scanning Sonar (BOSS)

Table 4.1 summarizes the BOSS system POs. The objectives include assessment of the probability of detection, the degree of burial, size, shape, and orientation determined and localization accuracy against a combination of small and large UXO targets. (Leasko, 2014) The planned tests were not blind tests. They were designed to determine the sidescan, BOSS and RTG combined capabilities against *proud* (clearly visable and not buried) and buried targets and to determine whether further optimization of the multi sensor approach, and further performance testing was warranted.

The PO was to demonstrate and measure the ability to classify all contacts using: 1) the BOSS to measure target size, shape, and orientation, 2) the RTG sensor to determine which BOSS contacts are ferrous and non-ferrous and to measure the magnetic moment of the ferrous contacts and 3) compare BOSS with REMUS sidescan data to indicate which contacts are buried and which are proud and to enhance localization of those contacts. (Leasko, 2014)

Table 4.1 Performance Objectives for the BOSS Sensors

Performance Objective	**Metric**	**Data Required**	**Success Criteria**
Quantitative Performance Objectives			
Detection of all munitions of interest	Percent detected of seeded items	Location of seeded Items[5]	Pd=0.90 [6]
Determine the degree of burial, size, shape, and orientation of contacts.	Percent correct classification of the burial depth, size, shape, and orientation of the seeded targets.	Validation data for selected targets	Demonstration of >90% correct classification of the size, shape, and orientation of the targets. Length and burial measurements considered correct shall be within 25% of actual
Location accuracy	Average localization error in meters from latitude and longitude ground truth localization for seed items	Location of seed items surveyed to accuracy of 1.0m	ΔLocalization Error < 1m from ground truth
Qualitative Performance Objectives			
Ease of Use		Feedback from technician on usability of technology and time required	

Source: (Leasko, 2014)

Performance Objectives – Real-Time Tracking Gradiometer (RTG) / Laser Scalar Gradiometer (LSG)

The performance objectives for the RTG system are summarized in Table 4.2. The objectives include a demonstration of the performance of detection, the ability to measure the magnetic moment and be able to localize the contacts or clusters of targets.

Table 4.2 Performance Objectives for the RTG Sensors

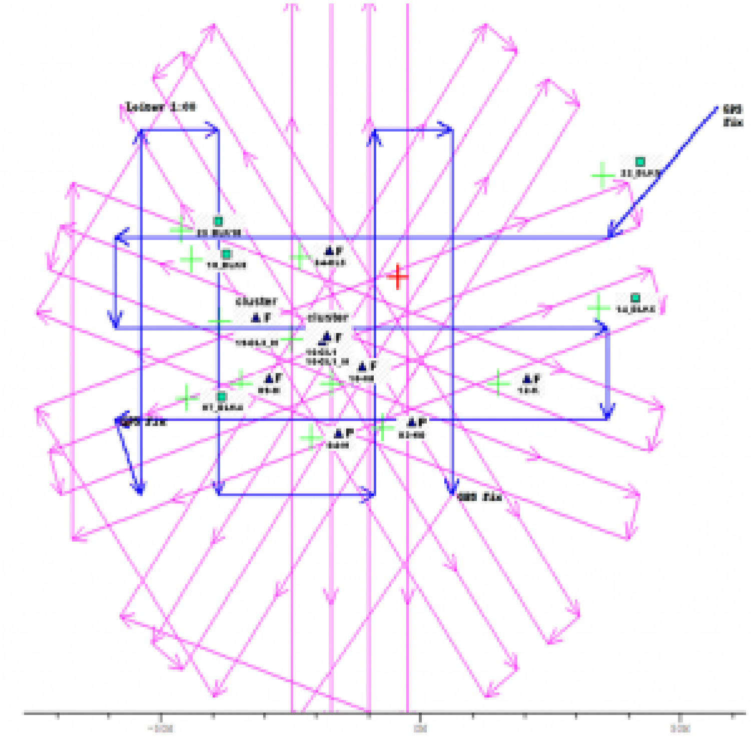
Performance Objective	Metric	Data Required	Success Criteria
Quantitative Performance Objectives			
Detection of all ferrous munitions of interest	Percent detected of seeded ferrous items	Location of seeded Items	Pd=0.90
Measurement of ferrous target magnetic moment	For individual planted targets, the percent of targets whose magnetic moment is measured during a flyover to within 20% of that measured in the laboratory, for the particular altitude flown.[7]	Validation data for selected targets [8]	Demonstration of >90% of individual ferrous targets moments measured to within 20% of actual.
Location accuracy [9]	Average localization error in meters from latitude and longitude ground truth localization for seed items	Location of seed items surveyed to accuracy of 1.0m[10]	ΔLocalization Error < 1m from ground truth
Qualitative Performance Objectives			
Ease of Use		Feedback from technician on usability of technology and time required	

Performance Assessments

Remote Environmental Measuring Units 100 (REMUS 100)

Figure 4.6 shows the REMUS 100 UUV mission over the test field. The mission was a combine 900 kHz and 1800 kHz sonar surveys. The blue lines with arrows, represents the track lines and vehicle direction as it traveled though the test field surveying at 900 kHz. The purple lines with arrows, represents the track lines and vehicle direction as it traveled though the test field surveying at 1800 kHz. The green (+) symbol represents the locations of the targets detected. Sonar imagery of this is displayed in Figures 14 – 26. The red (+) symbol represents the location of a detected UXO target out of place from Cluster 16-CL1_M. It is thought that the UXO target was moved by a shrimper's nets as they went through the test field.

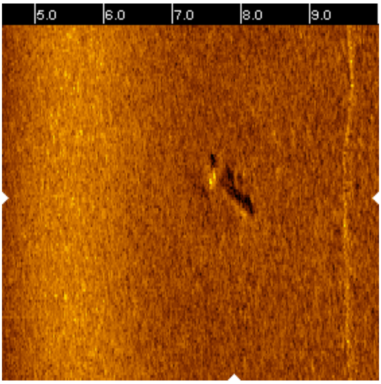
Figure 4.6 REMUS 100 mission map

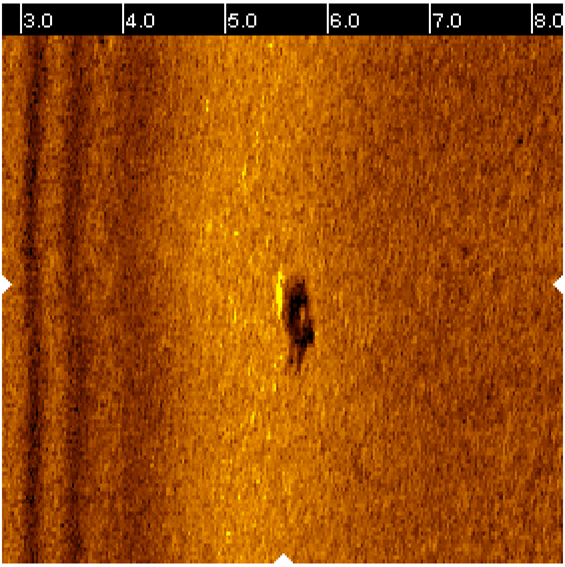


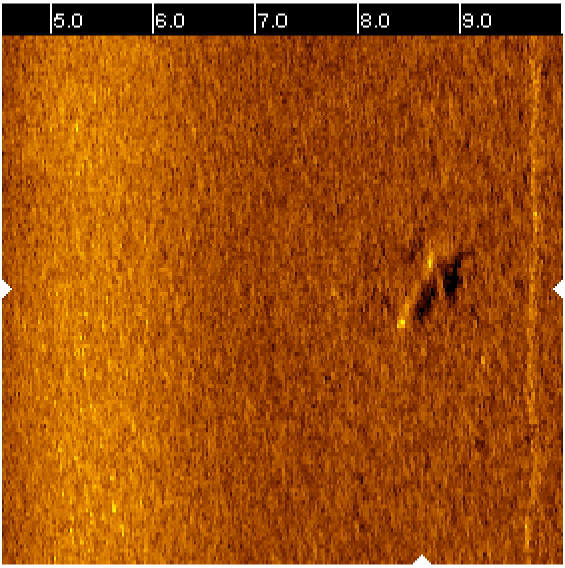
Source: (SERDP-ESTCP, 2012)

Figure 4.7 shows a sample RTG 1800 kHz sonar imagery of seeded point 04-M on Figure 4.6.

Figure 4.7 shows a sample RTG 1800 kHz sonar imagery of seeded point 04-M on Figure 4.6


5.0
6.0
7.0
8.0
9.0

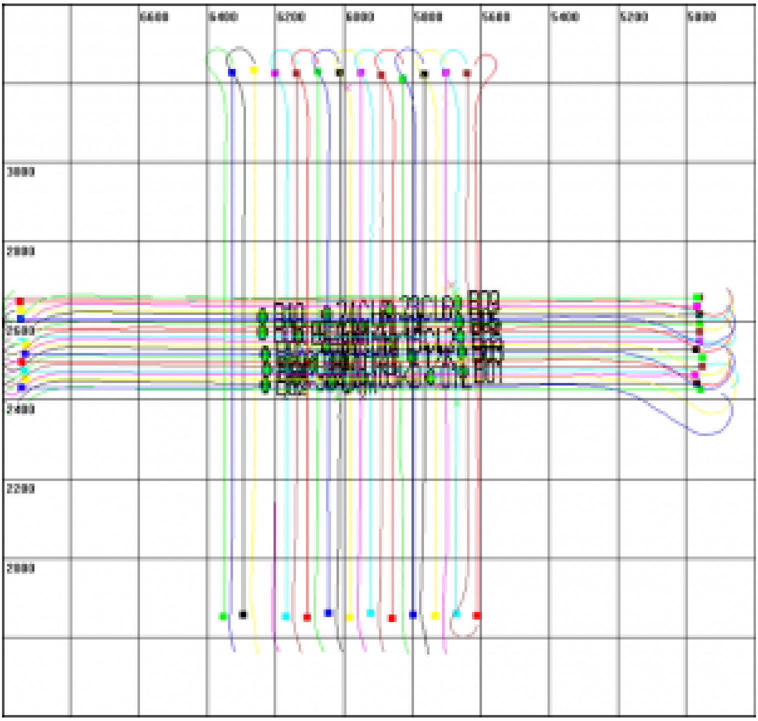

3.0
4.0
5.0
6.0
7.0
8.0



Source: (SERDP-ESTCP, 2012)

Figure 4.8 shows the interesting navigation tracks for the survey missions performed on 25 June 2011. Note the search patterns are designed to pick up proud and buried targets from 90 degree approaches.

Figure 4.8 Navigation tracks for the survey missions performed on 25 June 2011.



Source: (SERDP-ESTCP, 2012)

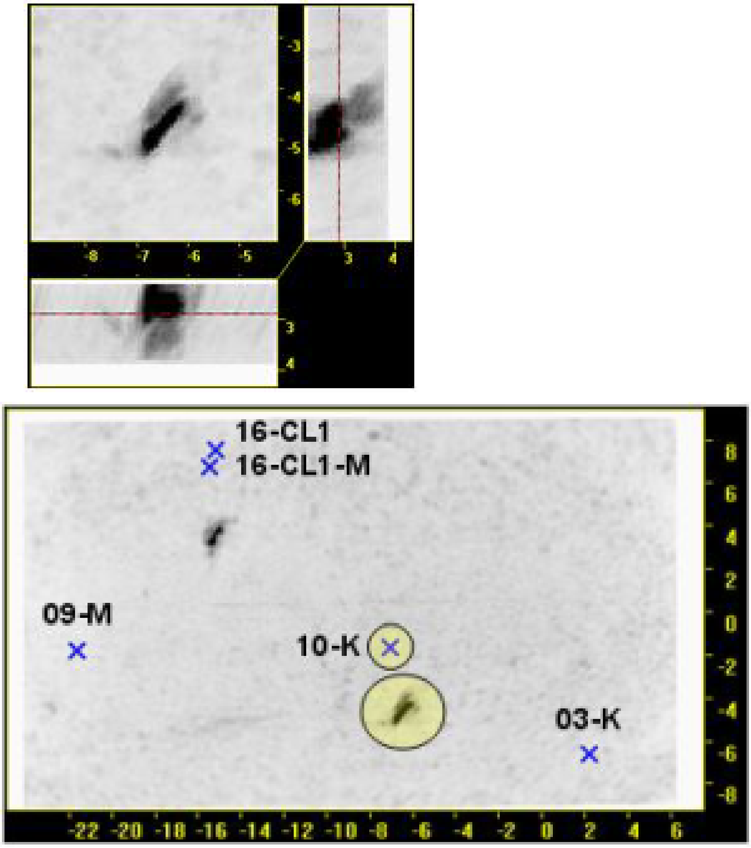
BOSS Images

The BOSS images consist of the X-Y plan view showing the plumbed position of the target represented by an "X" and the image of the target of interest highlighted with a circle and labeled with the target's designation. A zoomed, 3D multi-aspect BOSS image for each target is also provides the X-Z and Y-Z perspective views to show target burial state. BOSS target localization, distance from BOSS localization to diver plumbed positions ("X"), target dimensions and burial state information for each of the targets is provided from BOSS PMA.[11]

Note that all BOSS-generated images in this report are for cases with sub-critical grazing angles in the sand bottom field. (SERDP-ESTCP, 2012)

Figure 4.9 shows BOSS imagery for target 10-K: (a) plan view image and (b) zoom image of target 10-K. Vertical axes are cross track, and horizontal axes are along track, in meters.

Figure 4.9 Example of BOSS imagery



Source: (SERDP-ESTCP, 2012)

Summary – BOSS

According to Leasko (Leasko, 2014), the BOSS sensor clearly demonstrated the capability of detecting and imaging unexploded ordinance (UXO) targets of the class M targets in proud, partially buried and fully buried configurations. Discriminating between the different targets was accomplished by comparing the known target physical dimensions with the measured dimensions extracted from the BOSS imagery. However, discriminating multiple targets in a clustered configuration was difficult for the case of targets closely spaced together (target 16-CL1-M). This is due to the medium resolution of the BOSS sensor.

As to target localization, the BOSS system receives and uses UUV navigation information to calculate target localization. The present navigation package in the Bluefin12 UUV can be updated to improve its accuracy. The present method of obtaining the ground truth of targets deployed underwater can introduce errors especially in deeper water making it difficult to accurately assess target localization. (Leasko, 2014)

Modern mine warfare challenges today

What is the scope of the problem? The (Bernstein, 29 June 2012) demonstration referred to in this chapter constitutes a relatively small number of UXO targets to be detected, assessed and classified.

Mine warfare remains the most cost-effective of asymmetrical naval warfare. Mines are relatively cheap and being small allows them to be easily deployed. Indeed, with some kinds of mines, trucks and rafts will suffice. At present there are more than 300 different mines available. Some 50 countries currently have mining ability. The number of naval mine producing countries has increased by 75% since 1988. It is also noted that these mines are of an increasing sophistication while even the older type mines present a significant problem. It has been noted that mine warfare may become an issue with terrorist organizations. Mining busy shipping straits and mining shipping harbors remain some of the most serious threats. (Ocean Studies Board, 2012)

Clearing mines is an inexact science

Between 600,000 and 1,000,000 naval mines of all types were laid in WWII. Advancing military forces worked to clear mines from newly-taken areas, but extensive minefields remained in place after the war. Air-dropped mines had an additional problem for mine sweeping operations: they were not meticulously charted. In Japan, much of the B-29 mine-laying work had been performed at high altitude, with the drifting on the wind of mines carried by parachute adding a randomizing factor to their placement. Generalized danger areas were identified, with only the quantity of mines given in detail. Many WWII era still exist today. Mines aren't the only UXO in the sea or close to land. Bomb fragments or UXO can still be found in Germany and England. More recently, Iraq and Afghanistan has a proliferation and specialization of IEDs. The exact number isn't known but the injuries to US soldiers and indigence children / population is dramatic. For a lightly technically salted discussion of the types of mines, deployment history, and countermeasures see Naval Mines in Wikipedia. (Naval Mines, 2020)

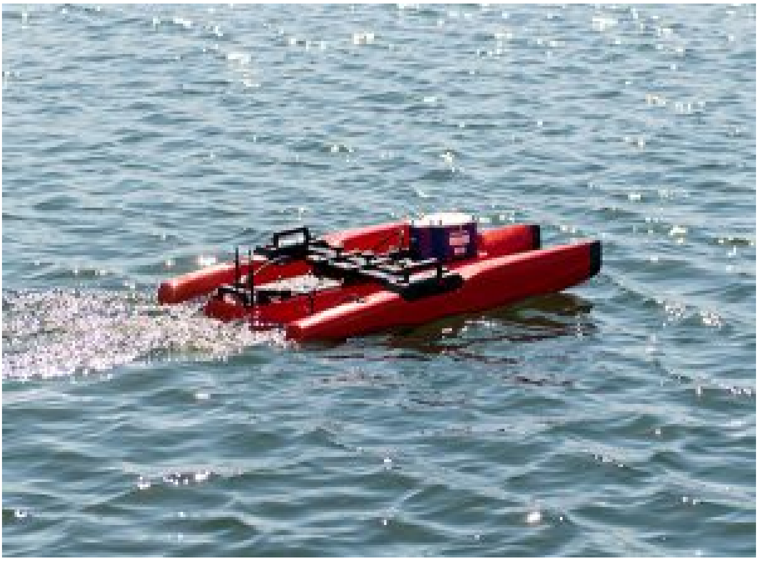
Innovation seems to be the name of the game in UUV / USV Surveying

Shallow water has always been a captain's concern and bottom conditions may obscure objects that are sonar resistant. Teledynemarine Oceanscience has produced a couple of interesting unmanned surface vehicles [boats] (USVs) for shallow water use, the 1250 and Boat 1800T – Trimble Edition. Teledynemarine Oceanscience Q-Boats® perform reliable remotely-controlled acoustic Doppler current profiling in streams, rivers, lakes and coastal waters all over the world. They reduce survey time, keep people safe during difficult conditions, and can access hard to reach locations. (Teledynemarine, 2020) See Figures 4.10 and 4.11

The Teledynemarine 1800-T Trimble edition has some key features:

- – Precise Trimble GNSS positioning and guidance
- – Real-time 2D survey for inspection and identification of obstructions
- – Cost effective method for ad hoc surveys
- – Increased safety and reduced cost: replaces dangerous diver inspection and expensive survey boat time. (Teledynemarine-1, 2020) [12]

Figure 4.10 Q-Boat 1250 designed specifically for shallow water applications



1250 Field shot
Source: (Teledynemarine, 2020)

Figure 4.11 Q-Boat 1800-T Trimble Ed.

Z-Boat fleet

Source: (Teledynemarine-1, 2020)

Conclusions: Why do the authors consider UUVs and USVs Disruptive Technologies of the future?

Several reasons.

Consider two interesting Black Swan events of the past and **how the technology exponentially grew out of small seeds**.

The date is December 17, 1903.

The Wright Flyer was the first successful heavier-than-air powered aircraft. Designed and built by the Wright brothers, they flew it four times on December 17, 1903, near Kill Devil Hills, about four miles south of Kitty Hawk, North Carolina. (Figure 4.12)

Figure 4.12 Wright brothers first flight photo

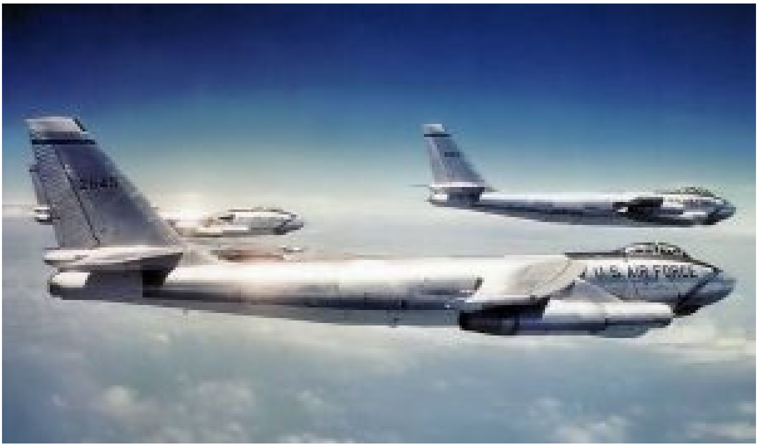
Source: (Crouch, 2014)

Results: Airline Industry, USAF, Space Command, FAA, Passenger and Freight Travel all over the world, bad airline snacks, unhappy TSA employees, Space Command. To prove the point see Figure 4.13:

17 Dec 1947–A mere 44 years to the day that the Wright brothers took to the air for the first powered flight of 12 seconds and traveled 120 feet at Kitty Hawk, NC, the Boeing B-47 Stratojet strategic bomber takes to the air for the first time. The Boeing B-47 Stratojet was a long range, six-engine, jet-powered strategic bomber designed to fly at high subsonic speed and at high altitude to avoid enemy interception. The B-47's primary mission was to drop nuclear bombs on the Soviet Union. With its engines carried in nacelles under the swept wing, the B-47 was a major innovation in post-World War II combat jet design and helped lead to modern jet airliners. The B-47 entered service with the US Air Force's Strategic Air Command in 1951. It never saw combat as a bomber but was a mainstay of SAC's bomber strength during the late 1950s/ early 1960s and remained in use as a bomber until 1965. Performance comparisons: Wright Flyer: wingspan: 40ft/ gross wt.: 604lbs/

range: 120ft/ top speed: 35mph/ ceiling: 10ft/ payload: 165lbs B-47: wingspan: 116ft/ gross wt.: 133,000lbs/ range: 4,000 miles/ top speed: 587mph/ ceiling 45,000ft/ payload 25,000lbs Incredible advancement in such a short period of time!

Figure 4.13 B-47 Stratojet



Source: (B-47 Stratojet, 2020)

The Date is: September 7, 1776

On September 7, 1776, during the Revolutionary War, the American submersible craft Turtle attempts to attach a time bomb to the hull of British Admiral Richard Howe's flagship Eagle in New York Harbor. It was the first use of a submarine in warfare. See Figure 4.14.

Figure 4.14 "Turtle"

Source: (Roland, 1977)

Results: Submarines, Submarine warfare, NAVSEA, precision munitions', improved propulsion, nuclear -power, UXO, 1.3 Trident

National Defense, advanced underwater technologies, Sonar applications, EO applications, extreme depth investigations, Search & Rescue, Sensors that work underwater and extreme conditions, pre-positioning of marine / maintenance platforms, oil exploration, and treasure hunting.

There will always be wars – somewhere. Chances are the US will be involved directly or selling munitions to a proxy. Terrorists might realize that mining the shipping areas is easier than naval ship warfare and its cost effective.[13] Sensors that work effectively underwater in hostile conditions!! This is amazing to say the least. Anyone who owns a recreational boat knows that they have to regularly clean the hulls of their boats and replace electronics 5x faster than the normal homeowner. Seawater is unforgiving to electronic and human life. UUVs and USVs handle DDD work so much better.

Just like UAS is revolutionizing the airline industry for all applications – especial defense, so will UUVs and USVs revolutionize the marine industries in both civilian and military applications. Bank on it.

Questions

1. Where do you see the next Black Swan event involving UUVs?
2. How might this technology be used to discover, recover, classify ancient artifacts?
3. How might UUVs be used to repair data communications cables at severe depths and tangled in unground obstructions?
4. Design a CONOP experiment for Counter UUV operations in foreign waters beyond claimed territorial rights.

References

B-47 *Stratojet*. (2020 December 17) Retrieved from: https://sk.wikipedia.org/wiki/Boeing_B-47_Stratojet

Bernstein, R. A. (29 June 2012). *MUNITIONS DETECTION USING UNMANNED UNDERWATER VEHICLES EQUIPPED WITH ADVANCED SENSORS*. Panama City, FL: NSWC PCD ESTCP Project Number MR-201103 Ver 7a.

Black Swan Definition. (2020, December 16). Retrieved from https://www.investopedia.com/terms: https://www.investopedia.com/terms/b/blackswan.asp#:~:text=A%20black%20swan%20is%20an,they%20were%20obvious%20in%20hindsight.

Bluefin Robotics. (2020, December 15). Retrieved from gdmissionsystems.com/underwater-vehicles/bluefin-robotics: https://gdmissionsystems.com/underwater-vehicles/bluefin-robotics

Crouch, T. (2014, March). *history-of-flight/wright-brothers-first-flight-photo*. Retrieved from www.airspacemag.com: https://www.airspacemag.com/history-of-flight/wright-brothers-first-flight-photo-annotated-180949489/

1. Sulzberger, J. B. (2009). *Hunting Sea Mines with UUV-Based Magnetic and Electro-Optic Sensors*. Retrieved from algebra.sci.csueastbay.edu/: http://algebra.sci.csueastbay.edu/~grewe/pubs/DistSensorNetworkBook2011/Atmosphere/UnderWaterSeaMineHunt.pdf

Kovacs, T. (1998). *Micromachined Transducers Sourcebook*. NYC: McGraw-Hill.

Leasko, R. (2014). *Munitions Detection Using Unmanned Underwater Vehicles Equipped with Advanced Sensors*. Scotts Valley, CA: CreateSpace Independent Publishing Platform (Amazon Media on Demand).

Naval Mines. (2020, December 16). Retrieved from en.wikipedia.org: https://en.wikipedia.org/wiki/Naval_mine#cite_note-minewar-83

Nichols, R. K. (2019, October 15). *Randall Nichols (October 15, 2019) Implications from Attack by Iran on Saudi Arabian Oil Fields (implications-from-attack-iran-saudi-arabian-oil-fields-nichols.* Retrieved from www.linkedin.com/pulse/: https://www.linkedin.com/pulse/implications-from-attack-iran-saudi-arabian-oil-fields-nichols/

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

Nichols, R. K., Mumm, H. C., Lonstein, W. D., Ryan, J. J., Carter, C., & and Hood, J.-P. (2019). *Unmanned Aircraft Systems in the Cyber Domain, 2nd Edition.* Manhattan, KS: NPP eBooks. 27. Retrieved from www.newprairiepress.org/ebooks/27

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

NSWC. (2020, December 15). *Warfare Centers NSWC Panama City.* Retrieved from www.navsea.navy.mil: https://www.navsea.navy.mil/Home/Warfare-Centers/NSWC-Panama-City/What-We-Do/

Ocean Studies Board, N. R. (2012). *Oceanography and Mine Warfare.* Washington, DC: Ocean Studies Board, National Research Council ISBN 0-309-51587-4.

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

REMUS -1. (2020, December 15). *REMUS 100 Technical Brochure (2017).* Retrieved from www.hydroid.com: https://www.hydroid.com/sites/default/files/product_pages/New_Generation_REMUS_100_%20Brochure_2017.pdf

REMUS -2. (2020, December 15). *REMUS 600 Technical Data.* Retrieved from www.hydroid.com/remus-600-defense-applications: https://www.hydroid.com/remus-600-defense-applications

REMUS. (2020, December 15). *REMUS 100 for Defense Applications Data Sheet.* Retrieved from https://www.hydroid.com/new-generation-remus-100-defense-applications: https://www.hydroid.com/new-generation-remus-100-defense-applications

REMUS -3. (2020, December 15). *REMUS 600 Technical Data Sheet.* Retrieved from www.hydroid.com/: https://www.hydroid.com/sites/default/files/product_pages/REMUS_600_Brochure_2017_0.pdf

REMUS -4. (2020, December 15). *REMUS 6000* . Retrieved from www.hydroid.com/: https://www.hydroid.com/sites/default/files/product_pages/REMUS_6000_Brochure_2017.pdf

REMUS -5. (2020, December 15). *REMUS 6000 Brochure.* Retrieved from www.hydroid.com/: https://www.hydroid.com/sites/default/files/product_pages/REMUS_6000_Brochure_2017.pdf

Roland, A. (1977). Bushnell's Submarine: American Original or European Import? *Technology and Culture: The Johns Hopkins University Press*, Vol. 18, No. 2 (Apr., 1977), pp. 157-174 (18 pages).

SERDP-ESTCP. (2012). *Munitions-Response/Munitions-Underwater/MR-201103-IR.* https://www.serdp-estcp.org/Program-Areas/Munitions-Response/Munitions-Underwater/MR-201103: NSWC PCD.

Teledynemarine. (2020, December 16). *Q-Boat_1250.* Retrieved from www.teledynemarine.com: http://www.teledynemarine.com/Q-Boat_1250?BrandID=13

Teledynemarine-1. (2020, December 16). *Z-Boat1800T_Trimble.* Retrieved from www.teledynemarine.com: http://www.teledynemarine.com/Z-Boat1800T_Trimble?BrandID=13

[1] Black Swan Event- A black swan is an unpredictable event that is beyond what is normally expected of a situation and has potentially severe consequences. Black swan events are characterized by their extreme rarity, severe impact, and the widespread insistence they were obvious in hindsight. (Black Swan Definition, 2020)

[2] The type of precision on sensors that work effectively underwater is an interesting science in itself. A primary reference on the subject is by Kovacs entitled "Micromachined Transducers Sourcebook." (Kovacs, 1998) There are many newer references, but students should start with this one to get a fundamental basis for the construction of specialized sensors before jumping into the next step in the process.

[3] (Leasko, 2014)Published in 2014 means that we are 6-7 years behind further advances in the sensors and hardening capabilities of the assets. However, students can get a lot of information and strategy from this UNCLASSIFIED report to chew on. This is why the author chose it as a primary reference for this chapter.

[4] The inventory has been obviously expanded and upgraded since this NSCW PCD evaluation. However, those upgrades have been in the sensor technologies not necessarily the UUV packages they arrive in. Concentrate on the beauty of being able to solve such a MCM detection / assessment / classification problem (underwater, cold temperatures, hostile environment, visibility issues, salt(s) corrosion, significant pressures, magnetic and electro-optic interferences, to name a few variables.)

[5] BOSS data will be collected over the seeded areas and analysis will follow to identify the number of targets detected by the system. The number of targets detected by the BOSS system will be cataloged and verified against the target listing and ground truth localization provided by the divers. (SERDP-ESTCP, 2012)

[6] Pd = Probability of Detection

[7] The magnetic moment is estimated by statistically fitting windowed time series to a magnetic-dipole model. The properties of the moment, including dipole strength and orientation, are extracted in this process. (SERDP-ESTCP, 2012)

[8] RTG/LSG data will be collected over the seeded areas and analysis will follow to identify the number of targets detected by the system. The number of targets detected by the RTG/LSG system will be cataloged and verified against the target listing and ground truth localization provided by the divers. (SERDP-ESTCP, 2012)

[9] The effectiveness of the RTG/LSG localization of proud to fully buried ferrous targets. (SERDP-ESTCP, 2012)

[10] Metric: Compare the RTG/LSG target localization with the diver provided target ground truth and determine the percentage of BOSS detections of seeded targets that can be identified as non-ferrous using RTG/LSG data. & Data Requirements:

RTG/LSG data will be collected over the seeded areas and analysis will follow to identify and localize the targets of interest. The RTG/LSG localization for each target will be cataloged and verified against the target listing and ground truth localization provided by the divers. (SERDP-ESTCP, 2012)

[11] Post Mission Analysis (PMA)

[12] Disclaimer: Author has no financial or legal relationship to vendors discussed in this chapter. Interest is purely technical.

[13] An example of this in the Straight of Hormuz which 5% of the world's oil transportation and gas purification processes are located. See author article on missile effects as a another POV: (Nichols R. K., Randall Nichols (October 15, 2019) Implications from Attack by Iran on Saudi Arabian Oil Fields (implications-from-attack-iran-saudi-arabian-oil-fields-nichols, 2019)

5. Challenging the Ammo Companies from Grass Roots [Mai]

Student Learning Objectives

1) The student will learn the 2nd

2) The student will learn the major influences that resulted in the modern guns and ammunition we enjoy today.

3) The student is encouraged to gain further study to understand how guns helped develop the United States, how guns protect the other amendments outlined in the bill of rights and keep and protect the Constitution of the United States of America.

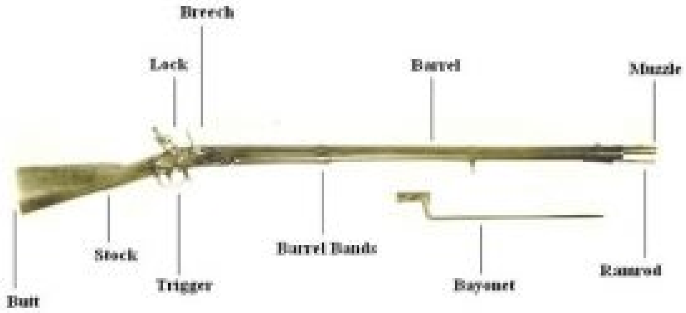
Introduction

The Constitution of United States of America 1791 (rev. 1992) Amendment II states explicitly: A *well-regulated Militia, being necessary to the security of a Free State, the right of the people to keep and bear Arms, shall not be **Infringed**.* (Madison, 1791) [1]

The wording leaves plenty of room for legal and political wrangling over the meaning of words like "well regulated," "militia," "right," "people," "keep," "bear" and "arms." (Ingraham, 2016) It does not leave room for any abridgement of the word Infringed.

The term 'Arms' in the 'Second' Amendment refers to weapons. The cutting-edge technology for weapons when the Amendment II was written, would have been the Revolution War era smoothbore musket (Figure 5.1):

Figure 5.1 American Revolution War era Smoothbore Musket



Source: (Ingraham, 2016)

Without gunpowder and bullets, a smoothbore musket was and is nothing more than a fancy walking stick or at best an artifact of history. This fact still relevant today. The relationship between gunpowder, bullets and their corresponding firearms/weapons/guns/arms is as intimate relationship as they come. One without the other, the guns and bullets intended function cease to exist and operate as they were designed. "….a musket is a smoothbore weapon much like a 12-gauge shotgun." (Harrington, 2013)

Few things have changed the world as much as when humans learned to harness the power of gunpowder. Gunpowder in its earliest form, was not called, 'Black Powder', until an early version of smokeless power was invented. At that time, it became known as 'Black Powder'. At the time of original discovery, it was black in color. Gunpowder was first thought to be discovered by the Chinese, they learned to use hollow tubes with gunpowder and projectiles to harness its power for something different than fireworks. Black powder formula in its purest variant is synthesized as Potassium Nitrate (saltpeter) 75%, Carbon (in the form of charcoal) 15%, and Sulfur 10% See Figure 5.2. (Wallace, 2018)

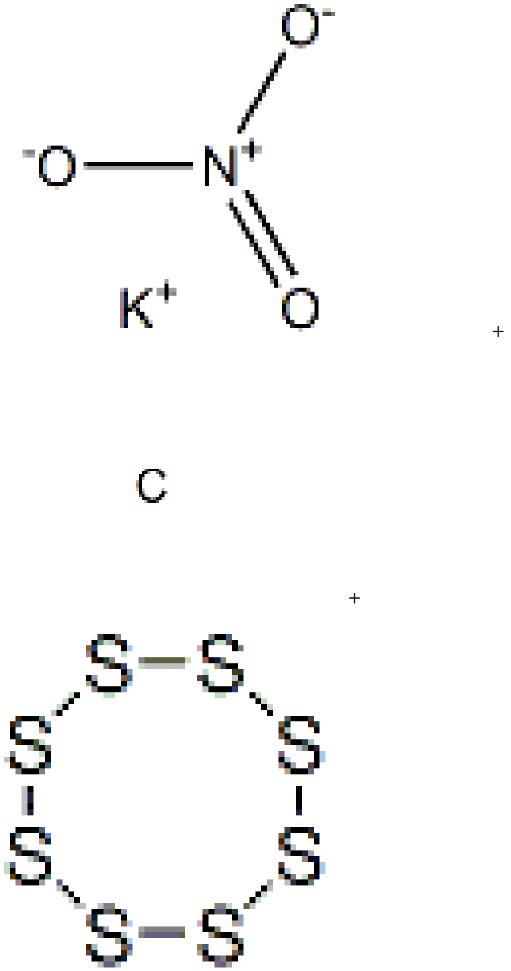


Figure 5.2 Gunpowder Composition

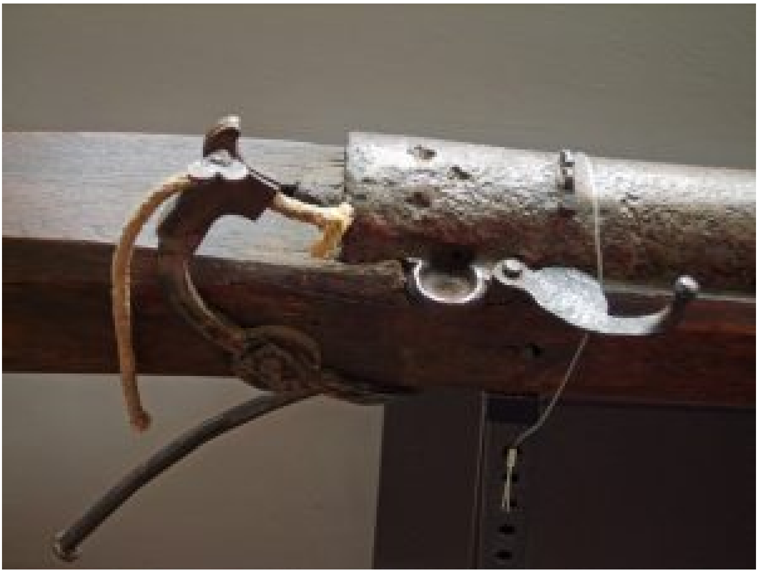
Source: (Wallace, 2018)

There have been many iterations in the development of guns, propellants, and bullets. The development and improvement of these three basics tend to occur within relative similar time frames. Guns over time have become more reliable and able to deliver multiple shots/rounds/bullets/projectiles in a shorter time. Black powder was the initial propellant of a bullet/projectile. As guns evolved, their propellants and bullets/projectile evolved with them and were dependent on gun evolution.

Relevant History – From Muzzle loaders to Modern Cartridges

The first useable guns started as a Matchlock (Figure 5.3) where a burning wick, typically made from hemp, was triggered to ignite a small amount of powder in a flash pan.

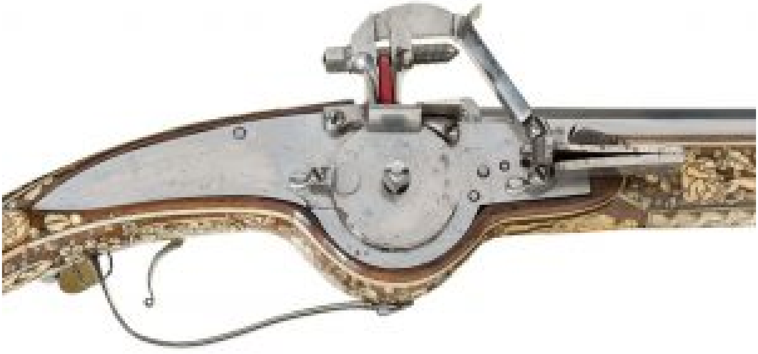
Figure 5.3 Match-Lock musket



Source: (Kolander, 2016)

This was difficult to control with a burning wick, which was not much more than a small burning piece of rope that maintained a hot ember. In an effort to eliminate the use of a burning rope, a wheel lock was designed to create a rotational force that created a spark. The wheel would be wound with a crank then released upon a pull of the trigger. The unwinding motion would create sparks and igniting the powder in the open pan (See Figure 5.4) .

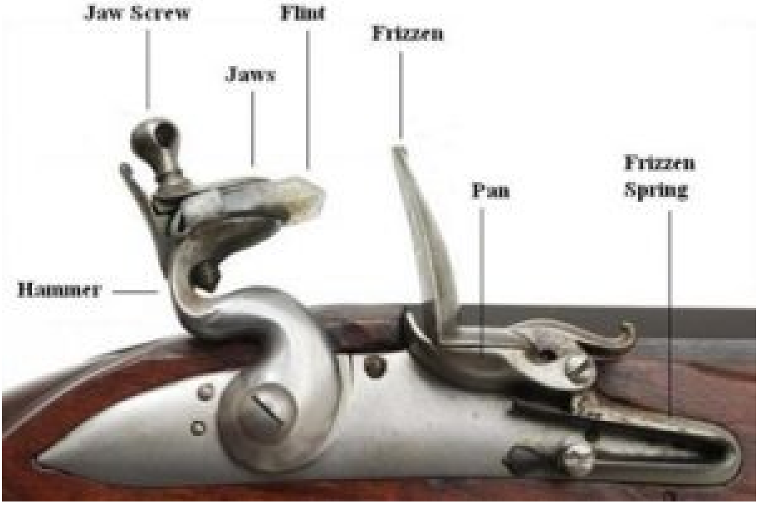
Figure 5.4 Wheel-Lock



Source: (Kolander, 2016)

This method was better due to elimination of the burning rope! However, being mechanical it was not without design problems and the open flash pan was still exposed and vulnerable to environmental moisture. (Kolander, 2016) The next most successful design was based on a piece of shaped flint-rock that was held in the jaws of a hammer. It would strike an extension, "Frizzen," on a flash pan cover.

Figure 5.5 Flint-Lock



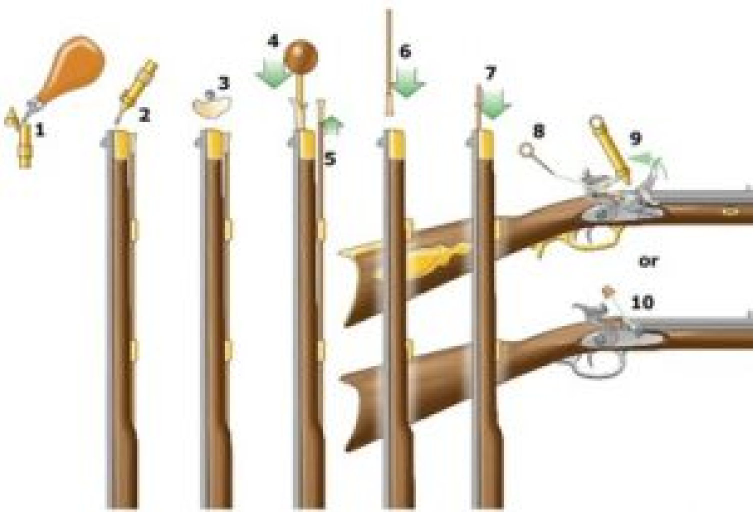
Source: (Kolander, 2016)

This design (Flint-Lock shown in Figure 5.4) covered the vulnerable gunpowder laying in the flash pan until the trigger was pulled allowing the flint to strike the Frizzen on the flash pan cover. That action forced the Frizzen out of the way and expose the gunpowder in the pan, allowing it to be ignited. It allowed for no burning rope and the spark created was relayed to the gunpowder being protected from moisture or spillage until an instant before firing. (Author, 2020) The gun was placed in halfcocked position while the flash pan was being loaded with powder. This design feature was to allow the operator to perform the pan loading procedure while not being in a fully cocked position, supposedly safer. However, sometimes the operator would set off the trigger in the halfcocked position either by accident or poor design. This is where we get the saying, ‘Don’t go off halfcocked!’ (Martin, 1761 (first Citation) 2021)

The initial, and up to this point, guns were considered muzzle loaders and their barrels were smoothbore. Muzzle loaders were loaded from the end of the barrel or what is commonly called the business end. Here are the loading steps for muzzle loaders (Figure 5.6):

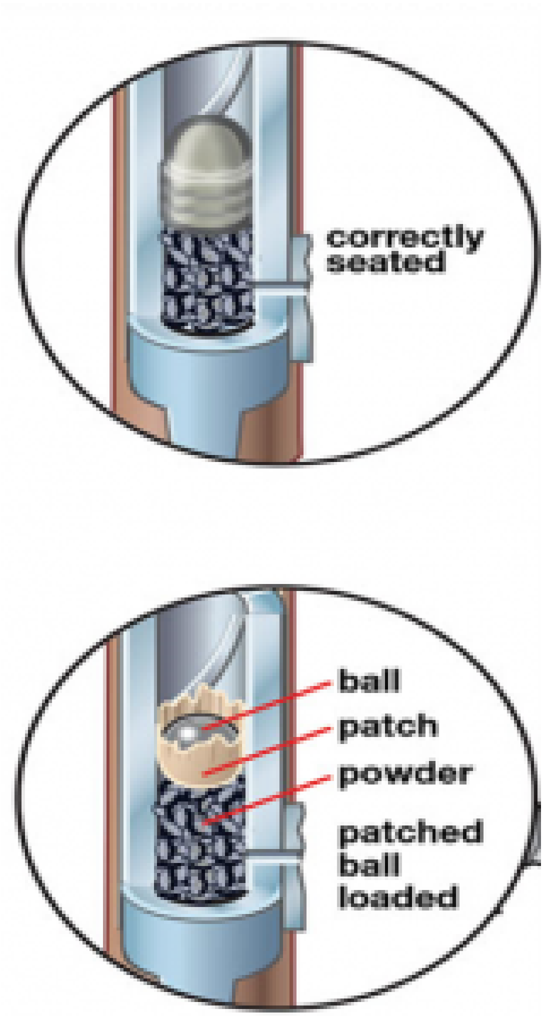
- Ø 1&2) a metered amount of gunpowder was first inserted into the muzzle end.
- Ø 3-7) a cotton wad with a round lead ball was inserted and tamped in the gun barrel until properly compacted.
- Ø 8&9) before being able to be fired, a small amount of gunpowder was then placed into the flash pan.
- Ø 10) Eventually, a percussion cap was developed, which sped up the operation. If everything had been done properly, the gun was ready to fire once the trigger was placed into the fully cocked position.

Figure 5.6 Loading Steps of a Muzzle loader



Source: (Martin, 1761 (first Citation) 2021)

Figure 5.7 Bullet position in a Muzzle loaded gun

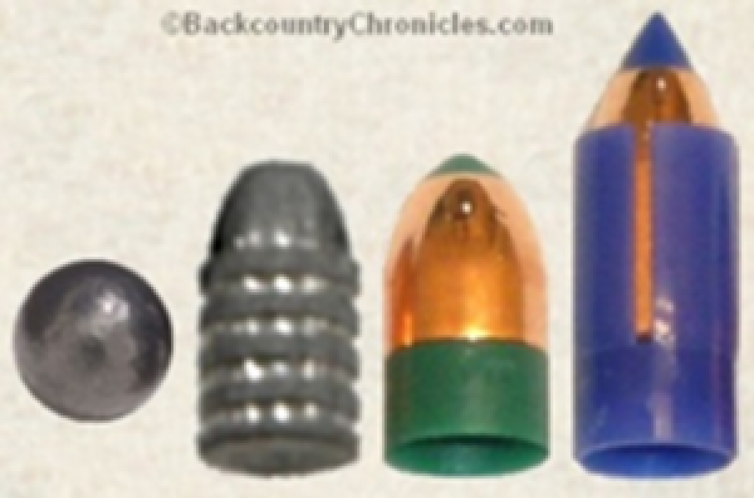


Source: (Youtube, 2021)

You can see how the ball in the lower portion of Figure 5.7 is positioned after loading. The upper portion of Figure 5.7 shows the bullet design after the round ball. Even though, it was called the mini-ball, it looked nothing like the earlier round ball. What the mini-ball did was capture all the escaping gases from the barrel. This increased muzzle velocity, distance, and accuracy. However, that caused the pressures within the barrel to increase which demanded that increased strength within the metallurgy of the barrel had to be increased. You can almost say that ammunition design and gun design became like a dog chasing its tail. An improvement forced and improvement in the other.

Eventually, breech loading guns were designed so that the powder and bullet could be loaded from the breech end. Several things had to come together to allow this to happen. The breech loading gun design had to be worked out at the same time as the cartridge had to be invented. The two were reliant upon each other.Early cartridges had a paper wrapped charge of powder and a mini-ball incorporated into the pre-assembled bullet or round. A round in the world of guns is considered to be a single bullet or called a shot. Many of the terms relating to guns and ammunitions become interchangeable and are usually familiar to the user or in this case the shooter.

Figure 5.8 Bullet design progression

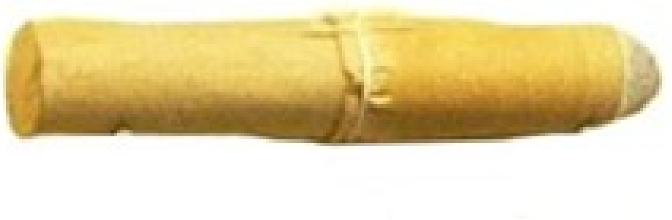


Source: (BackCountry Chronicles , n.d.)

Figure 5.8 shows how the bullet progressed in design. Muzzle loaded bullets and muzzle loaded guns are still used today.

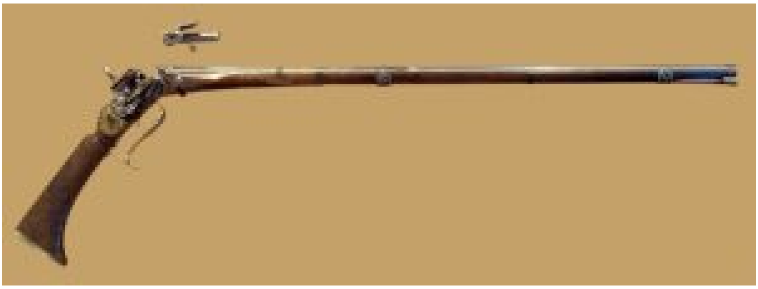
The first paper cartridges to include the bullet and placed into the breech were quickly replace with a canister called a shell or brass cartridge. A cartridge can be called a shell and vs. versa. A bullet can be called a shell, cartridge or a shell and ammunition. The context the words are used in are important. As the paper cartridge came into its existence breech loading guns became better.

Figure 5.9 Paper cartridge used in early breech loading guns



Source: (contributors, Paper cartridge, 2021)

Figure 5.10 Early breech loader w/ fitted cartridge



Source: (contributors, Breechloader, 2021)

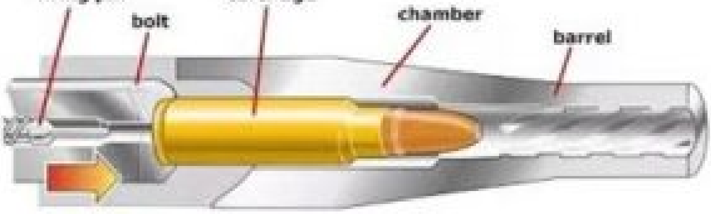
The above Figure 5.10 was a very early breech loading design. The actual cartridge was loaded much like that of the earlier muzzle loaders. However, the loading of the cartridge was then entered into the breech end of the gun.

Eventually, the paper cartridge led to advent of the metallic cased gunpowder and bullet. See Figure 5.11.

Figure 5.11 Bullets w/ brass casing

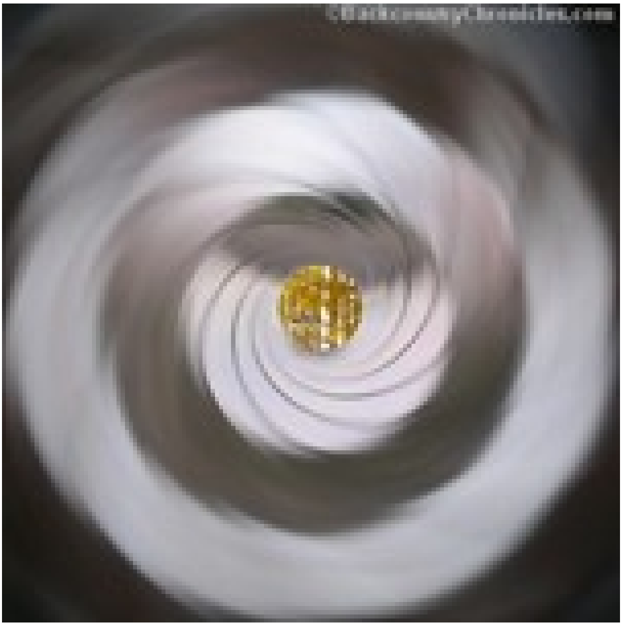
Source: (Jeff, 2020)

Figure 5.12 Metallic cased bullet in chamber of breech loaded gun



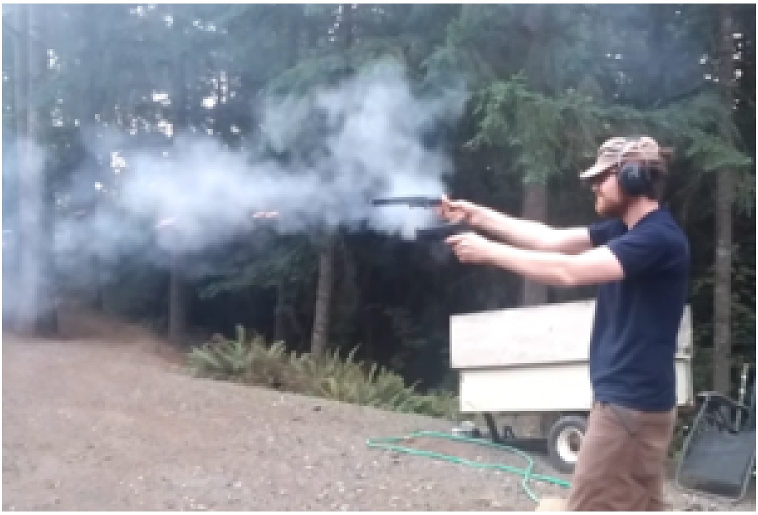
Source: (II, 2017)

Figure 5.13 Rifled barrel



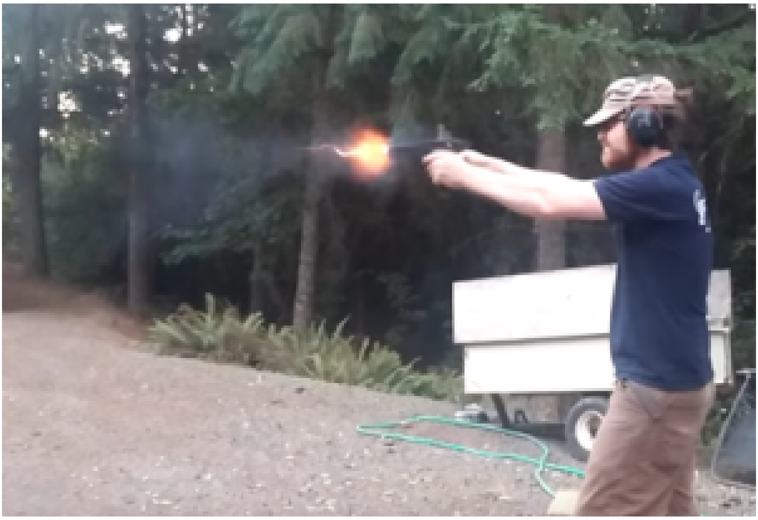
Source: (BackCountry Chronicles , n.d.)

Figure 5.14 Black powder



Source: (YouTube, 2021)

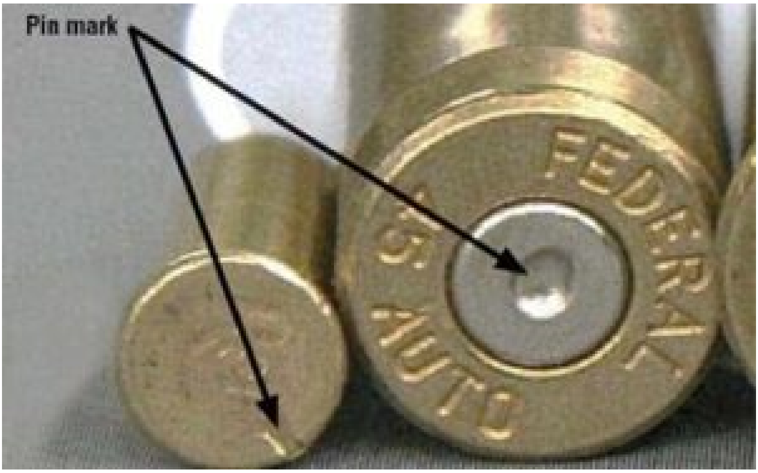
Figure 5.15 Smokeless Powder



Source: (YouTube, 2021)

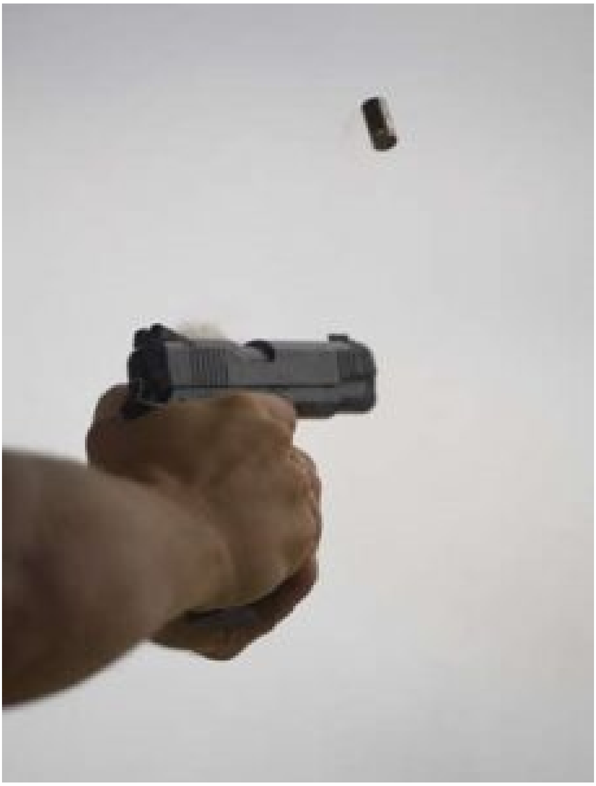
Several events came together to make a more powerful, accurate, reliable, and easier to use gun. Those events included: Preassembled metallic case shell (see Figure 5.11), Breech loading gun (see Figure 5.10 & 12), Smokeless powder (see Figure 5.14 & 15), improved metallurgy, gas operated case extraction and rechambering (see Figure 5. 16), center fire ammunition (see Figure 5. 16), Barrel rifling (see Figure 5.13). This discussion is by no means an all-inclusive recreation of the history of firearms and ammunition, only the highlights that made major shifts in the trajectory of guns and ammunition outcome are pointed out here.

Figure 5.16 Rim fire vs Center fire



Source: (SIMMONS, 2020)

Figure 5.17 Shell ejection and reloading using excess gas



Source: (Sagi, 2021)

Summary

To reach the technology of modern weapons (see Figure 5.17), it was important that a smokeless power was developed. The smokeless powders do not only give us less smoke but also greater chamber pressures that could push a soft metal such as lead through a rifled barrel that had no leakage around the bullet. The rifling spins the bullet giving it greater accuracy but also requiring higher chamber pressures to push it through the barrel that was fit so tightly. Only a shell that houses its propellant and bullet could assist with the tight fit. It also allowed for ease of loading and once the round was expended a grove at the base of the shell could be gripped by an extractor that is powered by some of the excess gas of the spent round to automatically remove the spent shell casing. This action was important to take place at the breech and is why breech loading designs became so very important to the semi-automatic weapons we see today. The early smokeless powder was from a nitrocellulose and nitroglycerin mix that gave less smoke, higher chamber pressure, by complete combustion and left less corrosive remains since it was mostly consumed, unlike Black powder that would not work in today's guns.

Figure 5.18 Modern AR-15 photo courtesy of Randall Mai

Today's shooters are typically more informed than ever before. Many hold conceal/carry licenses, have taken hunter safety courses, abide by all laws and regulations, some belong to hunting clubs where ideas and understand is shared and peer reviewed. Their reasons for owning and shooting guns vary from sport/target shooting, personal protection, game hunting to provide food for their families. Today's shooters understand the need to practice because shooting is a perishable skill and the need to be familiar with their gun is a must. This should be understood then that a gun owner will not buy a gun to put in a box unless they intend act as a collector. Just like a pilot that flies, a gun owner must practice. That being said, ammunition will be consumed on a regular basis; therefore, there is a continual need to replace a gun owner's ammunition stock.

The Nub – Ammunition shortages and government suppression of stocks

At the start of this writing there was rationing of ammunition and complete shortages. The next section was happening just 20 hrs. while these very words being typed:

[*OREM, Utah* — an amazing sight outside a Utah County gun store as hundreds lined up to buy ammo.

The line stretched around Gunnies, located at 396 South State Street in Orem, all throughout the day on Saturday.

Some traveled as far as Kamas to wait for hours in the cold.

KSL-TV spoke to a number of people — some said they came for the restocked ammo; others were more anxious. They mentioned current political events — the GA runoff, a soon-to-be transfer of power and Wednesday's violence at the U.S. Capitol. Many in line also yelled out: "Biden is going to take our guns."

"There were people down here, 200 lined up before the store opened," said gun owner Mark Greer who drove from South Jordan.

Recently, there has been a shortage on the most popular ammo.

"It goes fast because there's none out there," said Greer.

The ammunition shortage started in late spring of 2020 when the coronavirus altered manufacturing.

Ammo has been on and off shelves, but Gunnies restocked its AR-15 ammo supply on Saturday.

"Perfect storm for gun supply," said gun salesman Chris Hansen.

The masses came to get their hands-on part of that shipment.

One Gunnies employee couldn't get the ammo on shelves fast enough.

“This case has 1,000 rounds,” said the worker. “I have gone through 10 boxes already in two hours.”

Because the store has seen hoarding in the past, there was a limit placed on what a customer could buy.

“On this 223-556 that we got in that everybody’s here for today, we’re allowing 200 rounds per customer,” said Hansen.

Gunnies sales reps said they have seen some of their busiest days ever this year, adding that the shop is not usually busy like this in January.

“We have seen a rush on guns and ammo before – but never in January,” said Hansen. “Typically, after Christmas it slows down, but this year has been just the opposite.”

They mentioned that when Obama was elected in 2008 and again in 2012, there was a run-on guns and ammo.

Those in line expressed different reasons for showing up.

“With the changes coming of a new Presidential Administration, people are concerned about their 2nd Amendment rights,” said Greer. “That’s why you see so many here today.”

“People are coming in and they are pretty scared. They feel they are being attacked,” said Gunnies employee Josh Hansen. “They feel the need to fight back, or at least protect themselves.”] (Tait, 2021)

According to United States Government Experts, any proposed amendment to the Constitution needs to be passed by both the House and the Senate, with two-thirds majorities. It would then need to be ratified by three-fourths of the 50 states, or 38 of them. Historically, that’s proved unlikely and challenging. In the history of the United States, the only amendment that’s ever been repealed is Prohibition. (Tait, 2021)

So, what is happening? With close to 8 million new gun owners there is no doubt that there is increased demand on the ammunitions supply chain. But why are there so many new gun owners? Is it because of the individuals wanting to impose gun control on the nation? Is it because of the riots of 2020 in the

Portland area? Is because of the worries of the pandemic of 2019? The pandemic did create the toilet paper shortages, but they rebounded quickly. You *cannot go* to any of the stores and find ammunition. Even though the manufactures claim they have increased production.

One more little item almost 7+ years old and no one really took notice.

"The Denver Post, on February 15th, ran an Associated Press article entitled *Homeland Security aims to buy 1.6b rounds of ammo*, so far, to little notice. It confirmed that the Department of Homeland Security has issued an open purchase order for 1.6 billion rounds of ammunition. As reported elsewhere, some of this purchase order is for hollow-point rounds, forbidden by international law for use in war, along with a frightening amount specialized for snipers. Also reported elsewhere, at the height of the Iraq War the Army was expending less than 6 million rounds a month. Therefore 1.6 billion rounds would be enough to sustain a hot war for 20+ years. In America." (Benko, 2013) The interesting question to ponder is how much more ammo has been purchased since 2013 for DHS "practice?"

Figure 5.19 Empty shelves at a local gun store courtesy of Randall Mai

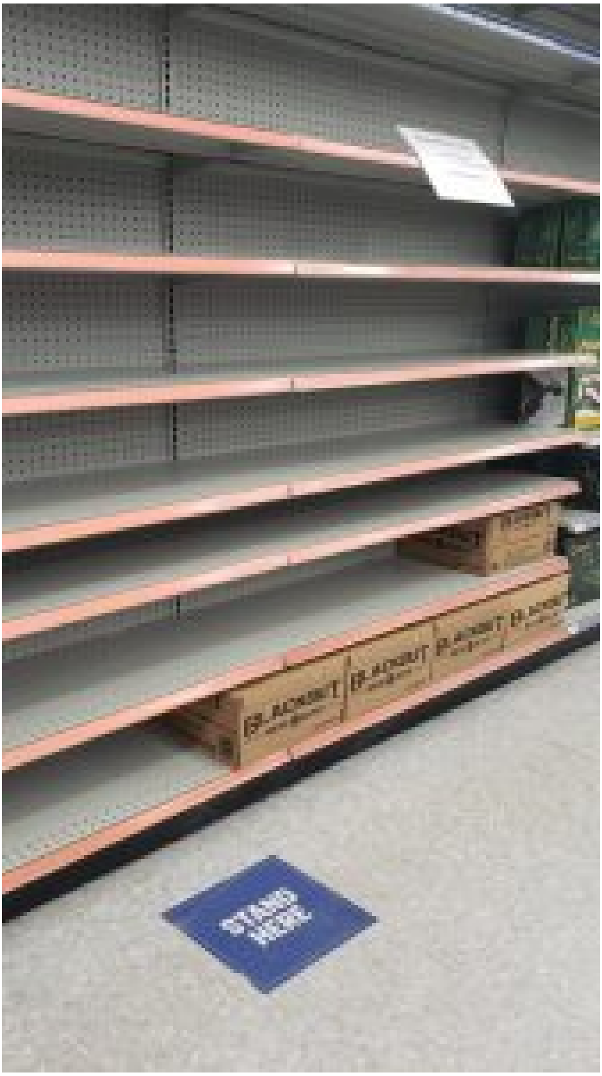
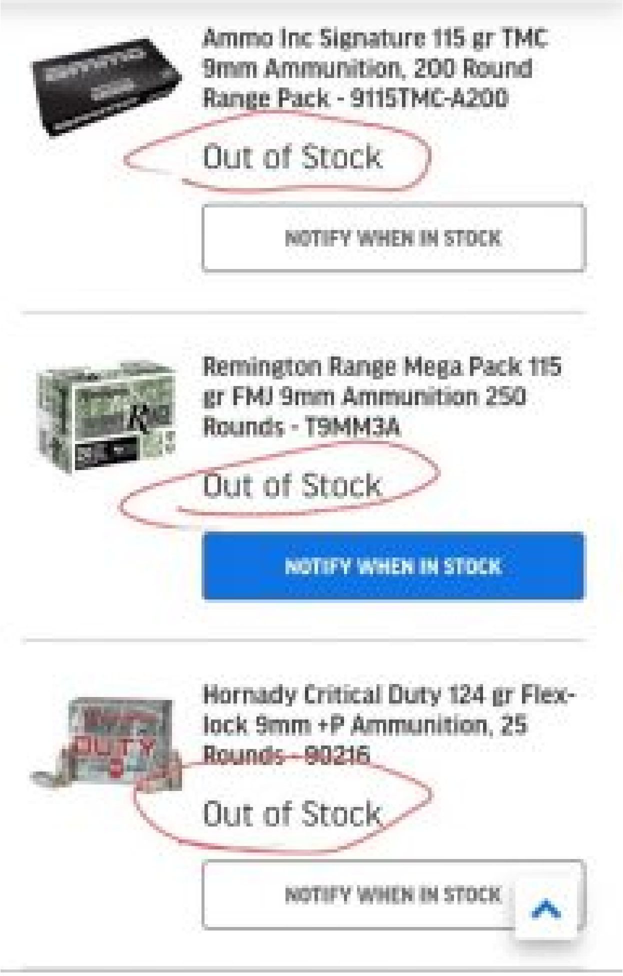


Figure 5.20 online buying Courtesy of Randall Mai



Ammo Inc Signature 115 gr TMC 9mm Ammunition, 200 Round Range Pack - 9115TMC-A200

Out of Stock

NOTIFY WHEN IN STOCK

Remington Range Mega Pack 115 gr FMJ 9mm Ammunition 250 Rounds - T9MM3A

Out of Stock

NOTIFY WHEN IN STOCK

Hornady Critical Duty 124 gr Flex-lock 9mm +P Ammunition, 25 Rounds - 90216

Out of Stock

NOTIFY WHEN IN STOCK

It is possible that hording, scalping, increased demand, fear buying will throw off the normal supply and demand. However, every caliber of ammunition and most of the guns are gone. It starts to make a person wonder if there is more at play. Especially when the incoming president says he is coming for people's guns.

It should be noted that the 2nd Amendment is considered a right from God and not given to people by the government. But it is considered to be protected by the government, as it says, '…shall not be infringed!' This may be true but by not supplying ammunition to the public has the same effect as disarming the American public and as stated at the start of this chapter, without ammunition, a gun is nothing more than a stick. Some gun owners have resigned themselves to reloading their own ammunition. But stores do not have reloading supplies. It is a little ironic that it's not just the popular calibers no components are available to reload but ever caliber has NO supply. That makes no sense!! Every re-loader will tell that they do not have the apparatuses to reload all calibers across the caliber spectrum. It makes no economic sense and would simply not be cost effective. Another red flag!

Ammunition – Like water in an ocean, everywhere but not a drop to drink

What do gun owners do for ammunition? Let's take a look at what other authors are saying: Ammunition purchasers across America—or make that would-be purchasers in record numbers—are finding shelves bare, and unfortunately that's hardly breaking news. If this were simply a Christmas-season run, we could insert a Grinch joke here and assume things would return to normal after the holidays. But, in fact, this shortage, as many readers can attest, traces back at least to spring when COVID mania shocked the country and has since intensified under an unprecedented chain of cultural phenomena. Many gun owners feel that the only way to ensure they have ammo when they need it is to buy in bigger-than-normal quantities, and the result is hoarding.

As detailed in a recent "Keefe Report," nearly any caliber that'll go bang in whatever quantity is up for grabs is snapped up almost immediately. (Keefe, 2020) Consumer frustration is rampant, and there's a real concern about personal- and home-defense shooters not being able to get ammo they need to be prepared.

Anyone who's been a gun owner and at least a semi-active shooter going back a decade can remember earlier shortages, and while those were truly galling and nationwide, this one's different. It's even more widespread and more pervasive in terms of unattainable calibers—nearly all of them, from what we're hearing. Like that other lingering current event on everyone's mind, we're left wondering: When it will end?

That question is landing in record numbers, too, in the inboxes, customer-help lines and direct attention of nearly everyone working for America's ammunition manufacturers. We talked to a few key executives who spoke about the inquiries and criticism coming their way—so much of it that, at times, it threatens to impede normal operations—and who shared anecdotal requests that would be comical if the shortage weren't so serious. They were also frank in answering the question about when relief will come, and while there are bits of good news, the outlook for returning to normal supply-and-demand in 2021 remains murky. (Zent, 2020)

Let's Listen to the Manufactures (See Table 5.1) : (Zent, 2020)

Table 5.1 Listen to the Manufacturer's

Hornady – Jason Hornady	"Ammunition is the new toilet paper……
	"The big problem here-we've seen it before, but not like this-is folk's panic thinking they won't be able to get any more and so buy more than normal…
	"We make it one day and ship it the next."
	"I've seen shortages six times in my career," said Hornady, "but the difference this time is the string of events—Walmart, Virginia [anti-gun legislature], coronavirus, riots, an influx of [6-7 million] new gun owners, a bad election.

Vista Outdoor – Chris Metz	“After seeing big sales spike as a result of COVID, civil unrest and then so many more people getting out this year going hunting – license sales are up like crazy…… “But ever since Joe Biden was named the presumed presidential-election winner, we have seen a reaction in the marketplace, and it hasn’t subsided… “Demand has been strong across the board—any type or caliber of handgun ammo; small rifle, big rifle, hunting rifle; even rim-fire—all of it really picked up.

“We make it one day and ship it the next.” “We talk to a big database of users on a monthly basis, and one thing we’re noting is that what we call ‘heavy shooters,’ those who shoot 10,000 rounds or more per year, a lot of them haven’t been purchasing. They’ve seen the frenzied activity and are holding back in hopes it’ll subside. Well, we all know what’s going to happen when they work through their stockpiles and at some point, come back to the market. So, no, we don’t foresee any slowdown in the demand in 2021.”Jason Hornady vowed his company is doing everything it can to meet that demand but not without concerns. “Our workforce has pushed hard through this but is fatigued. We have an issue finding people to keep the machines running, and trust me, everyone is working a *lot* of hours,” he said. “I was in a camp back in September where someone commented that such-and-such gun company was ‘shipping *only* 20 percent more than last year’ and that ‘they just don’t care about making more.’ Please. There’s no factory of any kind that doesn’t want to make as much as they possibly can. That’s us. We’re doing as much, making as much as we can,’ said Hornady. “For 2020, we’ve shipped 30 percent more than we did a year ago. We are adding capacity, but according to an existing plan.

“I’ve seen shortages six times in my career,” said Hornady, “but the difference this time is the string of events—Walmart, Virginia [anti-gun legislature], coronavirus, riots, an influx of [6-7 million] new gun owners, a bad election. It all adds up. Right then, hunting season comes along, and you know what consumer is the maddest? The ones who normally buy two boxes of deer ammo a year. They go into their local gun shops and can't believe [the shelves are bare]. Our local gun-store owner called to tell me about two guys who came into his place looking for hunting ammunition, and then they told him that Hornady has been shut down since June. Crazy!(Zent, 2020)

"At the same time, COVID is a reality for us, too," said Hornady. "If an employee has to quarantine, even if they're not sick, we can't just send a loading press home with them. We've had to spread out and guard against super-spreader events so that it won't shut down a big part of the factory."

Both industry leaders cited shortage of raw materials as a concern, too. Hornady said his firm laid in a "... six-month supply at the first signs of how serious COVID might be. We're grateful that we did, but when you have a six months' worth of material, you also have a space problem. And not just copper and lead, it's also packaging, staples and other supplies. Did you know there's a shortage on the DOT-approved cardboard required for shipping our loaded ammunition? We're now having to ship in white boxes instead of brown ones because we can get more of that."

Chris Metz echoed that, saying it's been challenging for his ammunition brands—Federal, Speer and CCI to keep enough brass and primers on hand, despite the fact that Federal and CCI are two of the world's biggest primer manufacturers.

The same has been true for Vista's newest brand, Remington Ammunition, which the outdoor conglomerate acquired in September. "Both the workers at Remington and those of us from Vista see this as a marriage made in heaven," said Metz. "And it couldn't have come at a better time from a capacity standpoint. That factory wasn't working, which contributed to the shortages." The high-production facility in Lonoke, Ark., which for decades has produced the familiar green-and-yellow-boxed ammunition, is ramping up this month, offering one glimmer of hope that the supply side will be buoyed.(Zent, 2020)

"We've been working to rehire 400 to 600 furloughed workers, have been retraining them and getting the manufacturing processes back in place," reported Metz. "Supplies of Remington ammunition should be coming back on the market in early January. We all grew up with the brand, we love it, and we know we're not alone."

It will also be interesting to see if some of the other names in U.S. ammunition manufacturing are able to step up production on the heels of developments in this pivotal industry segment. SIG Sauer, for one, is operating an ultra-modern plant in Jacksonville, Ark., and its loads have gained traction with several gun-owner segments.

Sierra Bullets began selling its own branded cartridge a few years back, primarily hunting rifle cartridges, but the company made a strong growth statement when it acquired Barnes Bullets during the Remington Outdoor Corp asset sell-off in late September. The Barnes installation in Mona, Utah, while not as large as the legacy brands' plants, has a history of producing a full range of highly regarded rifle and pistol ammo, and now that it's out from under the Remington corporate umbrella, is expected to again contribute more to the national supply chain.(Zent, 2020)

A third maker that bears watching is Fiocchi USA, which announced in July that it will be expanding its stateside manufacturing by adding a facility in Little Rock, Ark., to supplement an existing plant in Missouri. Expect to see an expansion in domestic-made Fiocchi product lines, which produces top-quality rifle, pistol and shotshell products. Furthermore, Fiocchi announced it has acquired Baschieri & Pellagri, who's high-end shotshells are the gold standard for many European clay's competitors and hunters, and they too will be produced in the United States.

When contacted, a spokesman for the Winchester and Browning ammunition brands simply commented: "Like many manufacturers in the shooting-sports industry, we are experiencing extremely high demand for our products. We are continuing to manufacture and ship our high-quality products on a daily basis."

Those final words really tell the tale. All hands in the ammunition industry are waging a daily battle to meet the unprecedented demand. Though there are a few reasons to expect supply to increase, those who know this market best are forecasting continued shortfalls. *AmericanRifleman.org* will keep you posted as developments occur. (Zent, 2020)

Other difficulties affecting the ammunition industry are the fact that many of the raw materials are no longer manufactured in the United States. For example: any lead is either imported or reworked. Many store owners have claimed they here that primers are in short supply. It is easy to understand when components can be made cheaper elsewhere why it would be tempting to outsource it; however, it makes about as much sense to outsource of critical computer systems to a country that does not have America's best interest at heart.

Let's play this shortage scenario out to absurdity. Let's say no more ammo is ever manufactured ever again. What then? It is pretty hard to follow a business model in times like these. It is very easy in business to get in over your head. Scaling up to a new level of production is not always wish. Yes you can increase output of existing machines and increase schedules. But to what percent? If you over commit in times like this by purchasing more equipment, what happens if there is a return to productions levels prior to the pandemic, administration change, hording and fear purchasing? You could easily bankrupt a busy in uncertain business cycles, like too much demand. Better to stay in business and let frustrations play out.

Let's not forget the North Korean's gave a U.S. lead NATO army a run for their money in the 1950's. (Figure 5.21) There source of small arms ammunition was created underground in caves and still almost defeated NATO. Production can be increased but to what level and how long can that be sustained in a society where people perform based on greed rather than with a whip at their backs.

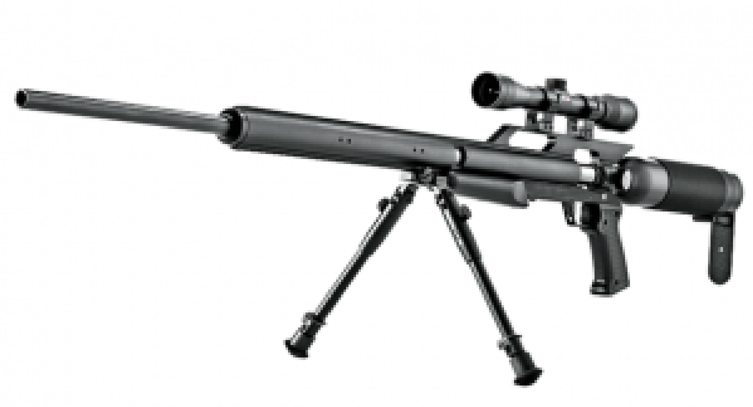
Figure 5.21 N. Korean small arms manufacturing

Source: (Netflix, 2021)

How do we get away from all the scarcity? What paradigm shift can occur? Well, it already has! There are individuals that believe they can reproduce or substitute materials by either acquiring them from other sources or recycle parts that are somewhat available. The problems these individuals will encounter is substandard materials/parts. They will be difficult to obtain and most likely inconsistent in quality. This is not what I would consider a good replacement for the current ammunition industry. By no means could scavenging parts ever attain the level of production needed to supply all gun enthusiasts with replaceable ammunition. Because the base elements for bullets would have to come from such things as old car batteries, dental waste, plumbing waste, wheel weights, scrap yards, thrift stores, or maybe old sailboat ballasts/keels, yard sales, roofing companies. Then there would have to be knowledge of component assembly. Building dyes and running a foundry would be another skill-set most will never have. What about the propellant? Will you have the license to create your own propellant or knowledge? Not only is it illegal to manufacture explosives because personal and public safety would be in danger if every gun enthusiasts were running around trying to manufacture their own propellants. Casing and primers, where would they come from?

The paradigm may have already shifted right under the noises of the gun world. There may already be a replacement for the gun and its history of using propellants that detonate. Who needs gunpowder when you have air??

Figure 5.22 AirForce Texan

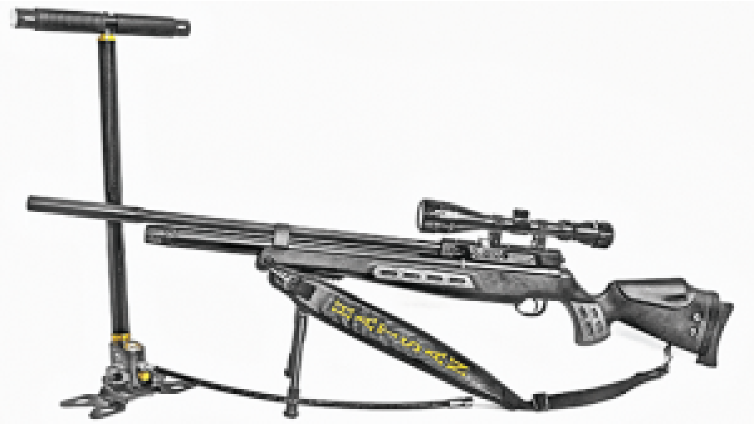


Source: (Depot, 2020)

AirForce Air guns (Figure 5.22) says this is the most powerful production air rifle in the world. It shoots .45-caliber lead projectiles at up to 1,000 fps for over 500 foot-pounds of energy. This is a single-shot, precharged pneumatic with a sidelever action and a 490-cubic-centimeter pressure tank equipped with a built-in pressure-relief device. It will effectively contain up to 3,000 psi of pressure. (Larson, 2015)

Several calibers of air rifles are being manufactured and many of the States are allowing hunting with these air guns. Calibers range from .177, .22, .25, .30, .338, .45, .50. There are .25 caliber guns that can shoot up to 60 times before needing a charge. Air guns you could argue are in their infancy much like the early musket muzzle loading guns. As materials, design, and projectiles improve its anyone guess to the level of quality, accuracy, and stopping power these forms of weapons could achieve.

Figure 5.23 Hatsan Big Bore Carnivore



Source: (Depot, 2020)

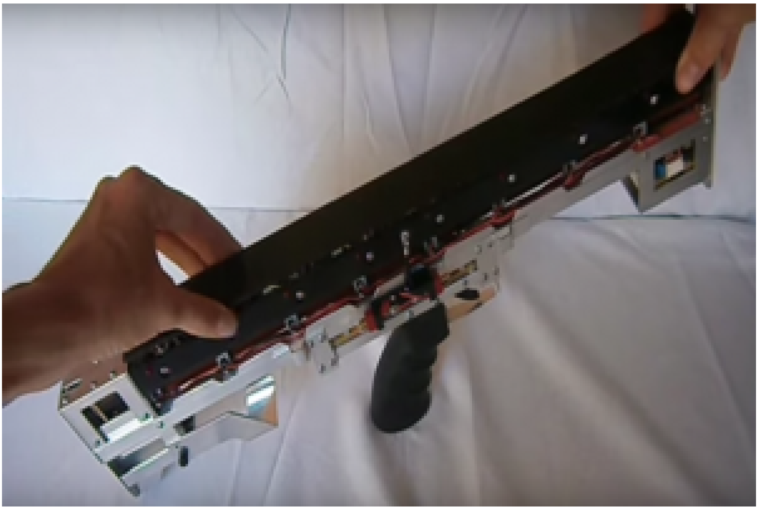
Figure 5.24 Whitetail with an Airgun

Source: (Clayton, 2019)

A 45 caliber Airforce Air guns Texan air rifle on the Dale River Ranch (www.daleriverranch.com) to harvest a whitetail buck with an air rifle. (Clayton, 2019)

The air rifle may not be the only firearm that totally disrupts the powdered firearm industry. A new kid is on the block and he is definitely in his infancy but shows beautiful room for improvement that would definitely be at its matchlock stage. What gun am I referring to you may wonder!! The hand-held coil gun. This gun is definitely in its infancy. Even though this gun appear to bigger and bulker, it tends to be lighter. That is because it is not slinging around bunches of weight from the cartridge ammo. Thanks to lead being too heavy. However, the coil gun makes some weight up with coils that are heavy. (See Figure 5.25)

Figure 5.25 Coil gun



Source: (YouTube, 2021)

Conclusions

Since 2020 ammunition has become less available for all calibers in all places. Retailers, in store and online have seen less and less ammunition come into theirs stores. The manufactures have claimed to step up their operations. But it seems to still be getting worse. The claim is the COVID, safety fears, hording, administration changes, increased gun ownership is having something to do with the lack of availability. It may not be the agenda, but the hard reality is that by not keeping the store shelfs stocked it has the effect of disarming the American public. And let's not forget the incoming administration has been noted for saying they want to take the guns away. Whatever the situation really is, people dedicated to having guns will switch to using something as air rifles. If they then try to regulate air, the author will have to claim that the desire to disarm the American public was the desire from the beginning. So rather than the air guns being the disruption, the government is the true disrupter.

Questions

1. What basic components and tools are necessary to load you own ammunition?
2. What would be necessary to build a small factory, secure the basic materials and manufacture ammunition at less than 50% of the market price. Develop the economic business model and consider the regulatory and public responses. Consider risks. Consider expected profit and market share.
3. What legal / international / ATF road blocks must be hurdled to import components not readily available as surplus or recycled materials?

References

Author, W. (2020, September 7). *Wikipedia*. Retrieved from Flintlock: https://simple.wikipedia.org/w/index.php?title=Flintlock&oldid=7100109.

BackCountry Chronicles . (n.d.). *BackCountry Chronicles*. Retrieved 2021, from Choosing a Modern Bullet for your Modern Muzzleloader: https://www.backcountrychronicles.com/muzzleloader-bullets/

Benko, R. (2013, March 11). *1.6 Billion Rounds Of Ammo For Homeland Security? It's Time For A National Conversation*. Retrieved from forbes.com: https://www.forbes.com/sites/ralphbenko/2013/03/11/1-6-billion-rounds-of-ammo-for-homeland-security-its-time-for-a-national-conversation/?sh=1152e4f4624b

Clayton, K. J. (2019, November 15). *Ketr*. Retrieved from All things considered: https://www.ketr.org/post/lukes-first-whitetail-airgun

contributors, W. (2021, January 9). *Paper cartridge*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Paper_cartridge

contributors, W. (2021, January 3). *Breechloader*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Breechloader

Depot, A. (2020, December 31). *Airgun Deport*. Retrieved from What is the most powerful Airgun: https://www.airgundepot.com/vault/author/admin/

Harrington, H. T. (2013, July 15). *Revolution, Journal of the American*. Retrieved from All things Liberty: https://allthingsliberty.com/2013/07/the-inaccuracy-of-muskets/

II, J. H. (2017, October 30). *What happens if you put a bullet into a gun backwards*? Retrieved from Quora: https://www.quora.com/What-happens-if-you-put-a-bullet-into-a-gun-backwards

Ingraham, C. (2016, June 13). *Economic Policy*. Retrieved from The Washington Post: https://www.washingtonpost.com/news/wonk/wp/2016/06/13/the-men-who-wrote-the-2nd-amendment-would-never-recognize-an-ar-15/

Jeff. (2020, October 28). *Best Deer Rifles*. Retrieved from Big Game Logic: https://biggamelogic.com/deer-rifles/

Keefe, M. (2020, December 15). *The Keefe Report: Where's All The Ammo?* Retrieved from www.americanrifleman.org/: https://www.americanrifleman.org/articles/2020/12/15/the-keefe-report-wheres-all-the-ammo

Kolander, J. R. (2016, April 1). *RockIslandauction*. Retrieved from Gun Blog: https://www.rockislandauction.com/riac-blog/what-is-a-wheellock-mechanism

Larson, D. (2015, December 15). *Most powerful air-guns*. Retrieved from Tactical-Life: https://www.tactical-life.com/firearms/10-of-the-most-powerful-airguns/

Madison, J. (1791). *Bill of Rights Institute*. Retrieved from Primary sources: https://billofrightsinstitute.org/primary-sources/bill-of-rights

Martin, G. (1761 (first Citation) 2021, January 7). *The meaning and origin of the expression: Go off at half-cock*. Retrieved from The Phrase Finder: https://www.phrases.org.uk/meanings/half-cocked.html

Netflix. (2021, January 10). *Modern Warfare: The Korean War.* Retrieved from Netflix: www.netflix.com

Sagi, G. (2021). *123rf*. Retrieved from empty shell 15885089: https://www.123rf.com/photo_15885089_empty-shell-being-ejected-from-a-semi-automatic-handgun.html

SIMMONS, M. (2020, December 3). *Gun advice*. Retrieved from Rimfire vs. Centerfire Ammunition – Which Is Best?: https://www.gunadvice.com/rimfire-vs-centerfire-ammunition/

Tait, B. (2021, January 9). *News*. Retrieved from KSL TV: https://ksltv.com/452788/hundreds-of-people-line-up-outside-gun-store-in-orem/

Wallace, J. S. (2018). *History of Gunpowder. In Chemical Analysis of Firearms, Ammunition, and Gunshot Residue (2nd ed., pp.* 13-14). CRC Press.

Wiki Dictionary. (2021, January 11). *Definition of Infringed.* Retrieved from en.m.wikipedia.org: www.en.m.wikipedia.org/wiki/infringment

YouTube. (2021, January 13). *Black powder.* Retrieved from www.youtube.com: https://www.youtube.com/watch?v=aAgxI4fHL80

YouTube. (2021, January 10). *Coil gun.* Retrieved from www.youtube.com: https://www.youtube.com/watch?v=TWeJsaCiGQ0

YouTube. (2021, January 13). *Smokeless Powder.* Retrieved from www.youtube.com: https://www.youtube.com/watch?v=aAgxI4fHL80

Youtube. (2021, January 10). *What bullets to use in your Muzzle loader.* Retrieved from www.youtube.com: https://www.youtube.com/watch?v=B0djX76p4oE

Zent, J. (2020, December 17). *American Rifleman*. Retrieved from News: www.americanrifleman.org

[1] The word **Infringed** means "act so as to limit or undermine (something); encroach on" and "actively break the terms of (a law, agreement, etc.) (Wiki Dictionary, 2021)

6. Future Proof Security [Shields]

Student Learning Objectives

Using IEC 62443 and other evolving standards, as inspiration for requirements, Chapter 6 is dedicated to the importance of both security and authentication in providing secure integrity management for systems now and the foreseeable future.

The student will be introduced to Autonomous Key Management (AKM) and its importance in replacing Blockchain – because it is more secure and offers advanced features against quantum computing.

Security Landscape

New and evolving threats to security include not only attacks on the security of the protected assets (both "in-motion" and "at rest"), but also to the validity of the protected assets. Requirements focused on both simultaneously securing the data as well as authenticating the source of the data are rapidly increasing in significance.

Standards like IEC 62443 (ISA, 2021), have evolved over the past five years to address this exact problem. IEC 62443 specifies a framework to address and mitigate current and future security vulnerabilities in *industrial automation and control systems* (IACSs). It also provides a firm foundation for other industries that are neither mission critical nor safety critical, but whose applications are just as important to their stakeholders and for whom value security and authentication as much as the stakeholders in mission critical and safety critical applications.

Security and Protecting Critical Assets

Malware on the rise and intruders increasing the scope, sophistication, and frequency of their attacks, the realization has been made that encryption alone cannot protect a system. The consensus is that a more wholistic approach must be taken and this is where IEC 62443 and other similar methodologies come to bear. (Michelle Michael, TÜV Informationstechnik GmbH, TÜV NORD GROUP, 2021)[1]

In parallel, those whose responsibility it is to provide network and asset security have accepted the notion that breaches are inevitable and thus, constant analysis of the system and its assets must be done perpetually for the life of the system. What this means, is that it is not enough to simply focus on protecting files and/or data. The focus initially shifted to intrusion detection, but then quickly expanded beyond that to include monitoring the entire system and integrity management.

Each data set, each hardware element, and each electronic component, must be identified, verified, and validated:

Asset Authentication = Asset Identity Validation + Asset Identity Verification (Eq 6.1)

Identity Validation refers to the concept that the identity is valid. That it is real. For instance, the verification of a social security number will determine if the number is a legitimate social security number, but not necessarily if it belongs to a specific individual.

Identity Verification refers to the concept that the validated identity is verified as being associated with the context it is being tested for. Again, using the concept of a social security number, not only is the social security number valid (i.e., associated with a real, living person), but it is indeed associated with the specific person who is claiming it as their own.

Put the two together and the result *asset authentication.*

By authenticating each asset, the integrity of the overall system is maintained. Additionally, authenticated physical assets, can then, themselves, become trust anchors and a means for extending the overall integrity and security of the entire system.

One-time authentication is not sufficient for protecting the overall system integrity. It is a process that must be repeated from power-on to power-down/reset and for the lifetime of each individual device and the system as a whole.

The driving factor for this is that the issues and concerns of what was once the dilemma of the Information Technology (IT) domain has now crept into the Operational Technology (OT)[2] domain as well. It is especially true for the critical infrastructure subset portion of OT represented by Industrial Automation Control Systems. This is because in an effort to interconnect OT and IT systems, OT systems now have many of the same components as IT. Thus, they automatically inherit and/or are susceptible to the same problems.

The problem with that is while there are plenty of security solutions for IT, OT presents a more difficult landscape to protect because of its diversity of systems, including systems that are comprised of many (if not all) proprietary solutions.

The below Table 6.1, obtained from a whitepaper created by TUViT (Michelle Michael, TÜV Informationstechnik GmbH, TÜV NORD GROUP, 2021), illustrates the disparity differences between traditional IT Security and IACS Security (and is also largely true for many OT systems because of proprietary and non-standard OT implementations):

Table 6.1: Differences between Traditional IT Security and IACS Security

Security Topic	Office IT Systems	IACS Systems
Antivirus	widely used & updated	complicated & difficult to implement
Life Cycle	3-5 years	5-20 years
Awareness	Good	Not Good
Patch Management	Often	Rare, approval from plant Manufacturers
Change Management	Regular & Scheduled	Rare
Evaluation of Log files	Established practice	Unusual practice
Time Dependency	Delays acceptable	Critical
Availability	Not always available; failure accepted	24/7
IT Security Awareness	Good	Poor
Security tests	Widespread	Rare & Problematic
Testing environment	Available	Rarely available
Security Audits	Regular & expected	Rare & avoided (Editor added)

Source: (Michelle Michael, TÜV Informationstechnik GmbH, TÜV NORD GROUP, 2021)

The takeaway from Table 6.1 is that while IT systems are challenged to keep up with the rapidly changing and increasing complex and sophisticated security attacks, OT faces almost insurmountable obstacles to overcome just to get near the same level of protection as IT. *The challenge for OT Industrial Automation Control Systems they are almost always managing critical infrastructure that must operate in an environment of continued availability and stability.* Not only is there an additional constraint that these systems can ill-afford to go offline because of the safety concerns of the resources they are managing, but these systems must be continually operational.

The foundation of why new and more comprehensive approaches for providing security and integrity services to OT, particular those managing critical infrastructure, have evolved. But one need not think that these approaches are limited to and benefit only OT critical infrastructure systems. These approaches also can provide great benefit to IT based systems, particular those which directly or indirectly impact the very fabric of our society.

Protecting Industrial Control Systems via Comprehensive & Secure Integrity Management & Monitoring

Having now established that security solutions for systems require more than simply encryption of data. That the basic integrity of those systems must also be maintained. The question then becomes, how to do this?

First, it will be easier and more straightforward to consider systems whose operating environment can be limited. That is systems that operate mostly as closed systems, with little to no interaction to external networks. Second, and with the aforementioned in mind, focusing on Industrial Control Systems (ICS) will have the greatest impact. As these systems can least afford to have a breach and the resultant behavior as consequence of a breach, can be catastrophic to both human life and property. Protecting these systems provides the ultimate ROI, by saving both money and human life.

Given this focus, the logical progression for thoroughly examining the challenges Industrial Control Systems face:

1) Describe characteristics of what sets Industrial Control Systems apart from typical IT systems.

2) Outline what an ideal solution would be

3) Given the ideal solution provided in (2) above, describe how current solutions fit within this framework, and

4) Provide alternative, perhaps yet to be defined solutions that can address the goals of the framework described in 2) above.

Secure Communication & Integrity Management & Monitoring Challenges for Industrial Control Systems

Systems which are typically considered as Industrial Control Systems, usually manage mission and/or safety critical types of systems, including critical infrastructure systems (that manage essential services). Typical examples of such systems are:

- Electricity: Power Generation and Power Distribution.
- Petroleum/Natural Gas: Exploration, Extraction, Pipeline, Production.
- Wastewater: Treatment/Purification.
- Transportation:
    - Aviation: Traffic Control, Aviation Vehicles.
    - Rail: Traffic Control (BackOffice, Wayside, and Onboard), Other non-traffic, onboard systems.
    - Maritime: Traffic Control, Onboard Shipping Control systems.
    - Automotive: Traffic Control, Individual Vehicle Control systems.
- Manufacturing
- Mining

These systems come under a variety of names:

- Industrial Control Systems (ICS).
- Operational Technology (OT).
- Supervisory Control and Data Acquisition (SCADA).
- Programmable Logic Controllers (PLC).
- Proportional-Integral-Derivative (PID).

And, usually have most, if not all of the following characteristics:

- *Communication within the system is local to the closed system.* Typical examples of this would be virtually all vehicles and other types of mission and/or safety critical systems.
- *Hardware components are static and do not change.* Thus, all possible combinations of communication paths are known up front.
- *Communication may be physically and/or logically separated into mission/safety critical communication and non-mission/non-safety critical communication.*
- *Updating of traditional security credentials is often physically prohibitive, difficult to do, and/or financially impractical or costly.* Some practical examples of this are:

- Updating the security credentials in automotive vehicles would be inordinately costly and practically impossible in all cases given that some vehicles may never visit an authorized service center to connect to the OEM backend server.
- Remote updating of security credentials of high-security military installations is usually prohibited and done locally. Making the overall security credential update process inordinately costly.
- Remote updating of security credentials of space systems is problematic both for reasons of security and practicality (including huge delays because of time and distance from

Earth).

- Updating of security credentials within nuclear facilities must be done locally. Making the overall security credential update process inordinately costly.

- *Availability* for many of these systems must be at or close to 100%. Meaning, the systems they control must remain online 24-hours a day, 365-days a year, without interruption. Systems that fall under this category usually have double or triple redundancy systems, but if there is a security breach, *depending upon the redundancy is achieved, it may easily affect all of the redundant systems as well.*

These systems, particularly those protecting critical infrastructure, are considered to be excellent targets by potential attackers. A successful attack on such a system can incur a huge loss to both a country and its economy.

Even though these systems usually have limited (or restricted) external network connectivity, because of their operational requirements and the aforementioned potentially catastrophic consequences in the event of failure or breach, their security requirements are far more demanding than most IT based systems. Careful thought must be given as to what the ideal solution would be to solve the security and integrity challenge for Industrial Control Systems.

The next section focuses on collating suggested requirements for providing security and integrity management to Industrial Control Systems, keeping in mind, the demanding nature of their operational environment.

Ideal Secure Communication & Integrity Management & Monitoring Requirements for Industrial Control Systems

Before delving into the suggested requirements, the concept of a security relationship must be defined. Which is, a security relationship is a set of two or more endpoints that form a communication network sharing a common set of security credentials. Another way of viewing the concept of security relationship would be that of a “security mesh”, given that the set of endpoints is not restricted to point-to-point communication, but rather multipoint to multipoint communication.

Logically, it is easier to break this task into two sections.

First, is to examine what the ideal security solution should look like. Then, using the security framework specified for the ideal security solution, the ideal Integrity Management framework can then be examined as well.

Ideal Secure Communication Requirements for Industrial Control Systems

Features and associated reasoning for each suggested requirement are provided below:

- *Security Credentials should be unique per security relationship, with no interdependencies on security credentials of other security relationships.* Different security relationships should have nothing in common with other security relationships.
- *Shared secrets that could lead to a breach of one or more security relationships, shall not be communicated between hardware modules* and preferably, are never exposed outside of a hardware module’s secure storage. Implies, security credentials are pre-provisioned, with no key exchange.
- *Security credentials should never be static and should be updated/refreshed on a regular basis.*

- *Security credentials should not be predictable.*
- *Security credentials should have Perfect Forward Secrecy* (even if someone discovers the current security credentials, it should not give them any insight as to what prior security credentials were).
- A *single set of security credentials should be capable of securing a communication mesh of two or more nodes*. That is, it shall be possible to have security relationships of more than two nodes (i.e., a multipoint, security mesh and not simply a P2P security connection). This is a property of scalability.
- *Hardware Modules may have multiple, overlaying communication security relationships*. Ideally, these security relationships shall be application specific and enable different virtual communication security relationships within the same hardware module. Hardware Modules may have multiple, overlaying communication security relationships. Ideally, these security relationships shall be application specific and enable different virtual communication security relationships within the same hardware module. This is also a scalability property.
- *Capable of authenticating the transmitting hardware module.*
- *Has little to zero latency* (zero ideally) (There is no session establishment phase, implying that it automatically comes up in "bulk encryption" mode).
- *Capable of providing same level of security to small hardware modules (ex. sensors) with minimal processing and storage capabilities*, ideally, security related algorithms are of linear complexity and utilize less than 15-KB in executable and runtime storage requirements.
- *Initial Provisioning of new security credentials shall be autonomous.*
- *Refreshing of security credentials shall be both frequent and autonomous*
- *Prevention of Replay Attacks should be a built-in feature.*
- *Must be quantum resilient*. With the advent of quantum

> computing on the horizon and serious discussions about the negative implications for existing security, particularly the asymmetric algorithms used for sharing the bulk encryption key in Public Key Infrastructure (PKI). It is imperative that any proposed ideal solution be absolutely quantum resilient.

The basis for each requirement is:

Unique Security Credentials per Relationship

Ensuring uniqueness amongst different sets of security relationships eliminates the possibility that a breach of the security credentials can provide insight into the credentials of other security relationships (as would be the case with a PKI asymmetric encryption breach of one Public Key/Private Key pair could lead to the breach of other Public Key/Private Key pairs).

No Communication of Shared Secrets

Eliminating communication of shared secrets prevents the attacker from directly discovering security credentials exchanged over the communication network. Elimination of shared secrets has the side-benefit of mitigating Man-In-The-Middle attacks, as it severely minimizes useful information an unwanted observer could use to launch such an attack.

Continually Refreshed Security Credentials

Security credentials should be updated frequently. Ideally, they should be updated every session, so that the security credentials are constantly moving target.

Security Credentials Cannot be Derived/Predicted

What this means is that even if an attacker gains access to a prior set of credentials, they should not be able to predict what future sets of credentials are. Credentials should have a legitimate amount of randomness within the security credential creation process to ensure future iterations cannot be mathematically derived or predicted.

Security Credentials should have Perfect Forward Secrecy

This is a follow-on to the previous requirement, but in the opposite direction. What this requirement means is that in the event of a breach and if the current security credentials are compromised, there is no way to backwards engineer what prior sets of security credentials were. In other words, if an unwanted observer had recorded prior sessions, a breach to the current set of security credentials would not enable them to decrypt prior sessions that had been previously recorded.

Security Credentials shall be Capable of Protecting Multipoint Networks (i.e., creating a Security Mesh)

It shall be possible to have security relationships of more than two nodes (i.e., a multipoint, security mesh and not simply a P2P security connection). Thus, increasing the scalability of a solution.

Hardware Endpoints may Have Multiple, Overlaying Security Relationships

This is another scalability property by allowing security relationships to be application specific with different virtual communication security relationships across one or more of the same physical hardware components. Thus, enabling hardware endpoints to have multiple, overlaying communication security relationships.

Authenticates Hardware Endpoint

Automatic authentication of the hardware endpoint both ensures against hardware spoofing as well as establishing the hardware endpoint as a local trust anchor.

Significantly Mitigates Latency

Ideally, latency is reduced down to zero, as an efficient solution will not have a session establishment phase.

Provides Consistent High-Level Grade Security Regardless of Processing Capability

The solution should be capable of providing the same high-level of security to small hardware modules (ex. sensors) with minimal processing and storage capabilities as it does with more capable hardware architectures. Ideally, security related algorithms are of linear complexity and utilize are capable of being compressed down to 15-KB or less in executable and runtime storage requirements.

Initial Provisioning of New Security Credentials is Autonomous

This feature significantly mitigates need for administrative personnel by enabling automatic new security relationships to be established without need for administrative oversight. The most obvious way to implement this into a security relationship would provide for an in-network management device the ability to automatically configure new security relationships in accordance with the direction of a downloaded (or modified) configuration file or database.

Autonomous and Frequent Refreshed/Updated New Security Credentials

This feature significantly mitigates need for administrative personnel by enabling the frequent, automatic update of new security credentials for perpetuity, presumably in accordance with some preconfigured policy.

Elimination of Replay Attacks

This is an easy enough feature to implement by including an unmodifiable replay counter within every frame.

Must be Quantum Resilient

Effectively, this means that no brute force attack with infinite resources is capable of breaching the security.

Ideal Integrity Management Requirements for Industrial Control Systems

As will be obvious after reviewing the requirements, many of the requirements for the ideal Integrity Management & Monitoring (IM&M) solution are identical or closely related to the requirements for the ideal Secure Communication solution. Thus, the ideal IM&M solution should be based on the ideal Secure Communication solution and listed below.

The IM&M Validates Hardware Endpoint

Automatic authentication of the hardware endpoint both ensures against hardware spoofing as well as establishing the hardware endpoint as a local trust anchor. This is identical to the Ideal Secure Communication requirement.

The IM&M Validates Every Software Component

Every electronic image that is part of the core application and required supporting infrastructure should be validated. This usually consists of a minimum of:

1) The Bootloader.

2) The Runtime Operating System Environment.

3) The Core Application (that implements the actual functionality for which the hardware module was designed).

4) Related Data Files.

Validates Every Subsystem

Every subsystem should be validated, where a subsystem is defined to be a collection of logically grouped, hardware modules.

Validates Every System

Every system should be validated, where a system is defined to be a collection of all subsystems and/or hardware modules within a physically distinct system

The Integrity Management & Monitoring System Shall Enforce the System Configuration

Every hardware module, subsystem, system and shall be defined as designated by a resultant configuration management file capturing the configuration of each individual hardware module, subsystem, and overall system.

Enforcement of the System Configuration shall occur for the Life of the System

The configuration specified for the overall system, its individual subsystems, and hardware modules shall be enforced throughout the life of the system from cradle to grave to comply with the specified configuration (which can and usually will change over time).

Enforcement of the System Configuration shall occur Continuously in Periodic Intervals During Runtime

Every aspect of the configuration, including the overall system itself, the subsystems within the system, and the hardware endpoints within the subsystems, shall be re-validated on a continual, periodic basis throughout the life of the system, including and especially during runtime.

The System Configuration Shall be Simple and Crosschecked with Other Components and Subsystems within an Individual System

The validation process shall be simple, immutable, and crosschecked with other components and subsystems within the system. Thus, ensuring that one module within a subsystem cannot be changed without simultaneously altering all other modules within the same subsystem.

Normal Operation of the Ideal IM&M, including

Enforcement of the System Configuration, Shall be Autonomous

The system should be simple and explicitly designed to automatically enforce the system configuration, so as to mitigate the possibility of nefarious alteration of the associated image integrity code and/or image. To ensure absolute compliance, images and their integrity codes can be configured to be cross-checked again immediately prior to them being loaded. Of course, this is the age-old tradeoff of security verses efficiency, and will be determined by the individual customer.

At a minimum, an image to be loaded should have its integrity code recalculated just prior to it be being loaded, to ensure it matches the integrity code value held within the local hardware store of the secure element.

Hardware Endpoints May be Members of Multiple Subsystems Simultaneously

This enables overlaying of security relationships in accordance with customer defined groupings and is an extension to the Secure Communication requirement stating that Hardware Endpoints may have multiple, overlaying, security relationships.

All Communication Between Logical Elements within the System Shall be Secure

All communication between logical elements shall use a secure communication solution that meets the requirements of an ideal secure communication solution outlined previously.

How do Current Solutions fit within the Outlined Ideal

Framework for Secure Communication and Integrity Management & Monitoring?

It should come as no surprise that existing solutions (ex. PKI + TLS and/or Blockchain) do not fit within the ideal outlined framework. The reason for this is simple. The ideal solution was derived with the goal in mind of solving issues currently plaguing existing solutions. This set of ideal requirements was created with the specific goal of correcting problems that have been discovered over time in how security and integrity management & monitoring works today. Thus, the only way to truly address these problems is with a new solution that is specifically and explicitly designed to solve these problems.

Current Solutions vs. the Ideal Secure Communication Solution

It is nonetheless instructive to compare the ideal requirements with the nominal solutions in use today, namely, the Public Key Infrastructure (PKI) Key Management System (KMS) and the Transport Layer Security (TLS) communication security protocol.

How Do PKI + TLS Address the Ideal Requirements for Secure Communication?

Unique Security Credentials per Relationship

PKI (plus TLS) Violation!

PKI is explicitly designed to enable one to many relationships, for as long as the security credential is in operation. Effectively, PKI is designed to explicitly violate this principal. Further, for many closed systems (like automotive passenger vehicles), their PKI certificate may never be updated. Thus, leaving a single certificate for the life of the vehicle.

No Communication of Shared Secrets

PKI (plus TLS) Violation!

The asymmetric key exchange phase of PKI is used to share the symmetric key used for bulk encryption with the other side of the PKI/TLS connection.

Continually Refreshed Security Credentials

PKI (plus TLS) Violation!

In many ICS/OT/SCADA/Etc. applications, security credentials are changed at best, every 9-12 months. In the case of automotive and automotive related passenger vehicles, these credentials may never be changed and could be static for the life of the vehicle.

In the automotive vertical, the logic used to defend this decision is simple:

1) It would be both prohibitively costly and physically impractical to update the security credentials in automotive vehicles.

2) Because automotive vehicles are closed systems, the likelihood and impact of a breach is relatively small.

Where that logic falls apart is simple. The goal of an attacker is not necessarily a total and complete takeover of every system. The goal of the attacker is varied and victory for some attackers could be achieved if they were able to significantly disrupt a specific industry, infrastructure, or company. A complete devastation of the economy would be at the top of the list of their wildest fantasies.

Just like prior to September 11th, 2001, it was inconceivable that someone would hijack a plane for the sole purpose of crashing it into a building. Similarly, if a state sponsored attacker wanted to significantly disrupt the economy, they would not need to hack all automotive vehicles, most vehicles, or even a large plurality of vehicles. A very minute subset, strategically placed, would do just fine.

We already know that many of these attackers have engineering backgrounds and could easily work within any number of vehicle manufacturers. All it takes is time, motivation, and planning and anything is possible. (Department of Sociology, University of Oxford, Manor Road Oxford OX1 3UQ, 2008) [3]

Transportation Terrorist Scenario [4]

Let's take the following example. (CENSEC, DK, 2019)

Suppose a state sponsored terrorist organization was able to gain insight into the security credentials used for twenty vehicles each of five of the major automotive companies. Meaning, a total of 100 vehicles. Suppose also they were patient in planning this, with their plans measured in years, not months or days.

If you had personnel who worked at these automotive manufacturers, discovering the security credentials programmed into a small subset of vehicles is very much within the scope of reality.

Now, suppose they planned the attack as such:

1) On the first day of the attack, they took over control of ten (10) vehicles of OEM brand 1 during peak traffic hours, causing all the ten vehicles to crash.

2) One week later, the attackers launch the second attack. This time doing the same thing to ten (10) vehicles of OEM brand 2.

3) Then, just to mix things up a little, the attackers waited for two weeks and one day, and launched a similar attack on ten vehicles of OEM brand 3.

4) Then, some arbitrary number of days later, they launched the same attack on ten vehicles of OEM brand 4.

5) They wait another arbitrary period of time and launch another attack on ten vehicles of OEM brand 5.

6) They, then wait another arbitrary period of time and launch a second attack on five vehicles of OEM brand 1.

7) They again wait some arbitrary period of time and launch a second attack on five vehicles of OEM brand 2.

Keeping in mind that at this point, they still have forty (40) vehicles at their disposal, how far into this series of attacks do you think it would take before significant numbers of people simply stopped driving their cars? The answer is, of course rhetorical, one should look no further than the current COVID-19 crisis to know this would devastate our infrastructure, our trust in government, our economy, and our entire way of life as we know it.

Now, to add a bit of excitement into this thought experiment, suppose that they anticipated that people would at some point switch to mass transit, so they also infiltrated companies that manufactured busses used for public transportation. Thus, after there was significant paranoia and anxiety created by the automotive vehicle attacks, they started doing the same thing to public transportation.

Suppose they anticipated that if people stopped using both private and public transportation, they would switch to a work-from-home based economy as a stopgap measure. Thus, delivery trucks would become even more important than they are today. Suppose this really patient group of attackers, had also infiltrated companies that made delivery trucks for companies like DHL, FedEx, and UPS, and launched similar attacks on these delivery trucks.

Now, for the final coup de grâce, they also infiltrated manufacturers of semi-trucks, doing the same sort of attacks with them, and thus affecting how the vast majority of goods are transported significant distances.

Think about this!

People would stop driving!

People would stop taking public transportation (at least they would stop using busses)!

People working for delivery company would demand something be done before they drive their vehicles again!

Truckers would stop driving and like the delivery truck drivers, would demand something be done before they drive their vehicles again.

Without question, the entire economy of the Western World would come to a grinding halt.

All of this damage could be done to the entire combined economies of U.S., Canada, U.K., and Europe, just by having the ability to hack into less than 200-different vehicles.

All of this could have been avoided if the security credentials were constantly changing, not predictable, and maintained within a tamper resistant KeyStore.

This is well within the realm of reality and it is not a matter of "if", but "when" someone decides to do this.

Until then, the automotive and related industries will continue to ignore these warnings, citing the extreme unlikelihood of this happening, just like flying planes into buildings seemed equally unlikely prior to 9/11/2001.

The automotive vertical is an extreme case, most other verticals within the ICS/OT/SCADA/Etc. landscape do not maintain static certificates. Most other verticals do update their certificates on a regular basis, but as stated in the beginning of this section, this is a period of time that is measured in months and not weeks or days (with the recommended period being every 9-12 months). Thus, leaving as a static target the certificate until it is updated and, in a world, where quantum computing has been presupposed to be a legitimate threat to traditional cryptographic methodologies like PKI and TLS, this does present a significant problem once quantum computing is available.

Even without the availability of quantum computing, traditional cryptographic methods are vulnerable if the attacker is able to garner even a minimum amount of information about the certificate. From there, it would just be a matter of time before the security credentials were fully or even partially hacked. The longer the time between updates, the greater the exposure of the security credentials.

Security Credentials Cannot be Derived/Predicted

PKI (plus TLS) Violation!

If the static certificate is breached in any way, even partially, the derived security credentials are predictable.

Security Credentials should have Perfect Forward Secrecy

PKI (plus TLS) Violation!

PKI's version of Forward secrecy typically uses an ephemeral Diffie-Hellman key exchange to prevent reading past traffic. The ephemeral Diffie-Hellman key exchange is often signed by the server using a static signing key. If an adversary can steal (or obtain through a court order) this static (long term) signing key, the adversary can masquerade as the server to the client and as the client to the server and implement a classic Man-in-the-Middle attack.

Security Credentials shall be Capable of Protecting Multipoint Networks (i.e., creating a Security Mesh)

PKI (plus TLS) Violation!

Standard PKI (plus TLS) is limited to binary security relationships.

Thus, in order for multiple nodes to participate in a multimode secured connection, there must either be an extension/deviation added to PKI (plus TLS) or multiple PKI security relationships must be created in order to provide secure communication to interconnect all nodes within the proposed security mesh.

Example: In order to interconnect 50-nodes using PKI (plus TLS), you would need 1,225 (i.e., [(n-1) + (n-2) + (n-3) + ... 3+ + 2 + 1] or [((n-1)**2 + (n-1))/2]) separate PKI (plus TLS) connections.

Hardware Endpoints may Have Multiple, Overlaying Security Relationships

PKI (plus TLS) Violation!

The PKI Public Key/Private key pair is usually reserved for ALL communication between EXACTLY two nodes and does not usually allow different security credentials for different applications between the same two nodes.

Authenticates Hardware Endpoint

PKI (plus TLS) Violation!

This is not a capability of either PKI or TLS.

Significantly Mitigates Latency

PKI (plus TLS) Violation!

PKI requires initialization of security credentials (the asymmetric key exchange phase) before it can begin its initial encryption session. How does this address or violate the previously stated IIoT Security Ideals?

- Requires an additional step prior to being able to initiate bulk encryption.
- By definition, an asymmetric key exchange is significantly greater than linear complexity.
- In order to avoid initial delay, PKI security credentials (the bulk encryption key shared by the Public Key/Private Key, key exchange) may remain static for a period of time.

TLS always requires a session establishment phase, prior to any bulk encryption phase starting (meaning, in addition to any delay added by PKI, TLS has its own delay).

Provides Consistent High-Level Grade Security Regardless of Processing Capability

Possible PKI (plus TLS) Violation!

Not automatically a violation, but because of the asymmetric encryption, key exchange phase, as well as TLS session establishment, PKI (plus TLS) is challenged when it comes to processor architectures with minimal amounts of processing power and/or storage capacity.

Initial Provisioning of New Security Credentials is Autonomous

Possible PKI (plus TLS) Violation!

Initial provisioning of the PKI certificate itself is definitely a violation, but that is so infrequently done, it is not really worth considering here. Insofar as the security credentials themselves, the vast majority of the time, the policy will be that new security credentials will be issued when the TLS session is renewed (which could be frequent).

Autonomous and Frequent Refreshed/Updated New Security Credentials

Possible PKI (plus TLS) Violation!

The vast majority of the time, policy will dictate that new/ refreshed security credentials will be issued when the TLS session is renewed (which could be frequent).

Elimination of Replay Attacks

Possible PKI (plus TLS) Violation!

TLS only protects the transport and thus it provides protection against modifying or replaying of the encrypted data only. It does not protect against any kind of modifications or replaying of the data before the encryption or after decryption. Sending the same data again over a TLS connection is actually perfectly valid. The cryptographic nonce and timestamp that are used to detect replay attacks do not protect against modification or replaying. The sender can still use the same data but “protect” these “replayed data frames” with a new cryptographic nonce and a new timestamp.

Must be Quantum Resilient

Possible PKI (plus TLS) Violation!

While no one will argue that PKI in its current form is quantum resilient, there are efforts under way to modify PKI in order to make it quantum resilient. Perhaps this is possible, but it will be just another band-aid that increases the threat surface of PKI and does not fit within anyone's concept of an ideal secure communication solution.

In fact, Roger Grimes, a well-known, published security expert had this to say about quantum computing and traditional security mechanisms:[5]

"Quantum computers will likely soon break traditional public key cryptography, including the ciphers protecting most of the world's digital secrets. These soon-to-be-broken protocols and components include HTTPS, TLS, SSH, PKI, digital certificates, RSA, DH, ECC, most Wi-Fi networks, most VPNs, smartcards, HSMs, most cryptocurrencies, and most multifactor authentication devices that rely on public key crypto. If the list just included HTTPS and TLS, it would cover most of the Internet. On the day that quantum computing breaks traditional public crypto, every captured secret protected by those protocols and mechanisms will be readable." (Cryptography Apocalypse Preparing for the Day When Quantum Computing Breaks Today's Crypto, 2021)

Current Solutions vs. the Ideal Integrity Management & Monitoring Solution

When considering technologies for configuration management, a common technology for consideration is blockchain, mostly because of its immutable ledger capabilities. Thus, given blockchain's relative popularity in this regard, it will be examined for its capabilities as an Ideal Integrity Management & Monitoring solution.

How Does Blockchain Address the Ideal Requirements for Integrity Management & Monitoring?

Blockchain is a technology (and not a product) that is primarily used for protecting the integrity of the information stored within the Blockchain. Thus, any Integrity Management & Monitoring product based on Blockchain will need to be developed, since it is not an inherent feature of blockchain.

Blockchain certainly has the fundamental infrastructure to address Integrity Management & Monitoring, but in addition to whatever effort it will take to first design and then subsequently implement an IM&M application, Blockchain is well-known for being a heavy and overly complex solution.

Therefore, because Blockchain is overly complex and heavy, any implementation utilizing blockchain will certainly fall short in terms of processing overhead, ease of use, complexity, security (given that it is based on encrypting its data via PKI), etc. Thus, it is relatively straightforward to eliminate consideration of blockchain without going into further detail.

Provide Solutions that Address the Goals for Ideal Secure Communication and Integrity Management & Monitoring (IM&M)

There are such solutions that exist today. As of November of 2020, a leading manufacturer of trains in it is now the official IM&M preferred solution for a major rail manufacturer in Germany has adopted the AKM-based Ideal Integrity Management & Monitoring solution for all of their trains being built in the future and addresses all facets of CENELEC 50701 (a new rail standard adopted in May of 2020 and still in a draft state, that was specifically designed to be the rail application of the ISO standard, IEC 62443 (ISA, 2021) and scheduled for release in mid-2021). (European Railway Association, 2020)

Earlier, it was stated that he ideal IM&M solution should be built on top of a solution that meets the aforementioned specified goals for an ideal secure communication solution. In keeping with this philosophy, that is exactly what was done for the IM&M solution described here.

Autonomous Key Management (AKM), the Ideal Secure Communication Solution

The secure communication solution is a concept known as Autonomous Key Management (AKM) and was initially conceived in November of 2014 to provide complete communication security for automotive vehicles. (SAE International, USA, 2017) (SAE International, USA, 2017)

AKM is both a Decentralized, Distributed, Ledger-Based, Key Management System (KMS) and Multi-point communication security protocol layer. AKM can naturally act as a drop-in replacement for PKI + TLS. AKM uses a Broadcast Architecture, that supports true, multi-point end-to-end encryption. [6]

AKM ideally sits on top of UDP and/or TCP and can be implemented directly on top of a physical layer driver using a proprietary thin transport layer. And, in fact, it has even been integrated into the MAC layer of a transceiver as the security layer for a deterministic, industrial wireless communication protocol.

Below is a list of AKM features and the underlying basis for how each feature is provided:

- Maintenance Free – Once a security group has been provisioned, no external maintenance should ever be required (thus, all AKM relationships are self-maintained and decentralized and require no external maintenance once provisioning has been completed).
- Real-time Data Analytics – Because AKM is a protocol, Data Analytics are available on a per frame basis and thus, in real-

time.

- Intrusion Detection – Because Data Analytics can be constant and immediate, if enabled, intrusion detection is a natural extendable feature of AKM.
- Automatic Breach Recovery and Re-provisioning – If enabled because Intrusion Detection is a natural extendable feature, automatic re-provisioning of infected relationships can be re-configured according to policy. Thus, effectively neutralizing threats as soon as a breach is discovered.
- Secure Boot with Device Authentication – This feature uses the unique AKM Protocol Identifier associated with the device, in combination with an onboard, AKM enabled HSM or hardware secure element to provide a Secure Boot Feature to AKM enabled devices. Thus, ensuring only the precise associated host hardware is being used.
- Anti-spoofing and Network Authorization – Because AKM can uniquely associated with a specific device, and because security relationships are constantly being automatically updated, stale or substitute devices cannot be re-inserted into an AKM protected network without being re-provisioned. This also ensures that only authorized devices can ever be inserted into an AKM protected network.
- Replay Attack Protection – The AKM protocol has a replay counter located within every frame. Thus, preventing previous frames from being retransmitted.
- Perfect Forward Secrecy – Because Next Session Security Credentials are calculated based upon a randomly selected subset of parameters from an AKM security relationship specific vector, termed, the Parameter Data Vector (PDV), there is no mathematically available means to determine which parameters were used in prior sessions for calculating previous session Security Credentials. The PDV minimum size is 128-bytes and can be longer if desired by the customer.
- Security Credentials are Re-Generated and NOT Derived – Because the Parameter Data Vector (PDV) is periodically

updated based upon configured policy, next session credentials cannot be predicted subsequent to the replacement of the PDV, which is randomly generated and locally distributed within the de-centralized security group.

- Enterprise Grade Entropy – Because the minimum PDV size is 128 and because the smallest allowable PDV subset is 15, assuming an evenly distributive function is used for selecting the PDV parameter subset, the entropy as calculated by the nPr function (the function which calculates the number of permutations of set size, 'n', and subset size, 'r'), is said to be: 1.72831541602 x 1031. For reference the age of the universe as calculated in seconds is said to be somewhere between 1016 and 1017. Thus, even with a quantum computer, these parameters cannot be predicated without also knowing information that is never exposed (i.e., the internal seeds which are part of each set of AKM Security Credentials).
- Scalability at IoT Scale – Because AKM may be configured as a broadcast architecture, and Security Credentials can be configured for any number of 'n' nodes, where 'n' is any value greater than '1', there is no limitation with respect to the number of nodes or size of an AKM Security Group Relationship (a security group is the entity for which the security credentials protect).
- Unlimited Virtual Security Relationships (i.e., Security Groups) – Each security relationship is unique from every other security relationship. Security relationships may be defined according to attributes and may co-exist with other virtual security groups on the same AKM Node. Thus, communication can be performed securely on a per attribute basis.
- Each member of a security group maintains the same exact ledger containing the security credentials. This is the primary mechanism for how all nodes within the same security relationship can stay in sync with each other because they all have the exact same information stored within their ledger. Thus, if any information within a particular ledger is not in

100% agreement with the information contained within the same security group ledger for the other members (hardware devices) of the group, then it will become immediately detected and the security group will become out-of-synch. Thus, a security group ledger may be considered to be immutable.

- All security groups have at least two levels of resynchronization in the event that one or more members of a group becomes out-of-synch. In truth, more than two levels exist within AKM, but the methods beyond the initial two levels are for special circumstances and add additional features; primarily for mobility and dynamic expansion/contraction of a security group and are not covered within this chapter.
- Low-Power and Energy Efficient – Because only linear hashing functions and symmetric encryption are used, implementation of AKM requires minimum computational resources.
- Low-overhead – Because Bulk Encryption begins with the very first frame of an AKM session, there is no appreciable latency (other than the protocol header) associated with an AKM protected network.
- Minimal Digital Footprint – Edge Node AKM Software Applets are typically under 20K bytes and can be compressed down to below 10K bytes.
- True Multipoint End-to-End Encryption – Security Credentials applied to ‘n’ nodes, where ‘n’ can be any number greater than or equal to 2.
- Quantum Resilient – Because no public key is used (as in PKI with asymmetric encryption used for the key exchange, which in a closed IOT system is usually there for the lifetime of the system) and because AKM does not share any secrets, there is nothing for a quantum computing device to attack.

AKM Based IM&M, the Ideal Secure Communication Solution

Based on AKM which was explicitly designed to be an "ideal secure communication" solution, it was simple and straightforward to design a corresponding ideal solution for Integrity Management & Monitoring, building on the principles already present within AKM. As AKM provides the framework for many of the concepts that the ideal IM&M solution also needs. This concept of the ideal IM&M was derived over a period of two years, between May 2018 and August 2020 and is designed directly from requirements contained within CENELEC 50701 (which as mentioned previously is the rail application of the ISO standard, IEC 62443).

Features of the AKM-based IM&M solution are:

- Physical Device Validation (i.e., Identification + Authentication of the Physical Hardware) – This feature uses the unique AKM Protocol Identifier associated with the device, in combination with an onboard, AKM enabled HSM or hardware secure element to provide a Secure Boot Feature to AKM enabled devices. Thus, ensuring only the specified associated host hardware is being used. This guarantees against accidental misconfigurations or intentional spoofing of the hardware.
- Electronic Image Validation (i.e., Identification + Authentication of the electronic image)– This feature Identifies and Authenticates every electronic image within the release set for the specified hardware.
- Subsystem Validation (i.e., Identification + Authentication of the logical subsystem) – This feature uses a combination of a unique AKM Protocol Identifier associated with the subsystem and shared immutable ledgers of all of the physical devices within the subsystem (direct downlinks at the subsystem level).
- System Validation (i.e., Identification + Authentication of the entire system) – This feature uses a combination of a unique

AKM Protocol Identifier associated with the system and shared immutable ledgers of all of the subsystems that are immediately beneath the system level (direct downlinks within at the system level).

- User Validation (i.e., Identification + Authentication of the individual users, both human and otherwise) – This feature uses a combination of a unique AKM Protocol Identifier associated with user and a physical ledger item maintained locally within the secure element hardware store of the devices, subsystems, and systems, for which the user is associated with to ensure the validity of the user.
- Remote Access – This feature enables remote access to the system via both legacy mechanisms like RADIUS, as well as AKM protected communication.
- Audit Trail of Assets with Tamper-proof Audit Logs – This feature is derived from the AKM concept of shared immutable ledgers for members of the same security relationship and extends the ledger by adding the capability of an audit trail.
- Military Grade Secure Communication between Devices – This feature comes from multiple facets of the AKM framework. First, because AKM is crypto-agile, any cryptographic function or encryption algorithm may be used. Second, because of the extremely limited threat surface, protecting the threat surface is straightforward and simplistic. Third, there is no information that are ever communicated as part of the normal session security credential update process that could ever lead to a breach if intercepted. Fourth, as is mentioned within the list of AKM features, new and refreshed security relationships are created with Enterprise Grate Entropy (which can be easily increased with minimal increase in overhead). Last, all sensitive information is continually protected within a hardware secure element or Hardware Security Module (HSM) and is never exposed outside of the hardware secure element or HSM.
- Real-time Data Analytics – This feature is inherited directly

from AKM, given that AKM is used to exchange information between hardware devices, and subsystems. Thus, AKM-based IM&M inherits and extends real-time data analytics as well.

- Intrusion Detection – Again, this is an inherited feature of AKM, and is facilitated by an IM&M Network Management Module, which locally manages the entire system (or subsystem if a large system and hierarchical management is required) and utilizes the real-time data analytics gathered by AKM as well as utilizing traditional intrusion detection mechanisms.
- Maintenance Free – This is another inherited feature of AKM. Once an IM&M security group has been provisioned, no external maintenance should ever be required (thus, all AKM IM&M relationships are self-maintained and decentralized and require no external maintenance once provisioning has been completed).
- Automatic Breach Recovery and Re-provisioning – Because an IM&M Network Management Gateway is required within the system or subsystem level (depending upon complexity of the overall network), this feature is always present, but the degree of automation is determined by configured policy. The IM&M Network Management Gateway automatically configures the network and acts as the local trust anchor. Thus, Intrusion Detection is a natural extendable feature, as is, automatic re-provisioning in the event of infected relationships that require re-configuring (in according to policy). This feature effectively neutralizes threats as soon as a breach is discovered.
- Anti-spoofing and Network Authorization – Because AKM is uniquely associated with a specific device, and because security relationships are constantly being automatically updated, stale or substitute devices cannot be re-inserted into an AKM protected network without being explicitly re-provisioned by a trusted device (such as the Backoffice server remotely or the In-Network Management Gateway locally). This also ensures that only authorized devices can ever be

inserted into an AKM protected network.

- Other features directly inherited from AKM are: Replay Attack Protection, Perfect Forward Secrecy, Security Credentials are Re-Generated and NOT Derived, Scalability at IoT Scale, Unlimited Virtual Security Relationships (i.e., Security Groups), True Multipoint End-to-End encryption, Quantum Resilience.
- Low-Power and Energy Efficient – Another AKM inherited featured, but also because IM&M uses static integrity codes that are calculated based upon linear hashing functions, AKM-based IM&M requires minimum computational resources.
- Low-overhead – Because AKM-based IM&M runs in the background during runtime, uses only linear hashing functions for the integrity code calculation of the individual components, and simple compares of the integrity codes for validating the components, the overhead of AKM-based IM&M is extremely low, with the frequency of background component integrity code recalculation adjusted in accordance with policy.
- Minimal Digital Footprint – Edge Node AKM Software Applets are typically under 20K bytes and can be compressed down to below 12K bytes.

Summary

While both of these solutions were initially designed for OT centric closed systems, over time, the author has discovered that they are equally applicable to the IT world and many of the problems that IT faces.

AKM can easily be a drop-in replacement in IT applications for the traditional cryptographic Key Management Systems (KMS) of Public Key Infrastructure (PKI) and the secure communication protocol, the Transport Layer Security protocol, with the most current revision being TLS 1.3. As AKM and AKM-based IM&M addresses all of the problems plaguing both PKI and TLS because that is what it was explicitly designed to do (address problems in IoT centric systems for both solutions).

More recently, it was discovered that the IM&M solution would provide an excellent framework for solving the larger problems of ransomware, malware, and zero-day attacks.

Using AKM & AKM-Based IM&M for Solving the Most Difficult Problems Plaguing IT Communication and Systems

AKM and its IM&M derivative provide the perfect foundation for solving the Ransomware/Malware/Zero-Day Attack, computer problem at the enterprise level (a solution for the individual small business/home office solution has also been addressed but will be presented in a future edition for the purpose of brevity and importance). Using both AKM and its derivatives, like IM&M, an extension to the concept of whitelisting, which is termed, White boxing within this document, is able to:

1) Identify, verify, authenticate, and monitor all known executables and data, marking them as "safe to use" once authenticated and moved to the "Trusted Component" list (the White box).

2) Calculate an integrity code derived from a hash based, digital signature for each "safe to use" software component. Thus, enabling instant verification of all known, components on the "Trusted Component" box.

3) Identify, verify, authenticate, and monitor each hardware endpoint, ensuring that only trusted hardware devices are on the network.

4) Create a digital signature for each "trusted" hardware device, that is based upon the aggregation of all "Trusted Components" within the device. Thus, enabling instant verification of each "trusted" hardware device.

5) Create logical security groups of hardware devices in accordance with application context and customer preferences, for which all hardware devices within the security group will communicate integrity data using its own, unique set of security

credentials that is refreshed on a per session basis, with perfect forward security, and without exchanging any secrets.

6) Ensure the immutability of each trusted device's integrity code information (distributed ledger based) given that all integrity codes and other related information for each trusted device within a security group is shared with all other trusted devices. Thus, ensuring that the integrity code of an individual device cannot be altered without altering the same integrity code contained within the secured integrity information of the other trusted devices that are part of the same security group (i.e., each device within a security group contains a copy of the integrity codes of all of the other devices within the same group, plus an integrity code representing the security group itself).

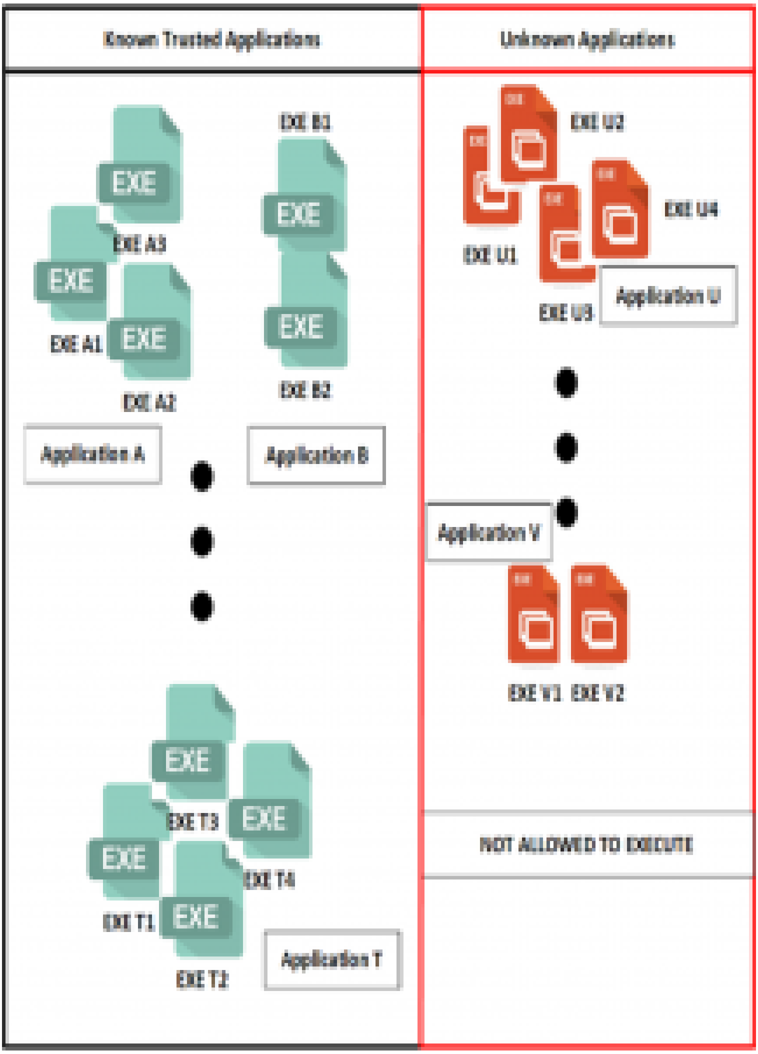
7) Create a digital signature for each security group based upon the aggregation of integrity codes of the individual trusted devices within each group. Thus, enabling instant verification of each security group.

8) Group the security groups hierarchically, so that the top-level security group represents the entire network, thus, enabling a quick check of the entire network, with a very simple, fast, linear cross-check of the system integrity code.

9) Periodically update the integrity codes of each component, both hardware and software within the entire system, on an ongoing and continual basis in the background, so as not to interfere with normal processing.

10) Using malware scanning functionality, scan each unknown application (or single executable if not contained within an encapsulating application) for validation of existing threats. If it is not on the existing threats list, add it to the list of applications to be cross verified by a human operator.

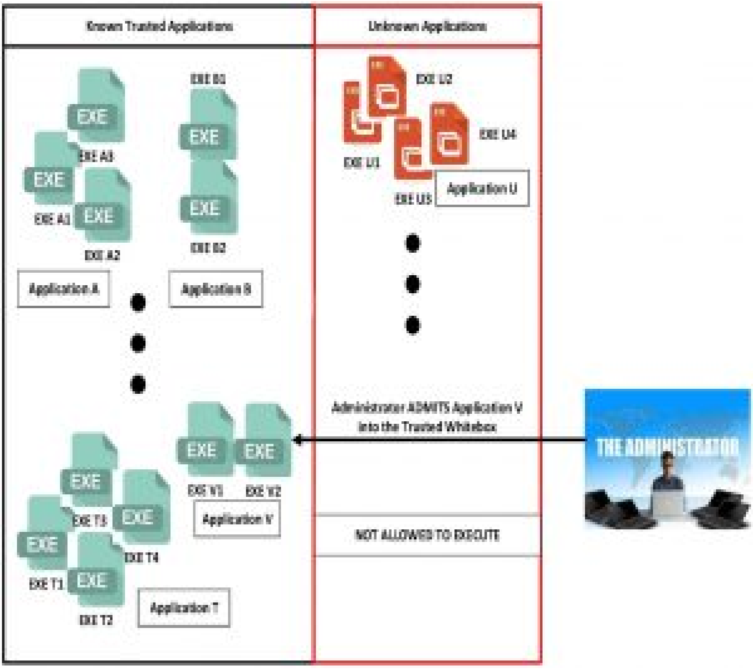
Figure 6.1 White boxing



Source: Olympus Sky (See endnote 5)

11) Once authorized personnel have authorized a new/unknown application (set of executables & related files) as safe, the IM&M-based White-boxing solution automatically updates the "Trusted Component" box with the new, trusted, application.

Figure 6.2 Human Operator moves Application V to Trusted Applications



Source: Olympus Sky (See endnote 5)

12) Application White-boxing denies the execution of any application that has not previously been explicitly approved as "known to not be malicious" (i.e., has not been previously placed

within the Trusted Component" box). This "default deny" approach offers a much higher degree of security than traditional antivirus blacklisting approaches for a number of reasons, with the single biggest reason that it denies "zero-day" attacks. Whereas, with standard "blacklisting", typical antivirus blacklist databases will not recognize the malware on "day zero", because it has never seen it.

The most difficult part of Application White-boxing (AWB) is admittedly managing what is and is not within the White-box. It is extremely difficult to keep the list of what is and is not allowed within a system where there are hundreds of thousands of files and many of them have a legitimate need to dynamically change at runtime. This is perhaps the core problem that modern AWB solutions exists to solve and is a very solvable problem. What makes it solvable is not expecting end users or IT administrators to figure out the details, but to ask them only for high-level approval of an entire action and then using software to track the precise details of exactly what files need to change, which is exactly how the IM&M-based White-box Enterprise solution operates (see steps (10) and (11) above).

Core elements of the IM&M-based White-box Enterprise solution are: AKM and AKM-based IM&M. The IM&M-based White-box Enterprise application sits on top of AKM-based IM&M, which in turn sits on top of AKM.

AKM-based IM&M first validates and authenticates the hardware device it resides in and then, for each software component within the hardware device that is part of a designated set of release files, executables, database files, configuration files, html files, etc., the AKM-based IM&M derives a unique integrity code for each software component. AKM-based IM&M then uses a hash of an aggregation of values from the hardware device in combination with the integrity codes from each software component within the designated set of release files, to create an integrity code for the hardware device.

Files that are part of the specified set of release files are all tracked and controlled using the aforementioned, unique integrity code. The AKM-based IM&M maintains a list of all integrity codes that are part of the system's release file set. Executable files that are part of this file list form the initial set of trusted applications. The AKM-based IM&M then, on a periodic basis, performs a check to ensure that the list of known valid files remain intact.

AKM-based IM&M maintains integrity across all nodes within a system by allowing nodes to be organized into logical groups in accordance with user preferences. Then, each node within that a logical group will form a security group based upon those user defined preferences. Using ledger-based technology, each individual node that is part of a security group, maintains a ledger both for itself, as well as each of the other nodes within its same security group. Therefore, rendering the ledgers of the individual nodes immutable, since identical copies of all ledgers are maintained across all nodes within the same group.

AKM-based IM&M allows as many of these logical group relationships as the customer wishes to create and they may be formed into any combination, and hierarchically as well. Thus, enabling the integrity code of any logical group to be an instant indicator of whether or not all hardware and software components within that group have been identified and authenticated. Meaning, the ability to discern the state of any part of the system is instantaneous and because the components are continually being reverified and authenticated in the background, the likelihood of malware being able to spread throughout the system is significantly mitigated.

This is the best of both worlds. AKM-based IM&M ensures release set files remain valid, while intrusion detection monitors for anomalous digital signatures.

The IM&M-based White-boxing solution takes this a step further, by managing the contents of the White-box. Only trusted applications will be allowed to execute. All other executables will be denied the ability to run. Working with the intrusion detection module, non-release set executables can be added to the list of trusted applications, but first must be checked against the known set of malware digital signatures for verification purposes.

Once a non-release set executable has been added to the set of trusted applications, it too is added to the designated set of release files and is assigned an integrity code, thus being tracked in the same way as if it had been one of the original sets of release files. In this way, the ability to instantly and continually verify the integrity of each hardware component, its subgroup, and the overall system to which it belongs, is maintained even as the system grows in its components list while simultaneously decreasing the overall threat surface.

The key attributes of this approach are threefold:

1) Using information known at system instantiation, it creates a list of all known good (validated) applications and continually verifies these known good applications throughout the lifetime of the system using a simplistic method for maintaining the integrity of the individual applications and comparing the resultant calculated integrity code with the previous known value of the application's integrity code.

2) Disallows any unknown application from running and isolates it a logically separate part of the system.

3) Uses human validation to admit new and/or unknown applications into the White box.

Clearly, the potential for exploitation is the human aspect, but a clear audit trail will be created for each interaction ensuring at the very least, the ability to trace actions with resultant consequences.

Conclusions

This chapter has focused on current problems plaguing both secure communication and the overall integrity of systems today. It has also suggested sets of requirements for what "ideal" solutions for both secure communication and integrity management and monitoring. Looking into the future, it has suggested a solution for some of the biggest remaining issues in IT and OT today, ransomware and malware, including zero-day attacks.

Questions

1. AKM states that it has the concept of Perfect Forward Secrecy. What is this feature and why is it important? Does this give AKM an advantage over PKI?
2. AKM couples a hardware endpoint (i.e., a hardware module) to a particular AKM Hardware Identifier (which is similar to a MAC address). How does this feature help AKM prevent hardware spoofing or ransomware?
3. Why will quantum computing be detrimental to PKI based security implementations?

REFERENCES

CENSEC, DK. (2019, June 3). *Railway Cyber Security Threats and Resilient Measures.* Retrieved from https://censec.dk/: https://censec.dk/wp-content/uploads/2019/06/Alex-Bishop-Railway-Cyber-Security-Threats-and-Resilient-Measures.pdf, slide 24

Cryptography Apocalypse Preparing for the Day When Quantum

Computing Breaks Today's Crypto, G. R. (2021). *Cryptography Apocalypse Preparing for the Day When Quantum Computing Breaks Today's Crypto, Grimes, Roger A., Cryptography Apocalypse (p. xxii).* Washington: Amazon, Kindle ed. Retrieved from Cryptography Apocalypse Preparing for the Day When Quantum Computing Breaks Today's Crypto, Grimes, Roger A., Cryptography Apocalypse (p. xxii). Wiley. Kindle Edition.

Department of Sociology, University of Oxford, Manor Road Oxford OX1 3UQ. (2008, February 8). *Engineers of Jihad.* Retrieved from www. sociology.ox.ac.uk/swp.html: www. sociology.ox.ac.uk/swp.html

European Railway Association. (2020, November 13). *webinar_cybersecurity_in_railways_en.* Retrieved from www.era.europa.eu: https://www.era.europa.eu/sites/default/files/events-news/docs/questions_answers_webinar_cybersecurity_in_railways_en.pdf

ISA. (2021, January 2). *New ISA/IEC 62443 standard specifies security capabilities for control system components- Summary* . Retrieved from www.isa.org: https://www.isa.org/intech-home/2018/september-october/departments/new-standard-specifies-security-capabilities-for-c

Michael, M. (n.d.). Retrieved from www.tuvit.de.

Michelle Michael, TÜV Informationstechnik GmbH, TÜV NORD GROUP. (2021, January 2). *Whitepaper Industrial Security based on IEC 62443.* Retrieved from www.tuvit.de. : www.tuvit.de.

SAE International, USA. (2017, September 17). *Autonomous Key Management* (AKM) *Security Architecture for Vehicle and* IoT *Applications* . Retrieved from sae.org: www.sae.org

SAE International, USA. (2017, March 28). *Autonomous Key Management* (AKM) *Security Architecture for Vehicle and* IoT *Applications* . Retrieved from sae.org: www.sae.org

[1] Whitepaper Industrial Security based on IEC 62443, Michelle

Michael, TÜV Informationstechnik GmbH, TÜV NORD GROUP, Langemarckstraße 20, 45141 Essen. +49 201 8999-629, m.michael@tuvit.de, www.tuvit.de.

[2] IT/OT – convergence is the integration of information technology (IT) systems with operational technology (OT) systems, IT systems are used for data-centric computing; OT systems monitor events, processes and devices and make adjustments in the enterprise and industrial operations.

[3] Terrorist study presented by Professor Nichols at Utica College in his Keynote: ***The Next Attack On America***

58th Annual Engineers Award Banquet, Whitesboro, NY, Feb 28th,2008 (available from editor)

[4] Railway Cyber Security Threats and Resilient Measures, 3 June 2019, https://censec.dk/wp-content/uploads/2019/06/Alex-Bishop-Railway-Cyber-Security-Threats-and-Resilient-Measures.pdf, slide 24

[5] Cryptography Apocalypse Preparing for the Day When Quantum Computing Breaks Today's Crypto, Grimes, Roger A., Cryptography Apocalypse (p. xxii). Wiley. Kindle Edition.

[6] Internal Olympus Sky Whitepapers:

i.https://www.dropbox.com/s/w89ebhma18i9fld/OlympusSky_AKM-Whitepaper.pdf?dl=0

ii.https://www.dropbox.com/s/hb9yo8bnue7oq80/OlympusSky_SecurityForAutonomousDrones-Whitepaper.pdf?dl=0

iii.https://www.dropbox.com/s/td4ouqdt6yu26n1/OlympusSky_IoT-TLS-SSL-Whitepaper.pdf?dl=0

Internal Olympus Sky Whitepaper on AKM-Based Integrity Management & Monitoring, https://www.dropbox.com/s/cz7vanrzessploi/OlympusSky_SecureRealTimeIntegrityMgmtValidation-Whitepaper.pdf?dl=0

PKI (oasis-pki.org).

RFC 8446 – The Transport Layer Security (TLS) Protocol Version 1.3 (ietf.org).

7. Failure of Climate Change [Nichols]

“The whole aim of practical politics is to keep the populace alarmed – and hence clamorous to be led to safety – by menacing it with an endless series of hobgoblins[1], all of them imaginary.”

– L. Mencken(Wrightstone G. , 2017)

Student Learning Objectives

Man-made / Influenced Catastrophic climate change (CC) and global warming (GW) are contentious issues hyped in the news and parroted with almost a religious following. It is time to at least understand the basic *scientific elements* that make up the climate change claims and real natural phenomena and driving forces.

It some cases, we need to push back against the outrageous and irresponsible. Our SLO is

- To understand the CC / GW processes,
- To separate facts from fiction regarding key natural phenomena: CO2 emissions, warming, temperature rise, tornadoes, hurricanes, forest fires, greenhouse gases (GHG),
- To develop facts that we can use to make up our own minds about CC / GW and its correlation to man-made behavior – especial in the last 50 years.

Introduction

Amy Coney Barrett declined to say that climate change is real, calling it instead a “a very contentious matter of public debate, especially one that is politically controversial.” during the third day of her Supreme Court confirmation hearings. (Boyle, 2020)[3] The judge made the comment on Wednesday as she was questioned by California Senator Kamala Harris, the Democratic vice-presidential nominee, (now VP) and a member of the Senate Judiciary Committee. The Supreme court nominee doubled down on comments she made on Tuesday, where she said that she has no "firm views" on climate change because she is "not a scientist". [4]

(Boyle, 2020)

According to the UK Independent (Bolton, 2016), "**Some 97 percent** or more of climate scientists agree that climate-warming trends over the past century are being driven by human activities, largely the burning fossil fuels." Maybe.

The purpose of this chapter is to develop a point – counterpoint discussion of fundamental concepts underlying climate change / global warming (GW). If we accept climate change as a disruptive technology or clear global megatrend, it behooves us to at least know the facts.

The Open Mind

Let's take a step back for a moment and recognize four key concepts: 1) science is not accomplished by consensus – just the opposite; scientists constantly challenge the status quo to improve understanding of our world; 2) since 1785, scientists have used a very organized methodology to continually test the validity / repeatability of the status quo by the Scientific Method. It is based on fact and quantifiable observations, not on political motivation, or money (university or private funding) or hyped up news; 3) humans do not control / influence everything in their world – it is arrogant to think so; and 4) data based on limited or biased scope yields limited / incorrect / spurious / or potentially fraudulent results. Policy decisions made on such reduced data / observations are bound to be incorrect.

This chapter is not meant for those who have made up their minds and will never challenge themselves or change – irrespective of political organization. It is meant for those who are uncomfortable with the information that we are barraged with each day and at are least open to discussion so that they can make up their own minds. The author will concentrate heavily on two important and diametrically opposing references with widespread appeal. Pierre Coutu wrote *Global Megatrends and Aviation: The Path to Future-Wise Organizations.* (Coutu, 2019) He devotes a full 77 pages to the subject of climate change. His book is the status quo. The second reference is by Gregory Wrightstone entitled *Inconvenient Facts: The science that Al Gore doesn't want you to know.* (Wrightstone G. , 2017) It is packed with facts and counterpoints, 2000 years of reference temperature data, and exquisitely sourced for each observation. Science, unlike religion or politics, is not a belief system. Science is based on a disciplined method of inquiry, by which a scientist applies pre-existing theory to observation and measurement, so as to develop or reject a theory, so as to unravel as clearly and as certainly as possible the distinction between "that which is and that which is not." (Wrightstone G. , 2017)

Scientific Method

The scientific method is an empirical method of acquiring knowledge that has characterized the development of science since at least the 17th century.[5] It involves careful observation, *applying rigorous skepticism* about what is observed, given that cognitive assumptions can distort how one interprets the observation. *It involves formulating hypotheses, via induction, based on such observations; experimental and measurement-based testing of deductions drawn from the hypotheses; and refinement (or elimination) of the hypotheses based on the experimental findings.* These are principles of the scientific method, as distinguished from a definitive series of steps applicable to all scientific enterprises.[6] (Wikipedia, Scientific Method, 2020)

Although procedures vary from one field of inquiry to another, they are frequently the same from one to another. The process of the scientific method involves *making conjectures (hypotheses),* deriving *predictions from them as logical consequences*, and *then carrying out experiments or empirical observations based on those predictions. A hypothesis is a conjecture, based on knowledge obtained while seeking answers to the question.* The hypothesis might be very specific, or it might be broad. Scientists then *test hypotheses by conducting experiments or studies. A scientific hypothesis must be falsifiable, implying that it is possible to identify a possible outcome of an experiment or observation that conflicts with predictions deduced from the hypothesis; otherwise, the hypothesis cannot be meaningfully tested.* (Wikipedia, Scientific Method, 2020)

The purpose of an experiment is to determine whether observations agree with or conflict with the predictions derived from a hypothesis. Experiments can take place anywhere. There are difficulties in a formulaic statement of method, however. Though the scientific method is often presented as a fixed sequence of steps, it represents rather a set of general principles.

Common steps /elements of the scientific method are: *Question, Hypothesis, Prediction, Experiment, and Analysis.*

There are additional components to the scientific method even when all iterations of the steps above have been completed.

Replication

If an experiment cannot be repeated to produce the same results, this implies that the original results might have been in error. As a result, it is common for a single experiment to be performed multiple times, especially when there are uncontrolled variables or other indications of experimental error. For significant or surprising results, other scientists may also attempt to replicate the results for themselves, especially if those results would be important to their own work. Replication has become a contentious issue in social and biomedical science where treatments are administered to groups of individuals. (Wikipedia, Scientific Method, 2020)

External review

The process of peer review involves evaluation of the experiment by experts, who typically give their opinions anonymously. Some journals request that the experimenter provide lists of possible peer reviewers, especially if the field is highly specialized. *Peer-review does not certify the correctness of the results, only that, in the opinion of the reviewer, the experiments themselves were sound (based on the description supplied by the experimenter).* If the work passes peer review, which occasionally may require new experiments requested by the reviewers, it will be published in a peer-reviewed scientific journal. The specific journal that publishes the results indicates the perceived quality of the work. (Wikipedia, Scientific Method, 2020)

Scientific Inquiry

Scientific inquiry generally aims to obtain knowledge in the form of testable explanations that scientists can use to predict the results of future experiments. This allows scientists to gain a better understanding of the topic under study, and later to use that understanding to intervene in its causal mechanisms (such as to cure disease). The better an explanation is at making predictions, the more useful it frequently can be, and the more likely it will continue to explain a body of evidence better than its alternatives. The most successful explanations – those which explain and make accurate predictions in a wide range of circumstances – are often called *scientific theories.* (Wikipedia, Scientific Method, 2020)

Most experimental results do not produce large changes in human understanding. Improvements in theoretical scientific understanding typically result from a gradual process of development over time, sometimes across different domains of science. Scientific models vary in the extent to which they have been experimentally tested and for how long, and in their acceptance in the scientific community. In general, explanations become accepted over time as evidence accumulates on a given topic, and the explanation in question proves more powerful than its alternatives at explaining the evidence. Often subsequent researchers re-formulate the explanations over time, or combined explanations to produce new explanations.

Properties of scientific inquiry

Scientific knowledge is closely tied to *empirical findings* and can remain subject to *falsification* if new experimental observations are *incompatible* with what is found. ***No theory can ever be considered final since new problematic evidence might be discovered***. If such evidence is found, a new theory may be proposed, or (more commonly) it is found that modifications to the previous theory are sufficient to explain the new evidence. The strength of a theory can be argued [by whom?] to relate to how long it has persisted without major alteration to its core principles. (Wikipedia, Scientific Method, 2020)

Beliefs and biases

Scientific methodology often directs that hypotheses be tested in controlled conditions wherever possible.

The practice of experimental control and reproducibility can have the effect of diminishing the potentially harmful effects of circumstance, and to a degree, personal bias. ***For example, pre-existing beliefs can alter the interpretation of results, as in confirmation bias; this is a heuristic that leads a person with a particular belief to see things as reinforcing their belief, even if another observer might disagree (in other words, people tend to observe what they expect to observe).*** (Wikipedia, Scientific Method, 2020)

This is a good place to Segway into the 97% claim.

97% Consensus can't be spelled without "con"

We have heard the drumbeat that 97% of scientists agree on human-driven climate change. (Bolton, 2016) (Coutu, 2019) We have also heard that those that don't buy into the climate -apocalypse mantra are Luddite science deniers. The author has been questioned “do I believe in climate change? His answer: “of course, it has been happening for hundreds of millions of years.” The real question relates to the human-driven actions.

Scientists do agree on two quantifiable truths:

- Carbon dioxide concentration has been increasing in recent years
- Temperatures, as measured by thermometers and satellites, have been generally increasing over the last 150 years.

What is impossible to quantify is the actual percentage of warming that is attributable to increased anthropogenic (human-caused) CO2. There is no scientific evidence or method that can determine how much warming we’ve had since 1900 was directly caused by us. (Wrightstone G. , 2017) We know that temperature has varied greatly over the millennia. (Coutu, 2019) We also know that for virtually all of time, global warming and cooling were driven entirely by natural forces, which did not cease to operate at the beginning of the Industrial Revolution. (Wrightstone G. , 2017)

The claim that most modern warming is attributable to human activities is scientifically insupportable. So what is the basis of the 97% conjecture?

Cook’s chaos

The primary paper that is often cited as the ultimate source of the 97% consensus “con” was written by John Cook and his merry band of climate extremists. He maintains a website where the paper has been downloaded more than 600,000 times. Cooks’ volunteer team [7] reviewed abstracts from 11,944 peer-reviewed papers related to clior global warming, published over 21 years 1991 -2011 to assess the extent to which they supported the “consensus view” on climate change. (Cook, 2013) Per Cooks paper:

“ We analysed a large sample of the scientific literature on global CC [climate change], published over a 21-year period, in order to determine the level of scientific consensus that human activity is very likely causing most of the current GW (anthropogenic global warming), or AGW)…." (Cook, 2013)

The paper concluded,

"Among the abstracts that expressed a position on AGW, 97.1% endorsed the scientific consensus… Among the papers expressing a position on AGW, an overwhelming percentage (97.2% based on sel-ratings, 97.1 % basted pon abstract ratings) endorses the scientific consensus on AGW." (Cook, 2013)

Cook's paper asserted **falsely** that 97% of the papers the reviewers examined **had explicitly endorsed** the opinion that humans are causing the majority of the warming on AGW! (Wrightstone G. , 2017)

When one looks closely at the data, one finds that **7,930** of the papers **took no position at all** on the subject and were arbitrarily excluded from the count on this ground. Adding these back into the total papers reviewed in the 97% count , the actual claim falls to **32.6%!** But a further look at the data shows that three categories of endorsement. (Table 7.1) Only the first category amounts to explicit statement that humans are the primary cause of recent warming. The 2nd and 3rd categories would include most of sceptics of AGW. (Wrightstone G. , 2017)

Table 7.1 Expanding the "consensus" broadly

Level of Endorsement	**Description**
(1)Explicit endorsement with quantification	**Explicitly states that humans are the primary cause of recent global warming**
(2) Explicit endorsement without quantification	**Explicitly states that humans are causing global warming or refers to AGW /CC as a known fact**
(3) Implicit endorsement	**Implies humans are causing AGW; e.g. research ASSUMES greenhouse gas emissions cause warming without explicitly stating that humans are the cause**

Source: (Cook, 2013)

Here is a new word: **Agnotology.[8]** David Legates and his co authors used this word to review / describe the Cook paper as an attempt to falsely promote the notion of broad scientific consensus surrounding the subject of a looming, man-made, climate apocalypse. (Legates, 2015) Legates reviewed their actual papers used by Cook and found ***only 0.3% of the 11,944 abstracts and 1.6%*** *of the smaller sample that expressed those papers expressing no opinion endorsed man-made global warming as they defined it.* (Legates, 2015)

97% [9] Consensus = con.

Global Warming – Status Quo (as applied to the aviation industry)

According to Contu, "at the heart of global warming are greenhouse gases (GHG) which are generated by human activity." He also states that "climate change is both a reality and a potential threat that "experts" believe could lead to global catastrophe if not addressed diligently and with vigor." "Lastly, the potential catastrophic consequences of climate change and global warming loom large in the public discourse, from headlines in the news and social media to boardrooms and living rooms, yet current measures to mitigate the phenomenon and begin reversing its destructive effects seem eerily wanting." (Coutu, 2019) [10]

Contu leads us down a path of 77 pages increasing expenditures, extreme policy making, fear and complete hype applied to emission controls in the aviation industry. Try these on for size: " The global climate change is one of the greatest, if not THE greatest human-made threats to its survival that humanity has ever faced."[11] "Humanity may not survive.." "There is no doubt that the Environmental / Climate Change megatrend will have major impacts on the aviation industry over the next 15-20 years and beyond. " (Coutu, 2019) Finally, his core premise is " Greenhouse gases (GHG) generated mostly by human activity are at the heart of climate change, (aka global warming). Half the fossil-fuel CO2 emissions produced by human activity in the last 300 years have occurred since the late 1980's and the 2014 global fossil-fuel carbon emission estimate was an all-time record." (Coutu, 2019) Again we have a good segway into a discussion about GHG.

Greenhouse Gases – our security blanket

The **greenhouse effect**,(GE) the important mechanism by which the earth remains, comfortably warm, and livable, is also the pretext for the advancement of the doomsday predictions about carbon dioxide-driven global warming. It is central to the CC debate. It is central to the (Coutu, 2019) presentation. Lets see if we can boil down the GE to basics.

While 30% of the Sun's radiation is reflected by clouds, most of it passes through the earth's atmosphere and strikes the surface. There it is absorbed and its energy is emitted in the near-infrared spectrum. [12] Some of the re-emitted energy is absorbed by greenhouse – gas molecules. As they absorb radiation, they in turn emit energy in the form of heat. This is the **greenhouse effect.** (Wrightstone G. , 2017)

Greenhouse gases and the warming they cause keep the Earth at a comfortable average temperature of 15o

Celsius (59o Fahrenheit). Without them, the Earth would be unlivable – 18o C (-0.4o F). (Wrightstone G. , 2017)[13] Extremes of GE warming are nearby planets of Venus & Mars. See Table 7.2 The Goldilocks effect. (Wrightstone G. , 2017)

Table 7.2 The Goldilocks effect.

Planet	Atmospheric composition	Surface Temperature (no greenhouse effect)	Relative size of greenhouse effect	Mean surface temperature
Venus	96% CO2	−40 oC (-40 o F)	100	462 oC (863 o F)
Earth	0.04% CO2 Ideal for life	-18 oC (-0.4 o F)	1	15 oC (59 o F)
Mars	95% CO2	-56 oC (−69 o F)	0.1	−55 oC (-67 o F)

Source: (Wrightstone G. , 2017)

The most significant greenhouse gas (driver) of all is **water vapor**. CC enthusiasts (Coutu, 2019) do not mention it at all. National Geographic and EPA list the greenhouse gases "include carbon dioxide (CO2) , methane, nitrous oxide (N2O), fluorinated gases, and ozone." (Wrightstone G. , 2017) A breakdown of these gases excluding water vapor is methane 19%, carbon dioxide 63% and other 18%. But including water vapor the breakdown is water vapor 90%, carbon dioxide 6%, methane 2% and other 2%. So water vapor contributes the lions share of the greenhouse effect. (Wrightstone G. , 2017) Both (Coutu, 2019) and (Wrightstone G. , 2017) agree that water vapor is a primary driver. There is serious disagreement on how much warming will occur due to increases of GH gases, or how much of that warming is or will be man-made. (Wrightstone G. , 2017) Warming allows the atmosphere to increase the amount of water vapor it can carry, which can then add to the GH effect (water-vapor feedback), but neither reference agrees on magnitude of this multiplier effect on global warming. Overblown estimates of water-vapor feedback will lead to overestimating the future warming in the climate models. This is why they fail. (Wrightstone G. , 2017)

Fact 1

Carbon dioxide is NOT the primary greenhouse gas.

Analysis

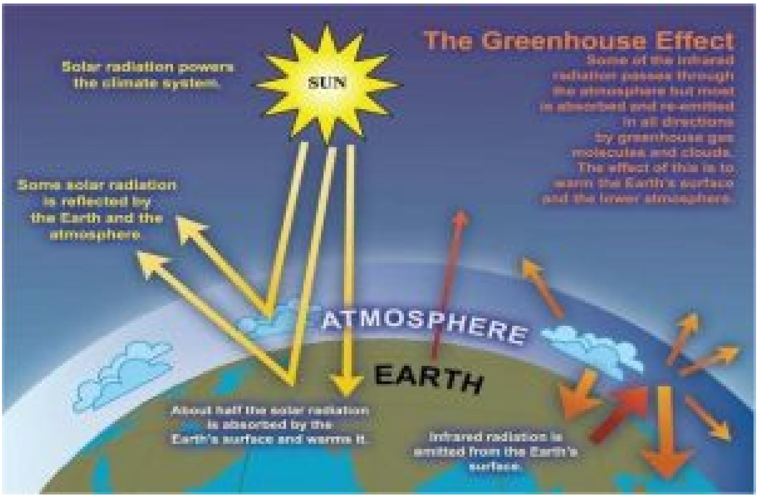
It is no more sensible to attempt to regulate weather by declaring CO2 to be a pollutant than it is to try to regulate water vapor or declare it to be a pollutant. Water vapor is the main contributor to the GH effect. (Wrightstone G. , 2017) The role of water vapor in climate models and predictions on it is an inexact science. The amount of water in the atmosphere varies markedly from place to place and from day to day. Absolute humidity can range from near zero in deserts and Antarctica – the Earth's driest continent to about 4% in the steamy tropics. Small changes in water vapor can so affect the GH effect as would a doubling of the present CO2 in the atmosphere. (Wrightstone G. , 2017) Downplaying or disregarding water vapor, or assigning too large a magnitude to feedbacks such as water vapor feedback will amplify the direct warming from CO2, and overemphasize man's contribution to the GH effect. (Wrightstone G. , 2017)

Fact 2

The warming effect of CO2 declines as its concentration increases.

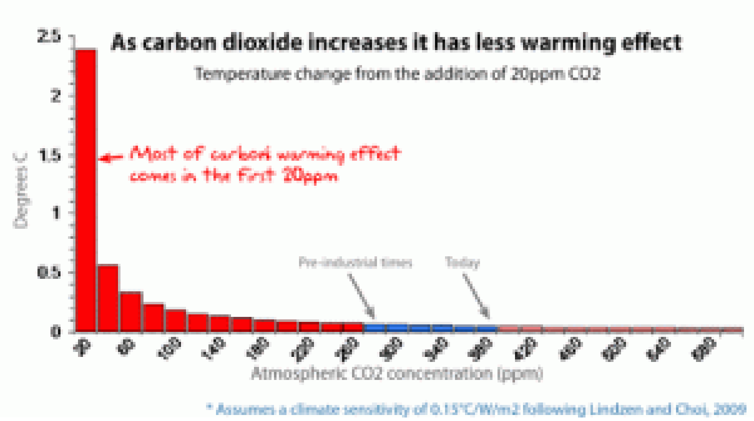
The warming effect of each molecule of CO2 decreases logarithmically as its concentration increase. (Wrightstone G. , 2017) Think about Fact 2 for a moment. Why haven't we experienced runaway GH warming when the concentration of CO2 was approaching 20X that of today? If you think about this fact, it undermines the theory of future catasphrophic climate change. [prediction per (Coutu, 2019)] Figure 7.2 shows that the principle of diminishing returns applies, i.e. as CO2 concentrations increase, the global warming effect diminishes. (Hoskins, 2014)

Figure 7.1 The Greenhouse Effect


The Greenhouse Effect
Some of the infrared radiation passes through the atmosphere but most is absorbed and re-emitted in all directions by greenhouse gas molecules and clouds. The effect of this is to warm the Earth's surface and the lower atmosphere.
Solar radiation powers the climate system.
SUN
Some solar radiation is reflected by the Earth and the atmosphere.
ATMOSPHERE
EARTH
About half the solar radiation is absorbed by the Earth's surface and warms it.
Infrared radiation is emitted from the Earth's surface.

Source: (Deshmukh, 2020)

Figure 7.2 The diminishing influence of increasing Carbon Dioxide on temperature



Source: (JoNova, 2010)

From Facts 1 & 2, we note that CO2 is a GH gas and that increasing CO2 concentrations will increase global temperature to a small degree. However, is this slight warming effect overwhelmed by natural climate drivers that have been active for hundreds of millions of years? (Wrightstone G. , 2017) And is it worth $100 trillion dollars or more to reduce a small increase of CO2?

Combined Fact(s) 3

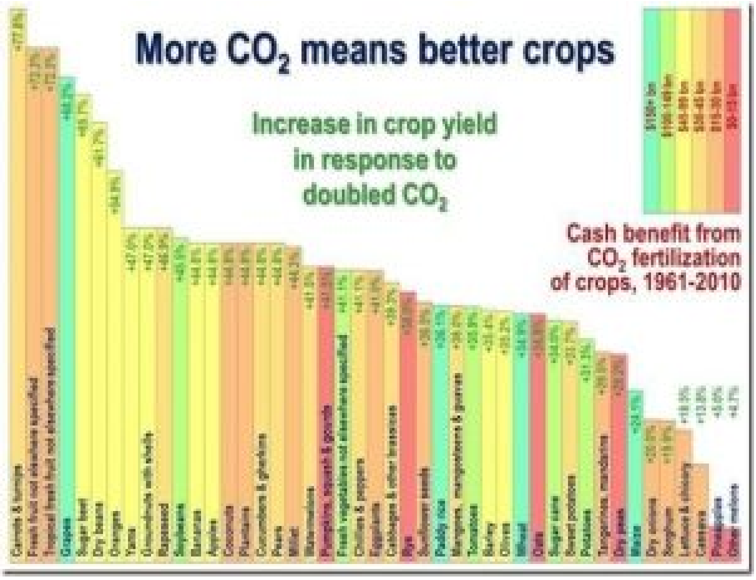
CO2 is not the demon causing catastrophic global warming; it is in fact an essential plant food. It means more plant growth, more food for people worldwide, and soil with more moisture.

According to the NIPCC, higher CO2 concentrations has the following benefits:

- Nearly all plants increase photosynthesis in response to increasing CO2 (CO2 fertilization)[14]
- More CO2 makes plants grow faster, with less stress and less water.
- Forests grow faster in response to increasing CO2
- More CO2 stimulates growth of beneficial bacteria in both soil and water.
- CO2 fertilization, leads to more plant growth, means less erosion of topsoil.
- More CO2 means bigger crop yields, and bigger flowers.
- More CO2 fosters glomalin, a beneficial protein created by root fungi.
- More CO2 means less water loss, less irrigation, and more soil moisture.
- More CO2 helps plants to create natural repellents to fight insect predators. (Carter RM, 2014)(Wrightstone G. , 2017)

Figure 7.3 improves on the above benefits description.

Figure 7.3 Shows 45 crops with crop yield growth and cash benefit with 300 ppm more CO2 (based on 3,586 experiments on 549 plant species)



Sources: (Monckton, 2019) (Idso, 2014)

Fact 4

400 PPM of CO2 is not a tipping point, not science and disinformation (propaganda)

"We are on the precipice of climate system tipping points beyond which there is no redemption."

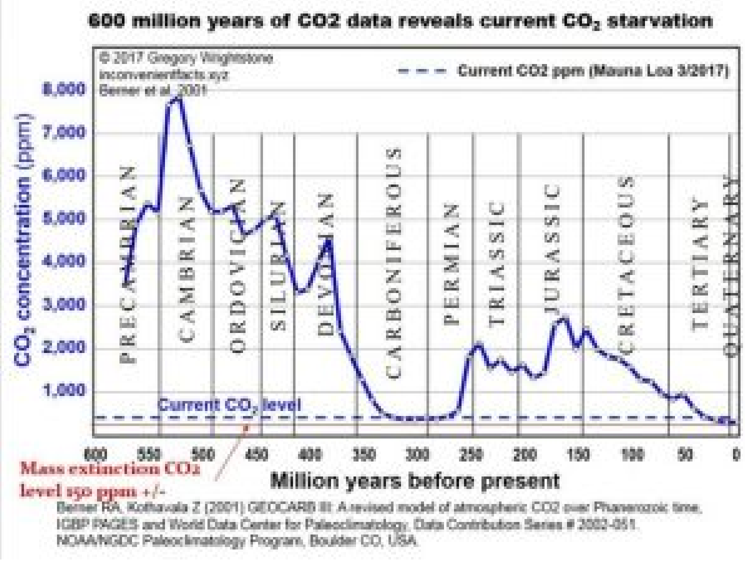
–James Hansen, Former head of NASA's Goddard Institute for Space Studies. (Wrightstone G. , 2017)

“This March [2014], global levels of CO2 passed 400 PPM..Already we are seeing the deadly effects of climate change in the form of rising seas, monster storms, wildfires, and extreme weather of all kinds. Passing 400 PP is an ominous sign of what might come next.” [15] (400.350.org, 2014)

The concentration of CO2 in the air has increased from about 280 PPM by volume in the mid-18th century, to a little above 400 PPM today. If we view this recent data through a narrow time-frame of a few decades

or centuries, this increase in 120 PPM in CO2 appears significant. But it is not on the timeline of Earth’s history. (Wrightstone G. , 2017) (Coutu, 2019)

Figure 7.4 Carbon Dioxide – 600 Million Years of Data



Berner RA, Kothavala Z (2001) GEOCARB III: A revised model of atmospheric CO2 over Phanerozoic time. IGBP PAGES and World Data Center for Paleoclimatology, Data Contribution Series # 2002-051. NOAA/NGDC Paleoclimatology Program, Boulder CO, USA.

Source: (Berner RA, 2001)

The notion of a “tipping point” beyond which Earth cannot recover, without a drastic reduction in CO2 emissions, is not science. It is disinformation by climate extremists and contradicts Earth’s history (reality).

Figure 7.4 shows that CO2 levels were many multiples of 400 PPM during virtually all of Earth’s history.

400 PPM represents an arbitrary number that was selected because it could likely be reached by 2014. (Wrightstone G. , 2017) It was an easy way to stoke fires of anti-CO2 legislation.

Fact 5

Our current geological period (Quaternary) has the LOWEST average CO2 levels in the history of the Earth[16]

Contrary to the disinformation from the media that today’s CO2 concentration is unprecedented, our current geologic period, has seen the lowest average levels of carbon dioxide in the Earth’s long history. The average CO2 for the past 800,000 years was 230 PPM. (Lüthi, et al., 2008)

The average CO2 concentration in the preceding 600 million years (Figure 7.4) was more than 2600 PPM, nearly 7X our current amount and 2.5 X the worst case predicted by the IPCC for 2100. Our current geological period (Quaternary) has the LOWEST *average* CO2 *concentration* in the history of the Earth. (Berner RA, 2001)

Ed Ring wrote a scathing letter which is quoted in part:

“What historians will definitely wonder about in future centuries is how deeply flawed logic, obscured by shrewd and unrelenting propaganda, actually enabled a coalition of powerful special interests to convince nearly everyone in the world that carbon dioxide from human industry was a dangerous, planet-destroying toxin."

"It will be remembered as the greatest mass delusion in the history of the world; that carbon dioxide, the life of plants, was considered for a time to be a deadly poison." [17] (Ring, 2015)

The carbon dioxide molecule, which has been more recently defined by radical environmental groups as a pollutant or poison, is absolutely essential to sustain plant and animal life here on Earth. To corrupt the English language in this way is simply a sleazy tactic to demonize this life-giving gaseous molecule."

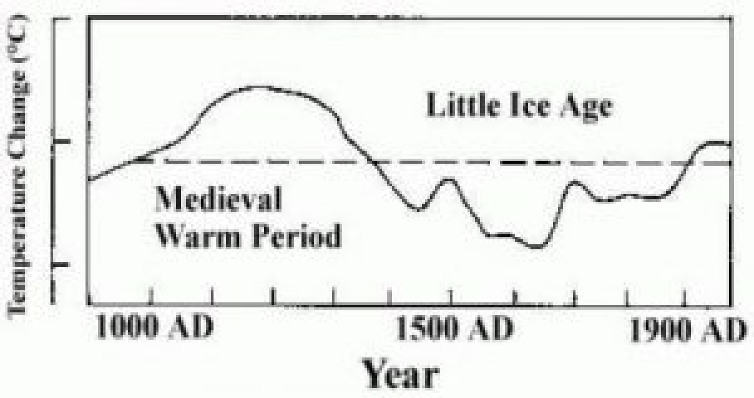
Temperature

Climate change enthusiasts tell us that the warming of recent decades is unusual and unprecedented. (Coutu, 2019) Climate -science research has focused on recent record – 250 years for thermometers and 50 years for satellites. This short time span skews interpretation of data. (Wrightstone G. , 2017)[18] To put the data into proper context, we need to take a long-term geologic perspective – thousands and millions of years.

Hockey- Stick Graph and prediction of Unprecedented Global Warming

Until 1998 the consensus view was that over the last several thousand years temperatures had risen and fallen as shown in noted climatologist Hubert Lamb's graph, Figure 7.5. (Houghton J. J., 1990)

Figure 7.5 Hubert Lamb's temperature graph of the past 1,100 years



Source: (Houghton J. J., 1990)

Study this figure. The figure shows warming beginning in the late 17th century as earth began to extract itself from the Little Ice Age (1250-1850). It was followed by recent temperatures significantly less than those experienced in the Medieval warming period (950-1250). Previous "consensus" established several warm periods had occurred over the last 10,000 years[19] and *all were warmer than today*, even though CO2 *concentration was only* 70% of today's. Note that higher temperatures at lower CO2 concentrations does not support the notion that connects rising CO2 to a harmful temperature increase to justify draconian measures to reduce carbon footprint. (Coutu, 2019) v (Wrightstone G. , 2017) Another observation by IPCC is that the current warming trend began more than 200 years before any significant man-made contribution to the GHG in the atmosphere. (Houghton J. e., 2001) See Figure 7.6.

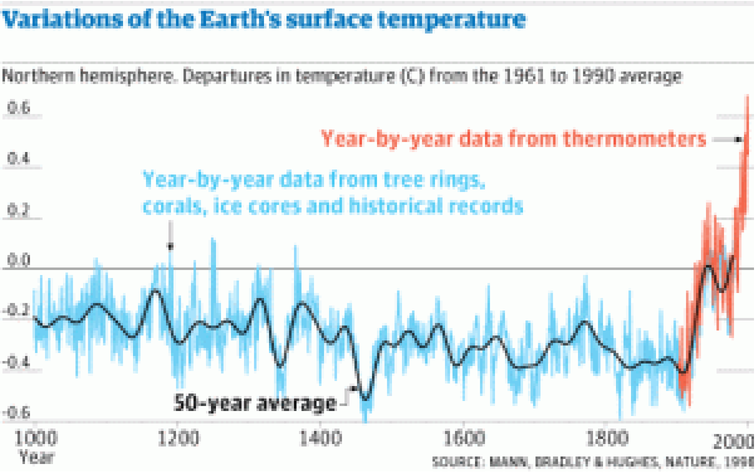
Michael Mann

Mann and his team purported to reconstruct 1,000 years of the Earth's temperature. They stated " temperatures in the latter half of the 20th century were *unprecedented* and that even the warmer intervals in the reconstruction pale in comparison with the mid-to-late 20th- century temperatures." This is the famous "hockey

-stick graph" which shows the 900-year shaft of slowly declining temperature followed by by a short blade of rapidly increasing temperature. (Mann ME, Global-Scale temperature patterns and climate forcing over the past six centuries , 1998) (Mann ME, Northern Hemisphere Temperatures during the post millennium: Inferences, Uncertainties, and Limitations, 1999) (Houghton J. e., 2001)

The hockey-stick graph became the linchpin as "proof" of the causal link between GHG and dangerous warming. (Houghton J. e., 2001)

Figure 7.6 Mann-made Hockey Stick



Source: (Mann ME, Global-Scale temperature patterns and climate forcing over the past six centuries , 1998) (Houghton J. e., 2001)

If Mann's depiction of temperature is correct, then his work is fundamental basis for recent warming being man-made. However, both sides of the CC argument have criticized the Mann graph. Two fundamental errors are data sourcing and data handling. Mann based his work on temperature proxies on a relatively small dataset of tree-ring data from California bristlecone pines, and a very small sample from cedars on the Gaspe Peninsula. The IPCC (his biggest fan) challenged the sourcing as a poor choice because the width of annual tree-ring will grow thicker only when the weather is warmer, but also wetter, or when more CO2 in the air fertilizes the tree and boosts growth. (Wrightstone G. , 2017) Mann ignored a significant number of trees in the sample area that did not show results that he desired. (Mann ME, Global-Scale temperature patterns and climate forcing over the past six centuries , 1998)

Two Canadian researchers McIntyre and McKitrick (MM) found that ANY data they plugged into Mann's formula produced the hockey-stick effect. They concluded that the temperature reconstruction was fatally flawed, poor handling of data and incorrect calculation. (Mann, 1998) (Jones, 2004) (Rutherford, 2004) To be fair, the MM challenge was also challenged by climate change enthusiasts as false procedures. (McKitrick, 2005) (Anonymous, 2004) [20]

Temperature Measurement

Of the three ways to measure atmospheric temperature: land and ocean surface thermometers (since 1659); weather balloons (mid-1950's) and satellites (since 1979) , satellites is the most reliable but with a short history. So what does this tell us? For the last 50 years , temperature measurements are accurate and this supports the Mann proposition of rapidly accelerating temperature data in the most recent five decades. If Mann's modelling of global temperatures were correct, then 900 years of cooling would be followed by a sharp temperature increase in the 20th century. This would be strong evidence linking man's activities to modern GW. *The counter evidence to the Mann argument would be data showing* *that modern warming began before CO2 began to rise sharply*. (Wrightstone G. , 2017) (Coutu, 2019) does not address this important issue. If the latter can be demonstrated , it would suggest that natural forces were the primary driver of warming prior to 1900 and likely remain in effect today.

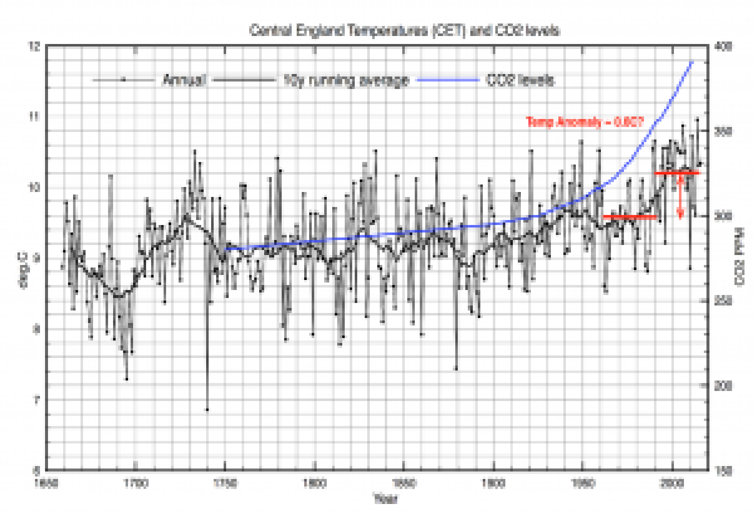
HadCET

The Central England temperature record (HadCET) contains the longest continuous measured regional temperature dataset in the world. It goes back more than 350 years. It began in 1659, during the coldest temperatures in the last 4,500 years. (Parker DE, 1992)(Boden TA, 2016)(Wrightstone G. , 2017)

Fact 6

Modern Warming began long before SUVs, Model T's or coal-fired plants, or modern planes

Figure 7.7 Central England Temperatures (CET) from 1659-2017 and CO2 levels



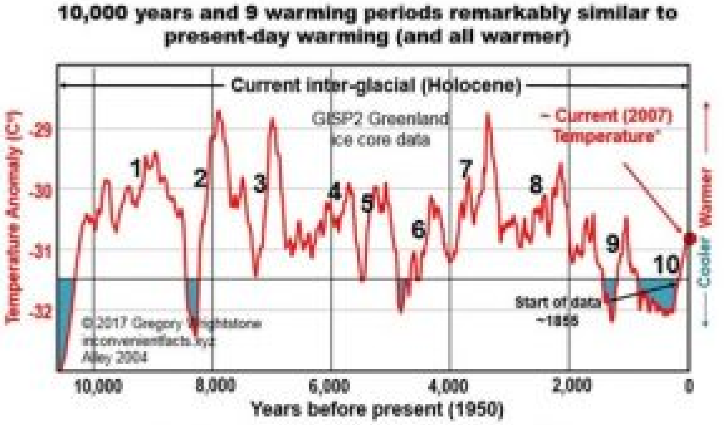
Source: (Best, 2017)[21]

Each period on Figure 7.7 has a name and associated effects on humanity. The key takeaway is that warming began more than 200 years before any significant contribution of man-made CO2 to the atmosphere. This contradicts the Mann hockey-stick depiction of steady cooling during this time. The natural forces driving temperature increases during the 18th and 19th centuries did not abruptly cease to act during the 20th century. (Wrightstone G. , 2017) (Boden TA, 2016) sees the same CET data but measures the CO2 in billions of metric tons emissions globally on the right horizontal axis. This is more dramatic in that CO2 emissions (bmt) is practically zero in 1759 -1859; is still less than 2 bmt in 1959 and then rises to 11 bmt in 2009. (Boden TA, 2016)

Melting Glaciers and Rising Sea Levels

(Wrightstone G. , 2017) spends considerable space on the argument that melting glaciers and rising sea levels confirm warming predated increases in CO2. The most significant Figure is his I-30 showing 10,000 years of warmth. Look at Figure 7.8.

Figure 7.8 10,000 years of warming



Alley, R.B.. 2004. GISP2 Ice Core Temperature and Accumulation Data. IGBP PAGES/World Data Center for Paleoclimatology Data Contribution Series #2004-013. NOAA/NGDC Paleoclimatology Program, Boulder CO, USA.
*Current Temp: Box JE, Yang L, Bromwich DH, Bai L (2009) Greenland Ice Sheet Surface Air Temperature Variability: 1840–2007". American Meteorological Society, Journal of Climate Vol 22, pp 4029 - 4049

Sources: (Alley, 2004)

Figure 7.8 is a substantial dataset that shows that *modern warming is neither unusual or unprecedented.* The data show that for more than 6,100 years (60%) of the current interglacial warm period, the temperature was warmer than it is today. Of the 9 significant periods of warming, since the last ice age, 5 had higher rates of temperature increase and 7 had larger total increases in temperature. This should lead to fact 7.

Fact 7

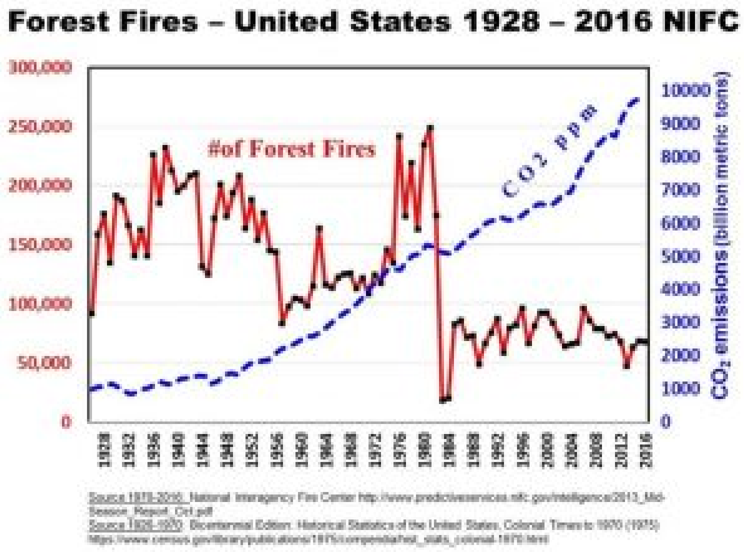
The current warming trend is a natural and predictable result

of driving forces since the last ice age (aka The Little Ice Age (1250-1850)

Forest Fires

Noted climatologist and egg layer, VP nominee Kamala Harris , in her attacks on Supreme Court nominee, Judge Amy Coney Barrett (ACB) stated unequivocally that forest fires are accelerating in frequency and size, owing to man-made climate change. The National Interagency Fire Center (NIFC) provides extensive information on forest fires in the United States. (NIFC, 2017) See Figure 7.9.

Figure 7.9 More CO2 but fewer forest fires



Source 1978-2016: National Interagency Fire Center http://www.predictiveservices.nifc.gov/intelligence/2013_Mid-Season_Report_Ctrl.pdf
Source 1928-1970: Bicentennial Edition: Historical Statistics of the United States, Colonial Times to 1970 (1975) https://www.census.gov/library/publications/1975/compendia/hist_stats_colonial-1970.html

Source: (NIFC, 2017)

Fact 8

Forest fires in the northern hemisphere are decreasing

A supporting study by the Canadian Forest Service (CFS) compared temperatures, CO2 concentrations and forest fire frequency over 150 years in North America. (Flannigan, Bergeron, Engelmark, & Wotton, 1998)

Their conclusions:

"*Despite increasing temperatures since the end of the* LIA**[22]**, *wildfire frequency has decreased as shown in many field studies from North America and Europe. We believe that* GW *since* 1850 *may have triggered decreases in fire frequency.*"**[23]**

Tornadoes

Tornadoes are scary because they kill and injure US citizens more than any other storm. The unique geography of the US makes it tornado-prone. The Rocky Mountains and the Gulf of New Mexico provide the key ingredients for formation of severe thunderstorms that spawn tornadoes: warm, moist air close to the ground; cool, dry air aloft; and horizontal winds that travel faster aloft than near the surface. (Wrightstone G. , 2017) NOAA keeps the records on tornadoes. [24] (NOAA, NOAA NCEI Historical Records and Trends, 2017) NOAA recommends only using the strongest tornadoes as a measure of pre-radar numbers. Doppler radar detection has facilitated better identification and reporting of tornados after WWII. Table 7.3 shows the tornados rank. NOAA recommends using 3+ on the scale for reporting. (NOAA, NOAA NCEI Historical Records and Trends, 2017)

Table 7.3 The Fujita tornado scale

F	**0**	**1**	**2**	**3**	**4**	**5**
Fastest ¼ mile (mph)	**40-72**	**73-112**	**113-157**	**158-207**	**208-260**	**261-318**
Fastest 3-second gust (mph)	**45-78**	**79-117**	**118-161**	**162-209**	**210-261**	**262-318**

Source: (NOAA, NOAA NCEI Historical Records and Trends, 2017)

Combined Facts 9

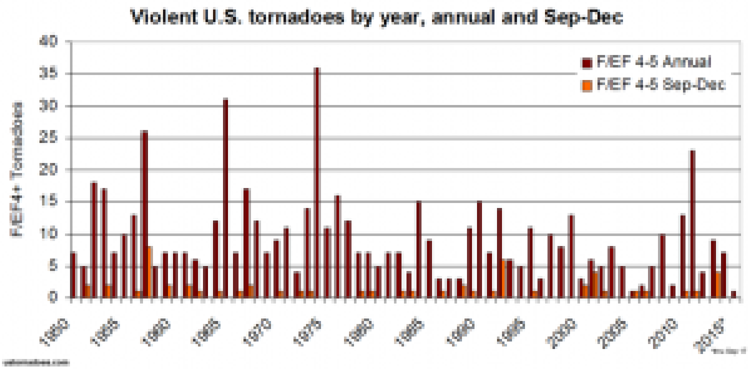
1. **The number of tornadoes is decreasing with 2016 showing**

the lowest on record (NOAA, NOAA NCEI Historical Records and Trends, 2017)

2. **CO2 global emissions has increased at the same time severe tornadoes (F3+) has decreased** (Boden TA, 2016)[25]
3. **US tornado deaths per million population continues to fall through 2000** (NOAA, us-annual-tornado-death-tolls-1875-present/, 2009)
4. **Science and data show no correlation between tornadoes and rising temperatures over the last 50 years.** (Wrightstone G. , 2017)

Figures 7.9-7.11 support the above FACTS 9. Figure 7.10 shows the decline of severe tornadoes (F3+) over last 50 years. Figure 7.11 shows that 2016 was a banner year. Figure 7.12 shows that tornado deaths per million population is also decreasing than 50 years ago.

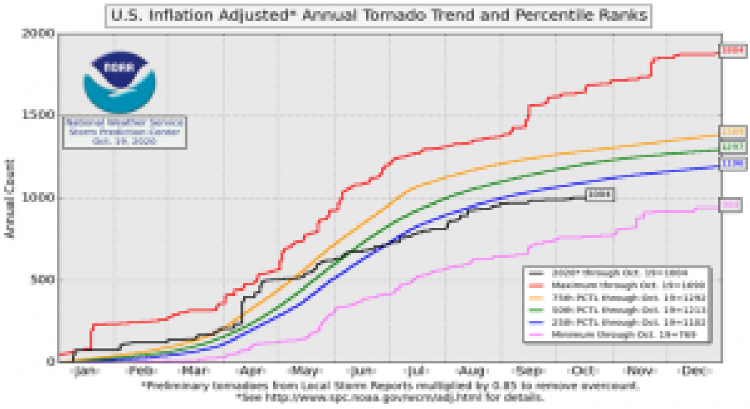
Figure 7.10 Severe tornadoes (F+4) are less frequent



Source: (ustornadoes.com, 2015)

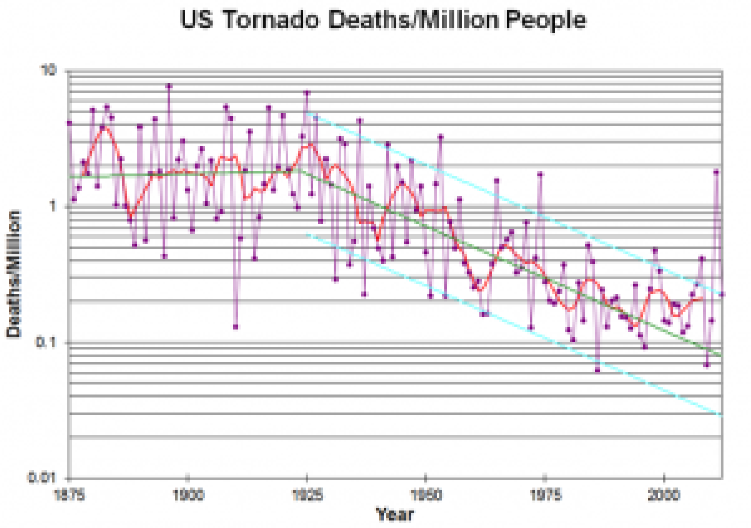
(Boden TA, 2016) confirms the growth of CO2 global emissions (bmt) [26] plotted against the same Figure 7.10 as increasing from 1954 -2015 to just under 10 bmt.

Figure 7.11 Lowest number of tornadoes in 2016



Source: (NOAA, Storm Prediction Center, 2020)
Note that 2106 had 901 tornadoes. 2020 logged 1004.

Figure 7.12 US tornado deaths per million population



Source: (NOAA, us-annual-tornado-death-tolls-1875-present/, 2009)

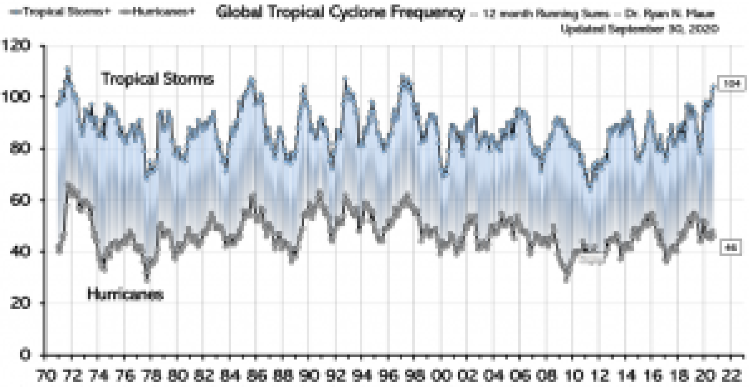
Hurricanes

Noted climatologist and egg layer, VP nominee Kamala Harris (now elected VP), in her attacks on Supreme Court nominee, Judge Amy Coney Barrett (ACB) also stated unequivocally that hurricanes are accelerating in frequency and size, owing to man-made climate change. *The conventional wisdom behind this thinking is that GW raises ocean temperatures, fueling tropical cyclones and hurricanes.* Actually, this sounds reasonable. However, we saw in our treatment of deadly tornadoes that the CW was wrong, and that the evidence / data suggested that frequency of deadly tornadoes was decreasing over last 50 years. (NOAA, NOAA NCEI Historical Records and Trends, 2017)

Promoters of the notion of GW causation of more severe hurricanes includes the National Climate Assessment (NCA) of 2014.

(Kossin JP, 2007) There review of power dissipation index vs time , using satellite-based re-analyses does show an solid increasing trend. Dr Ryan Maue challenged that data for insufficient range analysis.[27] (Maue, 2016) Using the entire dataset (not 15% like the NCA2014) and including land-falling hurricanes his conclusions were quite a bit different. (Maue R. , 2017) See Figure 7.13.

Figure 7.13 Global tropical storm and hurricane frequency is falling



Source: (Maue R. , 2017)

Dr Maue concluded that from 1970-2018 there is a downward trend of hurricane and tropical storm frequency. The author reviews the same data and sees an even or slight downward trend but not increasing.

Fact 10

There has been no increase in frequency of hurricanes in recent data

But what about the warming argument? Dr Landsea, a meteorologist at the National Hurricane Center (NHC) has quantified what an increase in intensity of major hurricanes, driven by GW, might mean. (Landsea, 2011) His work indicates that the warming over the last several decades translates into an increase of intensity of 1%. For Katrina (Cat 5), the wind speed would increase 2 mph. He wrote:

"The 1-2 mph change currently in the peak winds of strong hurricanes due to man-made GW *is so tiny that it is not measurable by our aircrafts* or *satellites technologies available today, which is only accurate to about* 10 *mph for major hurricanes*." (Landsea, 2011)

Which brings to Fact 11.

Fact 11

There is no significant increase in hurricane intensity due to warming

(Landsea, 2011) (Wrightstone G. , 2017)

Conclusions

This chapter has taken the idea that because of *man-made* GW / CC, our society is headed for climate Hell from which we cannot return. But Earth, its ecosystems, and we humans are actually **thriving** because of the increasing CO2 and rising temperatures, not in spite of it! (Wrightstone G. , 2017)

Yes there is a GH effect. Yes there is some warming. Yes, some of it might be man-made. We can expect more. They are all demonstrable. (Wrightstone G. , 2020)

But no, past and future anthropogenic warming does **NOT** mean that catastrophe will follow, or that measures to prevent GW are scientifically and economically justified. (Wrightstone G. , 2017) [Here we drastically differ from the thrust / organizational and investment measures suggested by (Coutu, 2019).]

As Wrightstone suggests, "*the first and most important conclusion is that the correct policy to address the non-problem of man-made global warming is to have the courage to do nothing*." (Wrightstone G. , 2017)

Questions

1) There are other claims about GW affects: ocean acidity, polar bears, melting ice caps, droughts, crops, and sea-level rise to name just a few. Choose one topic to research and see if you agree with the conventional wisdom and "consensus" or can you develop / find data / synthesize data using the scientific method that at least puts CW into question on your choice as to voracity. Make up your own mind. [28]

References

400.350.org. (2014). *GLOBAL CO2 CONCENTRATIONS JUST PASSED 400 PARTS PER MILLION.* Retrieved from 400.350.org/: http://400.350.org/

Alley, R. (2004). *GISP2 Ice Core Temperature and Accumulation Data.* Retrieved from ftp.ncdc.noaa.gov/pub: ftp://ftp.ncdc.noaa.gov/pub/data/paleo/icecore/greenland/summit/gisp2/isotopes/gisp2_temp_accum_alley2000.txt

Anonymous. (2004, December). *false-claims-by-mcintyre-and-mckitrick-regarding-the-mann-et-al-1998reconstruction/.* Retrieved from www.realclimate.org/: http://www.realclimate.org/index.php/archives/2004/12/false-claims-by-mcintyre-and-mckitrick-regarding-the-mann-et-al-1998reconstruction/

Berner RA, K. Z. (2001, February 1). GEOCARB III: A REVISED MODEL OF ATMOSPHERIC CO2 OVER PHANEROZOIC TIME. *American Journal of Science*, pp. Vol 301: 182–204]. Retrieved from https://agbjarn.blog.is/users/fa/agbjarn/files/geocarb_iii-berner.pdf: https://agbjarn.blog.is/users/fa/agbjarn/files/geocarb_iii-berner.pdf

Best, C. (2017, January). *CET-annual-CO2.png.* Retrieved from clivebest.com/blog: http://clivebest.com/blog/wp-content/uploads/2017/01/CET-annual-CO2.png

Boden TA, M. G. (2016). Global CO2 emissions from Fossil-Fuel burning Cement Manufacture and gas flaring 1751- 2013. *Carbon Dioxide Information Analysis Center*, , Oak Ridge Nat Lab.

Boller, J. P., & George, J. (1989). *They Never Said It: A Book of Fake Quotes, Misquotes, and Misleading Attributions.* New York: Oxford University Press. pp. 124–126.

Bolton, D. (2016, April 13). *97% of scientists believe climate change is caused by humans, study finds.* Retrieved from independent.co.uk/: https://www.independent.co.uk/news/science/global-warming-climate-change-man-made-scientific-consensus-study-a6982401.html

Boyle, L. (2020, October 15). *amy-coney-barrett-climate-change-supreme-court-2020-election.* Retrieved from www.independent.co.uk: https://www.independent.co.uk/environment/amy-coney-barrett-climate-change-supreme-court-2020-election-b1041390.html

Carter RM, e. a. (2014). Biological Impacts. In H. Institute, *Climate change reconsidered* II. Chicago: Idso CD, Idso SB.

Cook, J. N. (2013). Quantifying the consensus on anthropogenic global warming in the scientific literature. *Environ Res Lett*, 8(2):024024.

Coutu, P. (2019). *Global Megatrends and Aviation- The Path to Future-Wise Organizations.* Montreal: ASI Institute.

Deshmukh, C. (2020, October 16). *Greenhouse_gas_emissions_CH4_CO2_and_N2O_from_a_newly_flooded_hydroelectric_reservoir_in_subtropical_South_Asia_The_case_of_Nam_Theun_2_Reservoir_Lao.* Retrieved from www.researchgate.net/: https://www.researchgate.net/publication/278643412_Greenhouse_gas_emissions_CH4_CO2_and_N2O_from_a_newly_flooded_hydroelectric_reservoir_in_subtropical_South_Asia_The_case_of_Nam_Theun_2_Reservoir_Lao_PDR/figures?lo=1

Flannigan, M. D., Bergeron, Y., Engelmark, O., & Wotton, B. M. (1998). *Future Wildfire in Circumboreal Forests in Relation to Global Warming.* Retrieved from sites.ualberta.ca/~Flannigan/

publications/: https://sites.ualberta.ca/~flanniga/publications/1998%20Flannigan%20et%20al.%20J%20Veg%20Sci%20-%20Future%20wildfire%20in%20circumboreal.pdf

Hoskins, E. (2014, August 10). *the-diminishing-influence-of-increasing-carbon-dioxide-on-temperature/.* Retrieved from https://wattsupwiththat.com: https://wattsupwiththat.com/2014/08/10/the-diminishing-influence-of-increasing-carbon-dioxide-on-temperature/

Houghton, J. e. (2001). *Climate Change 2001 The Scientific Basis. Contribution of Working Group I to the Third Assessment Report on Intergovernmental Panel on Climate Change.* New York: Cambridge University Press.

Houghton, J. J. (1990). *Climate Change The IPCC Scientific Assessment.* New York: Cambridge University Press.

Idso. (2014). *The positive externalities of carbon dioxide.* Retrieved from www.co2science.org: http://www.co2sciuence.org/education/reports/co2benefits/monetarybenefitsof risingCO2on globalfoodproduction.pdf

Jones, P. M. (2004). Climate Over Past Millennia. *Reviews of Geophysics*, 42, RG2002, doi: 10.1029/2003RG000143, 2004.

JoNova. (2010, February 2). *carbon-dioxide-is-already-absorbing-almost-all-it-can.* Retrieved from http://joannenova.com.au/: http://joannenova.com.au/2010/02/4-carbon-dioxide-is-already-absorbing-almost-all-it-can/

JVL. (2020, October 15). *Joseph Goebbels: "On the Big Lie"* . Retrieved from jewishvirtuallibrary.org: www.jewishvirtuallibrary.org

Kossin JP, K. K. (2007). *Geophysical Research Letters.* Retrieved from nca2014.global-change.gov: http:nca2014.global-change.gov/search/node?search_api_views_fulltext=hurricane%20pdi

Landsea, C. (2011). *Hurricanes and Global Warming. Opinion Piece on* NOAA *website* . Retrieved from www.aoml.noaa.gov: http://www.aoml.noaa.gov/hrd/landsea/gw_hurricanes

Legates, D. S. (2015). Climate consensus and 'misinformation': a rejoinder to 'Agnotology, scientific consensus, and the teaching and learning of climate change. *Sci Edu*, 24:299-318.

Lüthi, D., Le Floch, M., Bereiter, B., Blunier, T., Barnola, J.-M., Siegenthaler, U., . . . Stocker, T. F. (2008). High-resolution carbon dioxide concentration record 650,000 – 800,000 years before present. *Nature*, pp. 453, 379-382. doi:https://doi.org/10.1038/nature06949

Mann ME, B. R. (1998). Global-Scale temperature patterns and climate forcing over the past six centuries . *NATURE*, Vol 392.

Mann ME, B. R. (1999). Northern Hemisphere Temperatures during the post millennium: Inferences, Uncertainties, and Limitations. *Geophysical Research Letters*, Vol 26, No 6, pp 759-762.

Mann, M. R. (1998). Global-scale temperature patterns and climate forcing over the past six centuries. *Nature*, 392, 779-787.

Maue. (2016). *Atlantic Basin Power Dissipation Index from HURDAT2.* Retrieved from models.weatherbell.com/tropical.php: http: //models.weatherbell.com/tropical.php

Maue, R. (2017). *Global tropical Cyclone activity.* Retrieved from weatherbell models: http: //models.weatherbell.com/tropical.php

McKitrick, S. M. (2005, February). *Hockey sticks, principal components, and spurious significance.* Retrieved from agupubs.onlinelibrary.wiley.com:
https://agupubs.onlinelibrary.wiley.com/doi/full/10.1029/2004GL021750

Monckton, C. (2019, September 17). *if-sir-david-king-is-scared-about-global-warming-we-neednt-worry/.* Retrieved from wattsupwiththat.com: https://wattsupwiththat.com/2019/09/17/if-sir-david-king-is-scared-about-global-warming-we-neednt-worry/

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

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

Domain, 2nd Edition. Manhattan, KS: NPP eBooks. 27. Retrieved from www.newprairiepress.org/ebooks/27

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

NIFC. (2017). *NIFC Total Wildland Fires and* CO2 *(1960-2015).* Retrieved from www.nifc.gov: https://www.nifc.gov/fireinfo/fireinfo_stats_totalfires,html

NOAA. (2009, March). *us-annual-tornado-death-tolls-1875-present/.* Retrieved from https://inside.nssl.noaa.gov: https://inside.nssl.noaa.gov/nsslnews/2009/03/us-annual-tornado-death-tolls-1875-present/

NOAA. (2017). NOAA NCEI *Historical Records and Trends.* Retrieved from www.ncdc.noaa.gov: https://www.ncdc.noaa.gov/climate-information/extreme-events/us-tornado-climatology

NOAA. (2020). *Storm Prediction Center.* Retrieved from https://www.spc.noaa.gov/wcm/adj.html: https://www.spc.noaa.gov/wcm/adj.html

Parker DE, L. T. (1992). A new Daily Central England Temperature Series 1772-1991. *Int. J. Clim.*, Vol 12, pp 317-342.

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

Ring, E. (2015, January 22). *opinion/letters-to-the-editor/letter-politics-disguised-as-science/.* Retrieved from https://www.aspentimes.com: https://www.aspentimes.com/opinion/letters-to-the-editor/letter-politics-disguised-as-science/

Rutherford, S. M. (2004). Proxy-based Northern Hemisphere Surface Temperature Reconstructions: Sensitivity to Methodology, Predictor Network, Target Season and Target Domain. *Journal of Climate*, in press.

Tallentyre, S. (1906). "*Helvetius: The Contradiction*". *The Friends of Voltaire.* London: Smith, Elder, & Co. p. 199.

ustornadoes.com. (2015, September). *violent-tornadoes-by-*

year-2015. Retrieved from www.ustornadoes.com: https://www.ustornadoes.com/wp-content/uploads/2015/09/violent-tornadoes-by-year-2015.gif

Wikipedia. (2020, October 15). *James_Watson*. Retrieved from en.wikipedia.org/: https://en.wikipedia.org/wiki/James_Watson

Wikipedia. (2020, October 17). *Photosynthesis*. Retrieved from en.wikipedia.org: https://en.wikipedia.org/wiki/Photosynthesis

Wikipedia. (2020, October 15). *Scientific Method*. Retrieved from en.wikipedia.org/: https://en.wikipedia.org/wiki/Scientific_method

Wrightstone, G. (2017). *Inconvenient Facts: The science that Al Gore doesn't want you to know*. New York, NY: Silver Crown Productions.

Wrightstone, G. (2020, October 17). *statement-to-the-pa-environmental-resources-energy-committee*. Retrieved from inconvenientfacts.xyz: https://inconvenientfacts.xyz/blog/f/statement-to-the-pa-environmental-resources-energy-committee

[1] Translate as "crises."

[2] Special Disclaimer:

The author of this chapter is not a climatologist. His formal training in weather is limited to USCG courses taken as an Ensign in USCGA, to better his experience as a boat captain. He is an experienced engineer, scientist, advanced mathematician, author, managing editor, and qualified researcher. His experience includes five decades of advanced simulation and modeling experience for chemical engineering, business, and INFOSEC / counterterrorism processes. He is recognized as a Subject Matter Expert in cryptology and forensics by the USDOJ and an SME in counterterrorism by the DTRA. He knows how to differentiate facts from fiction and to develop complex risk assessments of key threats, vulnerabilities, impact, and countermeasures for information and intelligence systems – most recently with unmanned aircraft systems. The point is he is neither a sheep nor parrot of conventional wisdom. He knows how to think and judge for himself the issues/ information in dispute. Climate change is a contentious issue where many minds are closed to challenges of their basic beliefs. However, by definition, scientific research is a constant challenge of our beliefs in the natural processes and order. By its very nature and methodology, scientific research provides us with tools to better understand our environment free (or should be free) of political or financial pressures to divine an answer because of popularity or agenda. Recognizing that the author does not breathe in a vacuum, this chapter does not necessarily represent the opinions of my employer, my professional Board(s) associations, certifying authorities, my team, my colleagues, my oldest daughter or newest daughter-in-law, my congressmen or state senators and any individual or organization that sponsors / reads my work or hears my presentations on unrelated issues like counter unmanned aircraft systems. The information provided is based on personal reasonable research and proffered as an alternative to "conventional wisdom."

[3] This is exactly what a SCOTUS nominee should do. Remain neutral and avoid public comment on contentious issues of public policy.

[4] This statement has been thrown around in so many media that it goes unchallenged. Saul Alinsky in his "Rules for Radicals" is credited with "if you tell a lie big enough and keep repeating it, people will eventually come to believe it." The actual source is Joseph Goebbels, Nazi propaganda minister. (JVL, 2020)

[5] The author is both a scientist and engineer. He was introduced to the method in 1959. In 1962, the author was awarded, as a senior in HS, a scientific internship and scholarship to Rockefeller Institute of Technology in NYC. In that august body one of the most famous

scientific discoveries was made and awarded the Nobel Prize to James Dewey Watson KBE an American molecular biologist, geneticist, and zoologist. In 1953, he co-authored with Francis Crick the academic paper proposing the double helix structure of the DNA molecule. Watson, Crick and Maurice Wilkins were awarded the 1962 Nobel Prize in Physiology or Medicine "for their discoveries concerning the molecular structure of nucleic acids and its significance for information transfer in living material" (Wikipedia, James_Watson, 2020) The author's contribution to DNA human genome mapping project was merely running a gas chromatograph and summarizing datasets for the "suits." But I met the top guns at a celebration of Nobel Prize in the auditorium. My point – the DNA project is a terrific example of the application of the scientific method. The reference also details the methodology. (Wikipedia, Scientific Method, 2020)

[6] Note there is no political, financial influence or consensus required in this definition.

[7] Cooks' team has 12 volunteers who classify themselves as activists and 9 of them have no training at all in any science.

[8] Agnotology is defined as the study of how ignorance arises via circulation of misinformation calculated to mislead.

[9] It appears that Cook and his co-authors manipulated the data to present an altogether untrue narrative of overwhelming support for catastrophic human-caused warming.

[10] Try to recognize the bias, hysteria, and lack of scientific basis in this status quo approach. Look at the inflammation in the words.

[11] Seems to me that nuclear war at the instigation of hostile nations or complete economic failure of society might rank fairly high.

[12] See Nichols CUAS textbook (2020) for a complete description

and frequency allocation of the EMS and small the near-infrared spectrum is in terms of the entire allocation of frequencies. (Nichols R. K., et al., 2020)

[13] Fahrenheit is the authors choice, but the world adores Celsius. Engineers can work with both F or C. o F = 1.8 (o C) +32

[14] Photosynthesis is the process by which green plants and some other organisms use sunlight to synthesize foods from carbon dioxide and water. Photosynthesis is important to living organisms because it is the number one source of oxygen in the atmosphere. Green plants and trees use photosynthesis to make food from sunlight, carbon dioxide and water in the atmosphere: It is their primary source of energy. Photosynthesis is usually represented by the equation 6 CO2 + 6 H2O + light –> C6H12O6 + 6 O2. During this process, organisms such as plants go through the light-dependent and light-independent reactions to convert carbon dioxide and water into sugars and oxygen. The O2 produced is used by living organisms as a vital part of the synchronicity of the ecosystem. (Wikipedia, Photosynthesis, 2020)

[15] We will examine some of these extreme weather conditions in this chapter.

[16] All "Facts" statements in blue are based on or quoted from (Wrightstone G. , 2017)

[17] Ed Ring writes for the Climate Disinformation Database, https://www.desmogblog.com/global-warming-denier-database . (Ed Ring, EcoWorld, 2008) Dick Pilard picked up his Letter in Aspentimes https://www.aspentimes.com/opinion/letters-to-the-editor/letter-politics-disguised-as-science/

[18] During the writing of this chapter, the author of (Wrightstone G. , 2017) was suspended for 3 weeks for his anti-global warming opinion piece on LinkedIn. I personally felt that Linkedin was the last bastion of reasonable professional level discussions. Such

censorship and non-acceptance of differing professional opinions on key issues is common place to the level of vulgarity on Twitter and Facebook. Their leaders are under investigation by Congress. It is most disappointing that a professional network like Linkedin should join the anti-FOS crowd. (Author opinion only) It behooves us to remember that science is NOT consensus and consensus is not science. Another interesting issue is does the First Amendment apply to publicly held social networking corporations. Evelyn Beatrice Hall wrote the phrase: “I disapprove of what you say, but I will defend to the death your right to say it.” (Tallentyre, 1906) This quotation – which is sometimes misattributed to Voltaire himself – is often cited to describe the principle of Freedom Of Speech. (Boller & George, 1989)

[19] This included the Modern, Medieval, Roman, Minoan, Egyptian Old Kingdom and Holocene climate optima periods.

[20] The author has reviewed all four documents. The counterattack on MM claims by an anonymous “mike @ 4 December 2004” has some interesting points but hiding from the public strains the credibility.

[21] The Best figure is better representation of CET data than Figure I-24 in (Wrightstone G. , 2017) However, there many images covering the same CET / Hadley dataset and some showing declining warming. This contradiction can be resolved by presentation XY scales and units.

[22] LIA = Little Ice Age (1250-1850)

[23] The Flannigan team further attributed the decline in wildfires to the combined effect of CO2 fertilization and rising temperature, leading to greater soil moisture.

[24] For a tornado to be counted, it must be observed. Early records and evidence of tornadoes – even in *Tornado Alley* – are unreliable

for the sparsely populated early 20Th century. (NOAA, NOAA NCEI Historical Records and Trends, 2017)

[25] CO2 emissions per bmt previously shown in Figure 7.8. (Boden TA, 2016)

[26] Bmt = billions of metric tons

[27] Insufficient range = “cherry picking the data”

[28] Keep looking because there are active efforts to censor any dissent. Scientific inquiry and discoveries are not political tools, they are the basis of intelligent life.

8. Nightmare Technologies [Nichols]

Student Learning Objectives

Two simple objectives: To be technology aware and think about their harmful effects on your life.[1]

Emerging vs Disruptive Technologies

There is a difference between emerging technology trends and disruptive ones. *Emerging technologies* are technologies whose development, practical applications, or both are still largely unrealized, such that they are figuratively emerging into prominence from a background of nonexistence or obscurity. (Wiki, 2021) Some sources say that emerging technologies are taking over the world by a storm and if misused, it could turn out to be our worst enemy. (Rose, 2019) *Toward Data Science* magazine lists Drone Swarms as number one in their list. The topic is covered in detail in (Nichols R. , et al., 2020). Smart home devices that spy, ex. IoT or AI / IoT is number two, followed by facial recognition, spy dust and autonomous robots. (Rose, 2019)

A *Disruptive technology* is one that displaces an established technology and shakes up the industry or a ground-breaking product that creates a completely new industry. (Rouse, 2021) , In this chapter, we explode and explore nightmare disruptive technologies, that if they come to full fruition may do more harm than good. Some of them might reach Black Swan event status.[2] The technologies are not presented in any particular order. They all have the capability of bringing evil to our doorstep and crushing what is left of our right of privacy.

Surveillance Technologies

On 6 January 2021, the author asked his writing team of twelve

SMEs in their respective fields, the following questions: 1) *What surveillance technology would you consider the most invasive to our privacy as citizens?*

2) *What surveillance technology has the potential to be the most damaging to our society or military defenses or law enforcement operations*? The list was fascinating and ranged from the real to semi- fantasy.

The list included:

- Alexa / Siri / Cortona [ASC group] (cute names for a massive systems of systems – always "listening")
- Quantum computing, especially when coupled with the ASC group,
- AI driven quantum systems
- Voting machines that tilt the scales or select a candidate rather than tabulate / confirm results. Voting machines designed to be the perfect transparency laundering tool. This results in the ability to fake manual voting in scale.
- Cellphones (an addition that has destroyed personal communications and catalogued our lives for fodder). They are vessels for listening / data collection / tracking / and biometric identification theft.
- Implant technology – for use on humans – similar to use on animals for location rendering
- AI driven mechanics / robotics -replacements for humans when not really justified
- IoT – connecting things that were not meant to be connected and made available online.
- Blockchain (however, two major pitfalls exist: a) a replacement better security technology see our Chapter 6 on *Future Proof Security* and b) regulations by banks, IRS, agencies will crush speculative use.)
- Exploiting Automation & Human-Machine Symbiosis for the wrong reasons. See chapter 2 on this subject.
- Mini drones (covered in (Nichols R. , et al., Unmanned Aircraft

Systems (UAS) in Cyber Domain: Protecting USA's Advanced Air Assets, 2nd Edition, 2019) . Drones can be made so small Chinese stink bugs can't tell the difference.

- Nanobots or intelligent sand (aka MEMS)
- Drone Swarms [covered in detail in (Nichols R. , et al., 2020) and (Nichols R. , et al., Unmanned Aircraft Systems (UAS) in Cyber Domain: Protecting USA's Advanced Air Assets, 2nd Edition, 2019)]
- Face / Voice / Biometrics recognition
- Weaponized social media – especially FB, & Twitter
- GPS units in everything from cars, phones, boats, animals, aircraft, watches, hearing aids, you name it the technology has become ubiquitous.
- Identity cards / Health vaccination cards / Social media scores (like the Chinese experiment) Real ID/ ammunition purchase cards / gun registration – bureaucratic control -paperwork designed to erode U.S Constitution and its amendments for purposes of "our safety or for our kids"
- Legalization of every known illegal drug – tracking by health agencies and permission slips to replace doctor's script.
- Enforcement of politically correct speech by investigations, informants, indoctrination camps
- Surveillance of radio stations and advertisers with federal enforcement of against alternative views.
- Registration and subsequent licensing of every facet of our lives.
- Coordinating databases and information storage facilities (where every conceivable piece of information on individuals and All their communications, in every media; in every language with translation capabilities are kept, catalogued, interrogated using keywords and summarized for intelligence dossiers.) (Burrington, 2015) Large amounts of encrypted data are also sucked up by this surveillance vacuum on the assumption that new crypto-cracking methods will be developed as they have since 1972. (Nichols R. K., ICSA Guide to

Cryptography, 1999)

- Ransomware, AI, and Bot-enabled Blackmailing, Hacking and Extortion
- AI Cloning – Deep fake Technology for Voice and Video recordings.

The above list combines actual technologies with the abuse of those technologies. It is not all inclusive. Every new method of control and surveillance has been abused by authorities and recently by corporations. This abuse is usually discovered and legislated against – from habeas corpus to mail, telegraph, telephones, cell phones, internet, GPS on transportation, to implants. (Elliott, 2019) The trend according to Timo Elliott, noted Innovation Evangelist, is bound to continue – and potentially get much worse- with AI -powered technologies such as face recognition. (Elliott, 2019)

All the above technologies bring together many diverse / disparate information sources [3] to get a single view of an operation, location, geopolitical activity, defense theater of operations, or market. (Elliott, 2019)[4]

This can be a boon to businesses but a nightmare for society if used by malevolent minds.

Col Joel Anderson,[5] OVPR at KSU is quoted: " *He who controls information controls the world.*"

To that the chapter author would add that the most effective vehicle to gain information is unrestricted surveillance.

For years businesses and agencies around the world were essentially leveraged or perhaps held hostage for ransom using software and network flaws that were kept deliberately secret by NSA and CIA to use for 1) against enemies and 2) wield influence. (Elliott, 2019) (Zegart, 2017)

But these same agencies were hacked, and their secrets exposed / spread across the globe. (Kass, 2020) (Shane, 2019)

Today's secrets will not stay secret for long. All you have to do is look at the deleted, purged emails, text messages, GPS locations, of politicians, criminals, cheating spouses, drug dealers, terrorists, and movie stars exploited every day in the news media to convince yourself of this fact.

Alexa / Siri / Cortona [ASC group]

Perhaps the most invasive of the ASC group is Alexa. "Would you let a stranger eavesdrop in your home and keep the recordings? For most people, the answer is, "Are you crazy?" Yet that's essentially what Amazon has been doing to millions of us with its assistant Alexa in microphone-equipped Echo speakers. And it's hardly alone: Bugging our homes is Silicon Valley's next frontier." (Fowler, 2019) "Many smart-speaker owners don't realize it, but Amazon keeps a copy of everything Alexa records after it hears its name. Apple's Siri, and until recently Google's Assistant, by default also keep recordings to help train their artificial intelligences." (Fowler, 2019) Fowler really hits the target point blank: "For as much as we fret about snooping apps on our computers and phones, our homes are where the rubber really hits the road for privacy. It's easy to rationalize away concerns by thinking a single smart speaker or appliance couldn't know enough to matter. *But across the increasingly connected home, there's a brazen data grab going on, and there are few regulations, watchdogs, or common-sense practices to keep it in check*." (Fowler, 2019)

Author Privacy Recommendation: Disconnect and delete everything you can find associated with ASC group.

Addiction

We are addicted to our cellphones! We are addicted to cell phone market basket of technologies. Forget the standard addictions (drugs, booze, cigarettes, sex, news, TV, porn). These pale in comparison to the need to ***immediately respond*** to a text message (even when driving at 60 mph).

Here is a fun set of statistics compiled by GSAA.

Smartphone usage statistics suggest that an average person spends 2 hours and 51 minutes per day on their mobile device. What's more, 22% of us check our phones every few minutes, and 51% of users look at it a few times per hour. (Miljic, 2019) [My personal stats show a daily average of 8h 16m] [6] Some more fun:

- 71 billion people in the world own a smartphone in 2019.
- More than 5 billion people in the world own mobile devices.
- Kids get their first mobile device around the age of 12.
- 194 billion mobile phone apps were downloaded in 2019.
- 92% of Americans believe that cell phone addiction is real.
- Two-thirds of the world is now connected via mobile devices.
- Mobile owners worldwide will increase to 7.33 billion by 2023.
- An average smartphone user has 63 interactions on her phones a day.

Have you ever tried counting the number of times you check your phone during the day? According to recent findings, an average person casually checks his/her phone about 63 times a day. Even 87% of us do it one hour before going to bed, while 69% check smartphones within the first five minutes of waking up.

Further, smartphone usage stats say that 86% of people constantly check their phones while talking to friends, which can be pretty annoying if you are the other person in the conversation. (Miljic, 2019)

5+ hours of smartphone usage a day increases the chances of obesity. Recent health studies have revealed an alarming number of obese people in the world. The risk of obesity has increased by 43%, and much is to blame on the modern and unhealthy lifestyle many people are leading. (Miljic, 2019)

Cellphone usage statistics coincide with this trend, and many doctors suggest that the prime cause for obesity are computers and handheld devices. Some doctors go as far as to say that cell phones and their overuse are the prime cause for some people getting overweight. (Miljic, 2019)

Increasing smartphone usage can *diminish our ability to interpret information.* A recently published study revealed a fascinating insight into smartphone use. The study included two controlled experiments that were based on current smartphone usage trends. It shockingly revealed that using smartphones too much diminishes our ability to understand the deeper meaning of the information that we get. (Miljic, 2019) You need more proof than the attention the public has on taking selfies and videotaping everything from bugs to riots to ? Do you think people really care about the subject or is it some deep down loss of connection which we had before the cellphone explosion? I have seen an employee fired with just a text or a date dumped on Valentines Day with a brief email. What does that tell you about the level of rudeness that we are experiencing in society today? (Nichols R. , Heinleins-symptoms-decaying-dying-culture, 2016)

Some clever people are designing algorithms to maximize engagement by ad clicks. This is an awful metric for society. Casino's use analytics to determine exactly how to get gamblers back to the gaming tables after losses – so they can lose more. Social media and gaming companies do the same thing on a massive scale, to make their platforms as "sticky" – i.e., as addictive – as possible. (Elliott, 2019) More engaging does not mean better. Hate is a virus, and we are spreading it more efficiently than ever before thanks to modern algorithm targeting. (Elliott, 2019) Fake news is engaging, interesting, but it is a lie and those that spread it or create it have no Honor. (Nichols R. , A Case for Honor, 2017) Speaking of fake news, lets look briefly at Deep Fake technology.

AI Cloining (Deep Fakes)

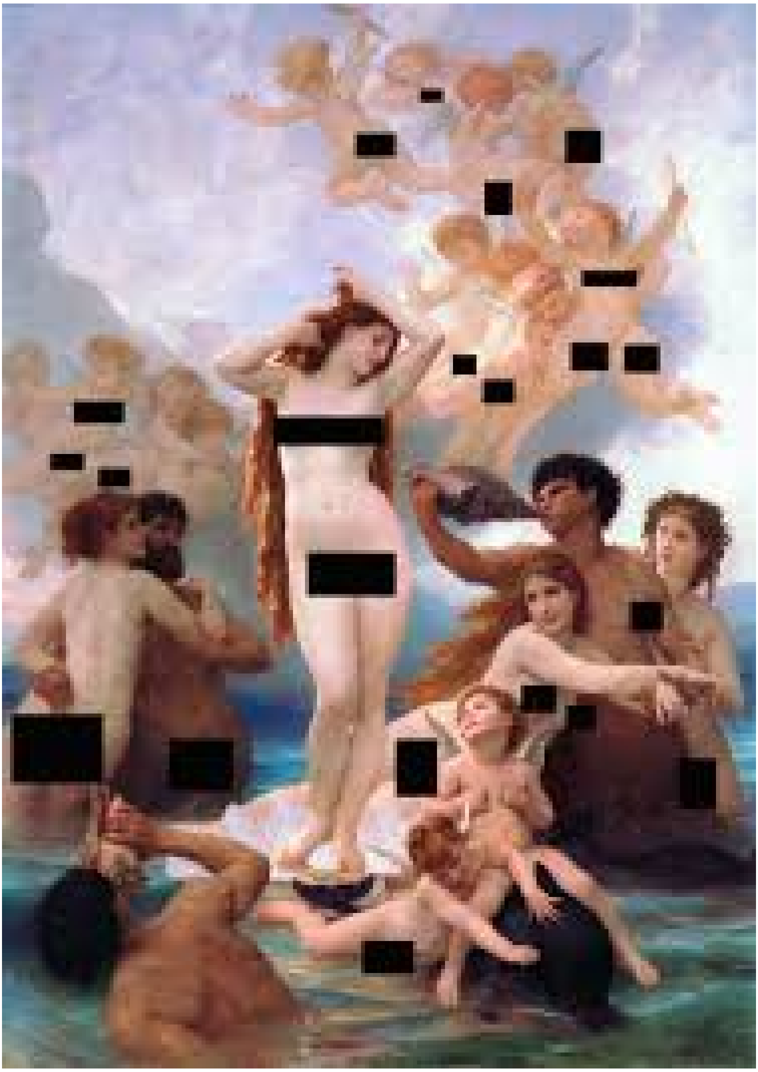
All that is needed to clone a person's voice is AI and a snippet of audio. Similarly, AI can take several photos or videos of a person and then create an entirely new – cloned video that appears to be original but with a very different message. AI can create an artificial YOU. The results are so convincing our brains have trouble differentiating between what is real and what is cloned. (Marr, 2019)

Deep fake technology uses facial mapping, machine learning, and AI to create representations of real people doing and saying things they never did. Celebrities are not the only targets; ordinary people are too. The technology is so advanced that it does not require much raw data to create a convincing fake video, plus there are a lot more images and videos of ordinary people from the internet and social media channels to use. (Elliott, 2019) An example is Facebook (FB) which people use extensively to swap images or post publicly things that 99% percent of us don't care a cent about. FB owns all those images!

De-Censoring Images

There is an interesting analog to deep fake technology called de-censoring images. The technology is not perfected but is making great strides via AI. A censored photo is an image with certain parts of it painted over or pixelated. Like this:

Figure 8.1 Censored Image The Birth of Venus by Sandro Botticelli, 1480 Source: (Birth of Venus, 2021) (InPlant, 2021)



It seems surprising that anyone would want to censor the extraordinary skill of Botticelli. Can this somehow be fixed? Is there a way to uncensor such an image and get its censored parts back?

To answer this question, let's go into what a censored image is. A photo can be censored in multiple ways of which the most popular are two: *painting over and pixelating*. Censorship of the first type is a black (or any other color) box painted over some part of the image, possibly with a "censored" mark on it. The second censoring method takes the area of the photo to censor and artificially lowers the image resolution of that area. The resulting image loses quality and becomes unreadable. Censoring is irreversible. You cannot restore original pixels of the image that are now painted over or blurred. There is a way to recover a part of original information using the surrounding (uncensored) pixels using Inpaint.© There are three steps: 1) Load the image into implant; 2) Mark the censored area using the marker tool; and 3) Run the retouching process. Inpaint lets you retouch the censored area and hide it from the picture by extrapolating surrounding pixels to the censored part of the image. Inpaint© will try to recover information from the surrounding pixels and makes the whole image look like it is not censored. (InPlant, 2021)

Can I uncensor a face or a bikini?

No, not yet. The censored image simply does not contain information about face or body features anymore. After all, that's the point of censorship, is it? Inpaint can only restore the censored part of the image by analyzing its other parts and applying them as a patch to the censored zone. As long as your photo does not contain another copy of the same face, there is nothing you can do here. However, Inpaint© can remove censored boxes from logotypes, labels, vehicle number plates and such. It can recover non-essential parts of the photo that was censored, like smoking cigarettes or any other small objects, censored territories on satellite photos and such. (InPlant, 2021)

Weaponized Algorithmic Addiction (Social Asymmetric Warfare) and Asymmetric Warfare

On Asymmetric Thinking / Warfare / Fear (Nichols R. , 2017)

Before we jump into *social asymmetric warfare (aka Weaponized Algorithmic Addiction*), let's review some important concepts: terrorism, asymmetric thinking / warfare, and fear.

Terrorism

Terrorism is violence or threatened violence against innocent people or symbols to change behavior by producing fear. Our foes of the future, will by necessity, engage in asymmetric warfare – the strategy, tactics, and tools a weaker adversary uses to offset the superiority of a foe by attacking the stronger forces vulnerabilities, using both direct and *indirect approaches* to hamper vital functions or locations to exploit advantage.

The author sees this as a struggle of intangibles constituting will: **fear, morale, surprise**. We will see both the kinetic (symmetric) elements (bullets, bombs and attrition) and non-kinetic elements (asymmetric) – such **as *perception management*, *deception*, *knowledge exploitation***, and cyberspace assault. The war against terrorism is a struggle for survival for a way of life and conflicting cultural and religious perspectives.

Our asymmetric foes of the future hope to recreate the massive second-and third- order effects that struck our country's social, political, economic, financial, military, and information systems on 11 September 2001. Asymmetric warfare and hence thinking, involves intangibles- achieving offsets through surprise, shock effects, and the ability to influence information ICGs[7] to create aggregate effects in command-and- control systems, the decision making of leaders, the will of the public to support them. (Nichols R. , 2017)

Knowledge War and Fear

Two areas where everybody can help defeat terrorism are: Knowledge war and recognizing Fear for what it is. Knowledge war deals with how people use information and knowledge in the intellectual sense – it's about superior thinking, planning and decision making under uncertainty.

One of the most important implications for people involved in knowledge war lies in the absolute requirement for expending resources to find and identify the intricacies of the opponent's decision-making processes. The concept of information center of gravity (ICG) has emerged. ICG is confluence of streams of communication, collection, automation, thinking, planning, and decision-making. Whether found in physical or virtual space, it is so important that its demise or manipulation can seriously jeopardize the success of a mission or task.

Aggregation

Asymmetric thinking involves aggregation. A great force comes from the power of aggregation. When we find relationships, then combine and exploit them, we are aggregating for advantage. A certain degree of synergy (the whole greater than the sum of the parts) comes from aggregating and connecting things, activities, actions, networks, and societal values. When things are connected in tightly woven relationships, they move together. However, the slightest perturbation or variance in one critical element can cause dramatic changes to whole (dominoes falling). This also explains the incredible power in the second-and third order cascading effects we witnessed after 11 September 2001.

Our most recent example of aggregation was on 6 January 2021, when the capital was stormed and Congress was breached by protestors. They were allegedly unhappy about President Trump's loss of his presidency and VP Pence not standing up to decertifying the results of the electoral college. They wanted an an audit of states laws, practices, and alleged allegations from 1000's of deposed witnesses in 6 key states. Witnesses claimed they were involved with / or witnessed fraudulent ballot counting or practices, and allegedly questionable results from Dominion machines.

Coping with Asymmetric Warfare

Asymmetric warfare represents the most significant challenge to this country in our entire history. How do we cope? First, we must change the way we think, plan and view the world. Second, people involved with security have to accept the concept of possibilities (potentialities not bound by constraints and avoid falling into the well-camouflaged trap of following the past and concentrating on capabilities (potentialities bound by constraints) and intent. Third, we must avoid mirror imaging our self on the world. This is a fatal flaw in our national character. Fourth, planners must consider the perceptions of the public, because asymmetric foes will target them as soft and vulnerable. The next big attack is on the National Will. The opponent's perception is more important than ours in this concept. Fifth, asymmetric assaults should be anticipated from any quarter, any time, and any place. Sixth, a learning, adaptive threat could very well know and understand our systems, process, and psyches almost as well as we do. Knowledge is available to all people and this must force improved decision-making and anticipation on our security people. (Nichols R. , 2017)

FEAR

The second factor is Fear. In teaching my self-defense and rape defense courses, I ask participants to experience meeting their Fears head-on. We all have them. Many of them irrational and many are real. Note, I did not say understand Fear. (In life, understanding is the door prize, whereas experiencing something is truth and self-actualizing.) Let me give you a new definition for Fear. Fear is False Evidence Appearing Real. Fear can be reduced / controlled / used to our own advantage / energizing and channeled into effective action through training and practice of skills.

In life, with or without terrorism, we have **One Encounter- One**

Chance to make the correct decisions to protect ourselves. There is no going back. We embrace our fears, we improve our skills, we challenge our knowledge assumptions, we create new choices, we think asymmetrically (potentialities not bound by constraints), better, faster, more holistically, making more effective decisions. (Nichols R. K., ONE ENCOUNTER – ONE CHANCE, 2018)

Weaponized Algorithmic Addiction (aka Asymmetric Social Warfare)

In traditional fighting, smaller armies using guerrilla tactics win much more often than would be expected. Now we are seeing *asymmetric social warfare*, where small groups with an agenda can destabilize society. Large companies like Facebook,© Google, © and Twitter© who all have public, on-camera, clear biases can leverage the potential deliterious effects of these small groups with an agenda by setting their business algorithms to support their attacks (aggregation). There are two very decent examples of this weaponization COVID-19 and social media reaction to POTUS after 6 January 2021 Congress breach. (Both these are discussed in detail.)

COVID-19

COVID-19 (and variants) has viciously struck the world. So many have died. COVID -19 does not discriminate on the basis of color, race, origin, sex, time, curfews, laws, business type, or age. It doesn't give a damn. It just kills. Evidence of the terrible numbers and losses are out there, all you have to do is let the information in. [8] Scientists all over the globe have been developing a vaccine to counter COVID-19. At least two companies, Pfizer and Moderna in the US have reached the goal posts and are distributing their life-saving vaccines in two inoculation packages. They are ~95% effective! It is no secret that the US government under President Trump's urging / direction sped up the normally long-time federal approval process and contracted for millions of doses to be distributed to the American populace. It is also no secret that

Democrats as a group are not fans of the outgoing president. Extremists in their party have publicly derided the effort and fostered FEAR about the vaccine as ineffective (all scientific evidence to the contrary). Many have called for Not taking the vaccine even though it represents a life-saving measure available to 100,000's citizens / non-citizens – especially seniors.

Americans have a relatively low understanding of disease and vaccines, in general. Many respondents a consumer survey[9] were unable to name the leading COVID-19-vaccine manufacturers and had limited knowledge of the vaccine candidates' key attributes. There are multiple reasons for this reality including the emergence of social media as a major source of information and the well-documented growth of the "antivaccination" or "ANTIVAX" movement. A recent in-depth analysis of online narratives about vaccines on social media by the organization First Draft found that the majority of social media discussions about COVID-19 focus on "political and economic motives" of actors and institutions involved in vaccine development and the "safety, efficacy, and necessity" concerns around vaccines. (Conway, 2020)

Regardless of which vaccines emerge, it is reasonable to assume that significant amounts of incorrect or misleading information will be spread. This is especially problematic given that, based on a recent survey, more consumers source their COVID-19-vaccination information from social media (27 percent) than from physicians (16 percent) or from state-, local-, and federal-government officials (22 to 24 percent). (Conway, 2020)

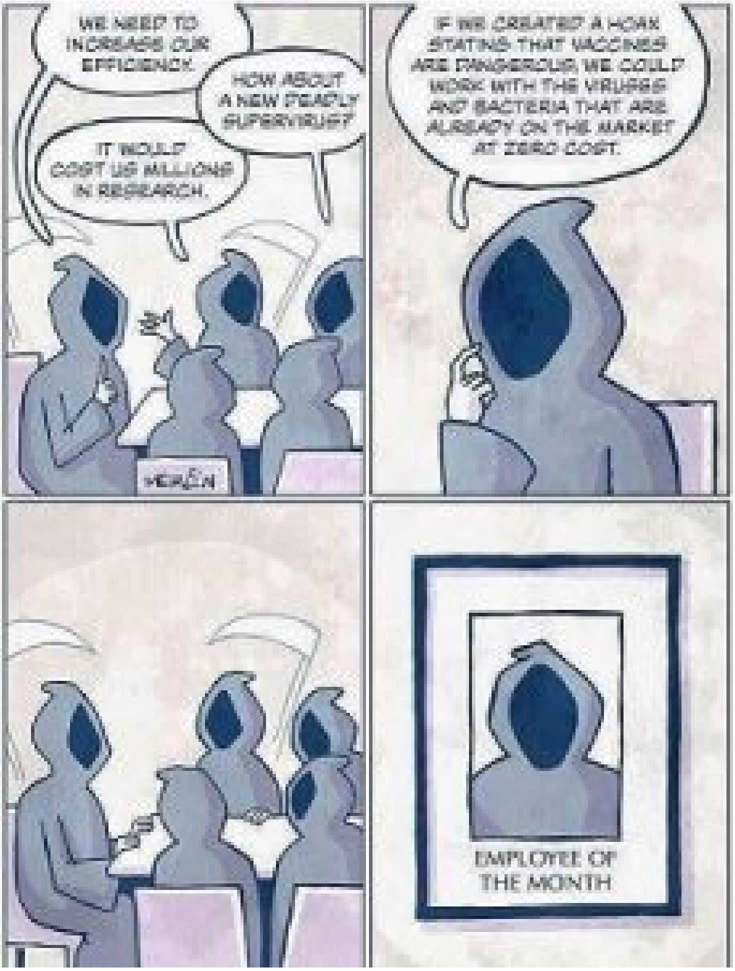
According to a recent US-consumer research, 63 percent of respondents are cautious about or unlikely to adopt COVID-19 vaccination. The "cautious," who comprise 45 percent of respondents (the largest segment), are those who will wait and see how a vaccine performs in the "real world" before deciding if they will get vaccinated. Another 18 percent say they are unlikely to vaccinate. The relative proportion of consumers in the “interested,” “cautious,” and “unlikely” segments has remained largely consistent in the past five months, with some slight positive shifts in subsegments of the “cautious”, even following positive readouts from the clinical trials of the Moderna and Pfizer–BioNTech vaccines. (Conway, 2020)

At-risk Americans are also uncertain. Despite the well-documented risks that elderly people face when contracting COVID-19, only 65 percent of respondents older than 65 years reported that they are interested in getting vaccinated. Only 31 percent of black respondents and 36 percent of Hispanic respondents said that they are interested. Other recent surveys show similar results. While 60 percent of those earning more than $100,000 per year report that they are interested in getting vaccinated, only 31 percent of those who earn less than $25,000 report the same. These findings are consistent with observed, historical behavior among higher-risk segments with respect to other vaccines. (Conway, 2020)

Consumer sentiment does not always predict actual behaviors, of course. First, sentiment can and does evolve. Second, there has always been a gap between what people say they will do about public health and what they actually do. That said, the research suggests that about 30 to 50 percent of people are interested in getting vaccinated against COVID-19, and the other 50 to 70 percent are uncertain or unlikely. That means that among the 195 million Americans who would likely need to be vaccinated to reach herd immunity in the population, about 100 million to 150 million would need to be engaged further to decide and take action to get vaccinated. (Conway, 2020)

Another look at the COVID-19 through the eyes of a destabilizing social agenda is superbly illustrated in the cartoon (Figure 8.2) below on the ANTIVAX movement by Dragoes de Garagem.

Figure 8.2 Antivax Movement by Dragoes de Garagem (Elliott, 2019)


WE NEED TO INCREASE OUR EFFICIENCY.
HOW ABOUT A NEW DEADLY SUPERVIRUS?
IT WOULD COST US MILLIONS IN RESEARCH.
IF WE CREATED A HOAX STATING THAT VACCINES ARE DANGEROUS, WE COULD WORK WITH THE VIRUSES AND BACTERIA THAT ARE ALREADY ON THE MARKET AT ZERO COST.
EMPLOYEE OF THE MONTH

Twitter© & Facebook© Actions

The headline read *Twitter, Facebook (permanently)*[10] *block Trump from posting amid Capitol violence.* In an unprecedented step, Facebook and Twitter suspended U.S. President Donald Trump from posting to their platforms Wednesday following the storming of the Capitol by his supporters. (Hindi Staff Editor, 2021)

Twitter locked Mr. Trump out of his account for 12 hours and said that future violations by Mr. Trump could result in a permanent suspension. The company required the removal of three of Mr. Trump's tweets, including a short video in which he urged those supporters to "go home" while also repeating falsehoods about the integrity of the presidential election. Mr. Trump's account deleted those posts; had they remained; Twitter had threatened to extend his suspension. (Hindi Staff Editor, 2021) Facebook followed up in the evening, announcing that Mr. Trump wouldn't be able to post for 24 hours following two violations of its policies.

While some cheered the platforms' actions, experts noted that the companies' actions follow years of hemming and hawing on Mr. Trump and his supporters spreading dangerous misinformation and encouraging violence that have contributed to Wednesday's violence. (Hindi Staff Editor, 2021)

Forget the obvious position of the aforementioned report and clearly recognize two things: 1) two organizations have so much control that they can cut off millions of interested people (globally) from any discussion or reasoning because they are setting the agenda. They can force their opinions and bias on a huge populace. This is a disturbing technology trend. How can an organization be so arrogant as to think they know the hearts and thoughts of millions based on their *weaponized* algorithms?

Drone Swarms

The British, Chinese, Russians, Israelis, Iranians, Syrians, North Koreans, South Koreans, and United States armed forces are testing how interconnected, cooperative drones can be used in military operations. Drone Swarms represent a real threat and technologies to support their use are in major development. (Nichols R. K., et al., 2020), (Nichols R. , et al., Unmanned Aircraft Systems (UAS) in Cyber Domain: Protecting USA's Advanced Air Assets, 2nd Edition, 2019), (Nichols R. K., et al., 2020), and (Nichols R. K., 2018) all devote considerable writing effort to the operation, organization, threat, application, risks, vulnerabilities, and countermeasures required for Drone Swarms.

Inspired by a swarm of insects working together, drone swarms could revolutionize future conflicts by overwhelming enemy sensors with their numbers and unrelenting mission devotion, or to effectively cover a large area for S & R missions[11]. They can reduce lives lost or cause more to be lost.

The difference between swarms and how drones are used by the military today is that a swarm can organize itself based on the situation and through drone interactions with each other to accomplish its mission. (Marr, 2019) The reality of a swarm smart enough to coordinate (without human intervention) its own behavior is approaching. The thought of killer machines being able to "think" for themselves is fodder for nightmares and movies. (Marr, 2019) Swarm technology is being deployed in all conflicts and will be in future conflicts. (Nichols R. K., et al., 2019) (Nichols R. , et al., 2020)

IoT and ASC Devices in the Home – The spy in the home

For smart home devices to respond to queries and be as useful as possible, they need to be *listening* and *tracking information about you and your regular habits*. This is exactly what the ASC group does. When you added the Echo to your room as a radio and alarm clock (or any other smart device connected to the Internet via IoT or directly or wirelessly or Bluetooth or IR), you also allowed a spy to enter your home. All the information smart devices collect about your habits such as your viewing history on Netflix; where you live and what route you take home so Google can tell you how to avoid traffic; and what time you typically arrive home so your smart thermostat can make your family room the temperature you prefer, is stored in the cloud. Of course, this information makes your life more convenient, but there is also the potential for abuse. In theory, virtual assistant devices listen for a "wake word," before they activate, but there are instances when *it might think you* said the wake word and begin recording. Any smart device in your home, including gaming consoles and smart TVs, could be the entry point for abuse of your personal information. There are some defensive strategies such as covering up cameras, turning off devices when not needed and muting microphones, but none of them are 100% foolproof. (Marr, 2019)

Smart Electric Meters

One of the most deceptive and invasive devices is the smart electricity meter. Modern meters can track not only when you're not home, but what you're up to when you're there. When you are home, it can determine how many times you flush your toilet. [12] (Nichols R. K., Invited Speaker, (19 September 2018) Lions Club, speaking on Personal Privacy: How to Defend against Invasions of It, 2018)

Consumers already face a laundry list of daily privacy issues ranging from Facebook's failure to police how user data is abused, to ISPs that routinely track your every online movement down to the millisecond.

But another, less talked about privacy problem has slowly been gaining steam: the modern, electrical utility smart meter. Modern electricity usage meters provide innumerable benefits to utility companies, including a variety of remote access and monitoring tools to better manage the power grid. They also dramatically reduce the cost of technician visits for on-location meter readings. The benefits to consumers have been less impressive, however. Some models have been found to interfere with some home routers, and, like so many *internet-connected devices*, other *variants are easily hacked*. But these devices also collect an ocean of private customer data, including detailed information that can be used to infer when you wake, when you sleep, and when you're at home or away. In the past, electricity meters delivered a lump monthly KW use figure to utilities; *but smart meters transmit data in granular detail, often in increments ranging from fifteen minutes to every few hours.* This, in turn, has sparked concern from locals in places like Naperville, Illinois, where, since 2011, one citizen group has been fighting the intrusive nature of the devices. Under the name Naperville Smart Meter Awareness, citizens sued the city over a policy mandating that all city residents must have smart meters installed by the local city-owned power utility. In their lawsuit, they argued that the city's smart meter data collection violated their Fourth Amendment rights against unreasonable searches and seizures. This week, the group notched a notable win when the Seventh Circuit Court of Appeals ruled that the *Fourth Amendment does in fact protect energy-consumption data collected by smart meters.* The ruling leans heavily on the Kyllo v. United States precedent that declared the use of thermal imaging tech to monitor citizens without a warrant also violates the Fourth Amendment. (Bode, 2018)

The court was quick to point out smart meter data collection often provides much deeper insight than could be obtained via the thermal imaging tech that was at issue in the Kyllo ruling. In large part because modern appliances often have distinct energy-consumption patterns or "load signatures" that not only tell the utility when you're home, but precisely what you're doing. (Bode, 2018)

"A refrigerator, for instance, draws power differently than a television, respirator, or indoor grow light," the ruling notes. "By comparing longitudinal energy-consumption data against a growing library of appliance load signatures, researchers can predict the appliances that are present in a home and when those appliances are used." The ruling could prove to be important for the growing number of homes that have smart meters installed. This is especially true given the growing interest among law enforcement and intelligence agencies in gaining access to this data without a warrant, and the apparent lack of interest in meaningful federal or state privacy protections for consumers. “The Seventh Circuit recognized that smart meters pose serious risks to the privacy of all of our homes, and that rotely applying analog-era case law to the digital age simply doesn’t work,” Jamie Williams, staff attorney at the Electronic Frontier Foundation, told Motherboard. “We hope that courts around the country follow the Seventh Circuit and find that the Fourth Amendment protects smart meter data,” Williams added. According to the U.S. Energy Information Association, roughly 70.8 million smart meters were already deployed by the end of 2016, with roughly 88% of them in residential homes. It’s expected that about 80% of U.S. homes will have a smart meter installed by 2020. While this ruling generally only applies to government access to this smart electricity data, Williams noted that state regulators can also play a sizeable role in preventing corporate utilities from collecting and potentially selling this data without your permission. Said data could prove invaluable to data brokers that also traffic in cellular location data. In 2011, the California Public Utilities Commission passed regulations protecting the privacy and security of consumers’ electrical usage data. In 2014, the CPUC also passed rules that let users pay a fee to opt out of such data collection. California’s Pacific Gas and Electric wasn’t a fan; and was busted for spying on activists in a bid to undermine smart meter opposition. “In order to protect consumers, other state utilities commissions, including the Illinois Commerce Commission, should pass similar regulations,” Williams recommended. (Bode, 2018)

Back in Illinois, the court warned that the entire fight could have been avoided if the city-owned utility had simply provided users with the option of using a traditional meter instead of forcing the upgrade. They also could have provided consumers the ability to opt out of data collection. “Naperville could have avoided this controversy—and may still avoid future uncertainty—by giving its residents a genuine opportunity to consent to the installation of smart meters, as many other utilities have," the court said. (Bode, 2018)

As the country debates new privacy rules in the wake of endless hacking scandals, rampant social media and broadband ISP data collection, it's important not to forget about the lowly electrical meter.

Facial Recognition

There are some useful applications for facial recognition. However, it can easily fall into sinster hands. China stands accused of using facial recognition technology for surveillance and racial profiling. They can spot Hong Kong protestors and monitor to control Uighur Muslims who live in their country. Russia's cameras scan the streets for "people of interest". Israel tracks Palestinians inside the West Bank.

What about the US?

A raging battle over controversial facial recognition software used by law enforcement and the civil rights of Americans might be heading to a courtroom. The latest salvo includes the American Civil Liberties Union suing the FBI, the Department of Justice, and the Drug Enforcement Agency for those federal agencies' records to see if there is any secret surveillance in use nationwide. The lawsuit, filed Oct. 31, 2019 comes as organizations and law enforcement are going toe-to-toe over what is private and what isn't.

A facial recognition system uses biometric software to map a person's facial features from a video or photo. The system then tries to match the information on databases to verify someone's identity. (Collins, 2019)

Police departments regularly use facial recognition to find potential crime suspects and witnesses by scanning through millions of photos; the software is also used to provide surveillance at public venues like concerts and schools and used to gain access to specific properties. But there's organized opposition against it, buoyed after California passed a law that puts a temporary ban on police across the state from using facial recognition in body cameras. The move comes while more than half of Americans polled in a recent Pew Research Center survey trust that officers would use the software responsibly. (Collins, 2019)

Apple's iPhone uses its Face ID facial recognition authentication system to help unlock the device for users, and is the subject of a $1 billion lawsuit. Social media giant Facebook uses facial recognition to recognize when members or their friends are tagged in photos. Some U.S. airports use facial recognition scanners in cooperation with the government to improve how travelers enter and exit the U.S., and some major airlines use facial recognition to help passengers check in flights, luggage, and boarding. The National Human Genome Research Institute also uses facial recognition to detect a rare disease that causes a change in appearance known as DiGeorge syndrome. (Collins, 2019)

Currently, there are no federal regulations on the use of this technology for commercial or government use as several questions emerge about whether facial recognition violates the First Amendment, granting certain freedoms including speech, religion, assembly, and the press; the Fourth Amendment, which protects people from unlawful searches and seizure; and the 14th Amendment, which guarantees equal protection of the laws. (Collins, 2019) Some companies may also use facial recognition to pitch products based on our social media profiles. This practice occurs despite the fact that many Americans despise the practice, according to the Pew Center survey; others may use the technology when it comes to people getting a loan to purchase a car or a house, and even hiring for jobs. (Collins, 2019)

While Congress has held multiple hearings about whether to ban or regulate facial recognition, law enforcement contends that the software is an invaluable tool that can quickly root out dangerous people.

According to a report from the Government Accountability Office, there are more than 640 million facial photos that are available for use that come from databases that can be searched by the Facial Analysis, Comparison, and Evaluation, also known as FACE, an internal unit of the FBI. (Collins, 2019)

In addition to tracking people without their knowledge, facial recognition is plagued by bias. When the algorithm trained to a dataset that is not diverse, it is less accurate and will missidentify people more. (Marr, 2019)

Ransomware

Ransomware is malware that is used to prevent access to a computer system to achieve criminal and malicious activities. According to CISA, It is on the rise and the ransoms cost less than just one year ago, because it is a popular scam and people pay. Scary as it is, standard encrypted backups of the user's PC's and networks to off-site and disconnected storage is a simple solution coupled with a complete wipe of the machines after infection. Or pay the $500 dollars. Generally, the hacker will give you the decrypt key. And if you think you are not vulnerable later, well there is a bridge in…. Why? When the infection has been successful, the target generally does not remove the original vulnerability. So fake emails, spear phishing, used to get private information are successful again and again and again. They have an "in" to the target. They usually leave backdoors. (Nichols R. K., Invited Speaker, (19 September 2018) Lions Club, speaking on Personal Privacy: How to Defend against Invasions of It, 2018) (Marr, 2019)

Smart Dust (MEMS)

Nichols covers the use of MEMS technology for taking down malicious UAS by Accoustic or DEW means. (Nichols R. K., et al., 2020) MEMS are Micro-Electro-Mechanical systems, the size of few grains of salt. They have sensors, communications mechanisms, autonomous power supplies, cameras and SCADA controls. (Nichols R. , et al., 2020)

Another name for MEMS is motes, or smart dust, and the technology has many postive uses. It also can be used to invade privacy practically without detection. This is an advanced technology and it is in play. (Rose, 2019)

Fake News Bots

GROVER is one AI system capable of writing a fake news article from nothing more than a headline!. The articles created such are believable. Elon Musk created the “deepfakes for text” that produces news stories and fiction so effectively, the organization initially did not release the research to the public. (Marr, 2019)

Lethal Autonomous Robots

Our last disturbing, nightmarish technology is Killer Robots (real life terminators). Currently five countries are developing autonomous robots with the intent to use them in combat. Our friendly Amazon and Microsoft have already come up with prototypes of terminator robots! (Rose, 2019) “Buy our product and we don’t break legs anymore, we have a new collector.” Can you imagine when one of these robots gets hacked? Hollywood has already developed the screen play and looking to buy the rights.

Conclusions

Technology is meant to make life simple, but it is imperative to make sure that these technologies are used only for good. This might mean regulations, new laws, restrictions on imports, quality checks, security audits, whatever. Per Neil Postman: “The effects of technology are not always unpredictable. But they are not always inevitable.” (Rose, 2019)

Questions

1) Review the list of Disturbing Technologies in the first section. Choose two that interest you. Develop the Risk profile for your choices which includes the Risks , Threats, Vulnerabilities, Impact and Countermeasures for misuse of those technologies. [13]

2) What is your prognostication about the misuse of social media? Where do you see the solutions?

3) Choose your top three Disturbing Technologies, rank them, research them, justify your arguments.

References

Birth of Venus, c. -S. (2021, January 7). *how-to-remove-censored-parts-from-photo.* Retrieved from theinpaint.com/tutorials/: https://theinpaint.com/tutorials/pc/how-to-remove-censored-parts-from-photo

Bode, K. (2018, August 24). *your-smart-electricity-meter-can-easily-spy-on-you-court-ruling-warns.* Retrieved from www.vice.com: https://www.vice.com/en/article/j5n3pb/your-smart-electricity-meter-can-easily-spy-on-you-court-ruling-warns

Burrington, I. (2015, November 19). *a-visit-to-the-nsas-data-center-in-Utah.* Retrieved from www.theatlantic.com: https://www.theatlantic.com/technology/archive/2015/11/a-visit-to-the-nsas-data-center-in-utah/416691/

Collins, T. (2019, November 19). *police-technology-and-surveillance-politics-of-facial-recognition.* Retrieved from eu.usatoday.com: https://eu.usatoday.com/story/tech/2019/11/

19/police-technology-and-surveillance-politics-of-facial-recognition/4203720002/

Conway, M. (2020, December 18). *covid-19-vaccines-meet-100-million-uncertain-americans.* Retrieved from www.mckinsey.com/industries: https://www.mckinsey.com/industries/pharmaceuticals-and-medical-products/our-insights/covid-19-vaccines-meet-100-million-uncertain-americans#

Elliott, T. (2019, June 17). 10-*interesting-disturbing-technology-trends-impacting society and business.* Retrieved from www.linkedin.com/pulse/: https://www.linkedin.com/pulse/10-interesting-disturbing-technology-trends-impacting-timo-elliott

Fowler, G. A. (2019, May 6). *Alexa-has-been-eavesdropping-you-this-whole-time.* Retrieved from www.washingtonpost.com: https://www.washingtonpost.com/technology/2019/05/06/alexa-has-been-eavesdropping-you-this-whole-time/

Hindi Staff Editor. (2021, January 7). *twitter-suspends-trump-amid-capitol-violence.* Retrieved from www.thehindu.com/news/international: https://www.thehindu.com/news/international/twitter-suspends-trump-amid-capitol-violence/article33516631.ece

InPlant. (2021, January 7). */how-to-remove-censored-parts-from-photo.* Retrieved from theinpaint.com/tutorials/: https://theinpaint.com/tutorials/pc/how-to-remove-censored-parts-from-photo

Kass, D. H. (2020, June 20). *cybersecurity-breaches-and-attacks/cia-hacker-tools-stolen.* Retrieved from www.msspalert.com/: https://www.msspalert.com/cybersecurity-breaches-and-attacks/cia-hacker-tools-stolen/

Marr, B. (2019, September 23). *The 7 Most Dangerous Technology Trends In 2020 Everyone Should Know About.* Retrieved from www.forbes.com: https://www.forbes.com/sites/bernardmarr/2019/09/23/the-7-most-dangerous-technology-trends-in-2020-everyone-should-know-about/

Miljic, M. (2019, October 7). 29+ *Smartphone Usage Statistics:*

Around the World in 2020. Retrieved from leftronic.com: https://leftronic.com/smartphone-usage-statistics/#:~:text=5.-,More%20than%205%20billion%20people%20in%20the%20world%20own%20mobile,66.5%25%20of%20the%20world's%20population.

Nichols, R. (2016, September 3). *Heinlein's-symptoms-decaying-dying-culture.* Retrieved from www.linkedin.com/pulse/: https://www.linkedin.com/pulse/heinleins-symptoms-decaying-dying-culture-randall-nichols-dtm/

Nichols, R. (2017, March 20). *A Case for Honor.* Retrieved from www.linkedin.com/pulse/: https://www.linkedin.com/pulse/case-honor-randall-nichols-dtm/

Nichols, R. (2017, February 26). *Asymmetric Thinking /Warfare/ Fear,.* Retrieved from https://www.linkedin.com/pulse/: https://www.linkedin.com/pulse/asymmetric-thinking-warfare-fear-randall-nichols-dtm/

Nichols, R. K. (1999). *ICSA Guide to Cryptography.* NYC: McGraw Hill.

Nichols, R. K. (2018, September 19). Invited Speaker, (19 September 2018) Lions Club, speaking on Personal Privacy: How to Defend against Invasions of It. Salina, Kansas : Professor Randall K . Nichols KSU.

Nichols, R. K. (2018, August 16). ONE ENCOUNTER – ONE CHANCE. Retrieved from www.linkedin.com: https://www.linkedin.com/feed/update/urn:li:activity:6435954717997744128

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

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

Domain, 2nd Edition. Manhattan, KS: NPP eBooks. 27. Retrieved from www.newprairiepress.org/ebooks/27

Nichols, R. K., Ryan, J., Mumm, H., Lonstein, W., Carter, C., Hood, J., . . . & Jackson, M. (2020). *Unmanned Vehicle Systems & Operations on Air, Sea, Land.* Manhattan, KS: New Prairie Press #35.

Nichols, R. K., Sincavage, S., Mumm, H., Lonstein, W., Carter, C., Hood, J., . . . & Shields, B. (2021). *Disruptive Technologies With Applications In Airline, Marine, Defense Industries.* Manhattan, KS: New Prairie Press, #TBA.

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

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

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

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

Rose, S. (2019, December 24). *5-horrifying-emerging-technology-trends-that-will-shake-you.* Retrieved from towardsdatascience.com: https://towardsdatascience.com/5-horrifying-emerging-technology-trends-that-will-shake-you-c7150c1f7eac

Rouse, M. (2021, January 4). *disruptive technology.* Retrieved from whatis.com: https://whatis.techtarget.com/definition/disruptive-technology

Scott, G. (2021, January 4). *Black Swan Event.* Retrieved from www.investopedia.com: https://www.investopedia.com/terms/b/blackswan.asp#:~:text=A%20black%20swan%20is%20an,they%20were%20obvious%20in%20hindsight.

Shane, N. P. (2019, May 25). *In Baltimore and Beyond, a Stolen*

N.S.A. *Tool Wreaks Havoc.* Retrieved from www.nytimes.com: https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html

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

Wiki. (2021, January 4). *Emerging_technologies definition.* Retrieved from https://en.wikipedia.org/wiki/Emerging_technologies#: https://en.wikipedia.org/wiki/Emerging_technologies#:~:text=Emerging%20technologies%20are%20technologies%20whose,background%20of%20nonexistence%20or%20obscurity.

Zegart, A. (2017, May 17). *A Stolen NSA Tool Is Being Used in a Global Cyberattack.* Retrieved from www.theatlantic.com: https://www.theatlantic.com/international/archive/2017/05/nsa-cyberattack/526644/

[1] Disclaimer: This chapter contains opinions not necessarily endorsed by the author's employer, clients, writing team or any entity quoted or cited. The author takes full responsibility for his opinions.

[2] A Black Swan is an unpredictable event that is beyond what is normally expected of a situation and has potentially severe consequences. Black swan events are characterized by their extreme rarity, severe impact, and the widespread insistence they were obvious in hindsight. (Scott, 2021)

[3] See (Nichols R. K., et al., 2020) Chapter 1 and Dr Ryan's Chapters on Information superiority in (Nichols R. K., et al., 2020), (Nichols R. , et al., Unmanned Aircraft Systems in Cyber Domain: Protecting USA's Advanced Air Assets, 2nd edition, 2019), (Nichols R. K., et al., 2019).

[4] Author added to this citation.

[5] See Contributors for a biography of this brilliant man.

[6] One of my first assignments I give in my graduate Homeland Security classes is to not allow students to use their cell phones short of an emergency for the first weekend. A prize is given for the longest time reported without the phone. In a class of 22, only 1 student went the entire weekend. He was on his honeymoon. The rest of the class average was 2 hours or less.

[7] ICG = Information Centers of Gravity. See Dr Ryan's brilliant chapter in (Nichols R. K., et al., 2020) & (Nichols R. , et al., Unmanned Aircraft Systems (UAS) in Cyber Domain: Protecting USA's Advanced Air Assets, 2nd Edition, 2019)

[8] Author interpretation / paraphrase of a Tom Selleck- Jesse Stone movie line.

[9] The Carlisle Sentinel, Carlisle, PA

[10] Two days later Twitter completely banned Trump and several of his major supporters.

[11] S & R = Search & Rescue

[12] How? Simple. Flushed water is measured in exact units of 1gpf or similar. Water comes to the toilet via a valve that is electrically controlled to determine how much hot water (sink, shower) is needed. The valve electrically opens or closes based on the need for hot water / cold water. It also measures the amount of water transferred and registered the minute amounts of electricity used to open or close the gate valve. Trace the water back to the water heater. Heat is generated by electricity to the heating coils. The measurement of how much heat is required and the flow of water through the heater to the gate valve (regardless of other cleaning or purifying systems) is measured and logged by the smart meter. This system, in turn, can and has been hacked. Now the criminal knows your behaviors: microwave, TV, bed warming blanket, telephone,

alarm system toilet, radio alarms, lights, internet, AC.. if its attached , it is measured, catalogued and discoverable.

[13] Students will recognize that this is set up for parameters of the qualitative information Risk equations- the Ryan-Nichols equations. Where Risk = Threats x Vulnerabilities X Impact / Countermeasures. And Risk ~ F(Threats / Countermeasures). The latter equation recognizes the differential state, where both Impact and Vulnerabilities are held constant with respect to time. See: (Nichols R. , et al., Unmanned Aircraft Systems (UAS) in Cyber Domain: Protecting USA's Advanced Air Assets, 2nd Edition, 2019) & (Randall K. Nichols, 2000)

9. Social Media - The Next Battlefield in Information Warfare [Lonstein]

Student Learning Objectives

This chapter will expose students to the design and deployment of information warfare throughout the annals of the history of war. We will examine concepts such as disinformation, censorship, suppression, consumption, dissemination of information, and their implementation throughout history. Next, we will introduce social media platforms as a ubiquitous form of communication. We will consider whether corporate control of the communication with no constitutional free speech protections, actions of de platforming and censorship, and their impact upon the 2020 United States Presidential election. Finally, we will consider possible methods to address the risks this new reality poses to various stakeholders ranging from individuals to governments, politicians, national security interests, and businesses.

THE HISTORY OF INFORMATION WARFARE

According to the Merriam-Webster Dictionary, the definition of "information" is "knowledge obtained from investigation, study, or instruction." Conversely, the term "disinformation" is "false information deliberately and often covertly spread (as by the planting of rumors) to influence public opinion or obscure the truth." (Merriam-Webster, 2020) While these definitions are the product of centuries of human experience with the dissemination of information from the days of cave drawings to the written, spoken, and eventually electronically transmitted, the reality is from a perspective of its use in warfare to at least the late 400's BC and the famed Military Strategist, Sun Tzu. In his treatise "The Art of War," he postulated "all warfare is deception," which is, in essence, the seminal discussion of information or disinformation usage as a warfare tool. (Tzu, 1971) Over many centuries, Chinese military treatises include and expand upon this concept. For instance, in Essentials of Sun Tzu's Art of War and Submarine Operations, a Chinese People's Liberation Army publication highlighted four information/disinformation concepts espoused by Sun Tzu

- **"Show yourself to intimidate the enemy."**
- **"Show the false to confuse the enemy."**
- **"Create momentum to harass the enemy."**
- **"Deceive to obstruct the enemy."** (Shixin, 2002) (Metcalf, 2017)

While ancient civilizations had minimal technology, written, and spoken communication was available and used just as effectively as today. Conflict was also a very significant reality in ancient China, with the conquest of adversaries a necessary and ever-present reality of any empire which sought to survive.

Figure 9.1 (Voice of America, 1957)

According to Major Nathaniel Bastian, in the 18th century, Frederick the Great created a Prussian spy's system that would gather information from travelers and conduct reconnaissance missions to determine infrastructure, weaponry, and other potential capabilities of its adversaries. He further references propaganda campaigns by Napoleon in the 1800s to publicly portray France as a victim of aggression by adversaries to craft public opinion in neighboring European countries. A few examples of this information warfare included domestic and foreign placards, articles and proclamations, and publications such as the "Bulletin de la Grande Armée" as examples of crafting public opinion, adversarial impressions of Frances military capabilities, and adversary's responses to the information. (Bastian, 2019)

In the 20th Century, World Wars I and II, as well as many other global conflicts, involved significant implementation of Information warfare whether it be an interruption of information flow via signal jamming, code-cracking, Office of War Information, Office of Strategic Services (now CIA), Voice of America and many more. (Crane, 2019).

Figure 9.2 Social Media Collage (PressureUA/iStock, 2019)

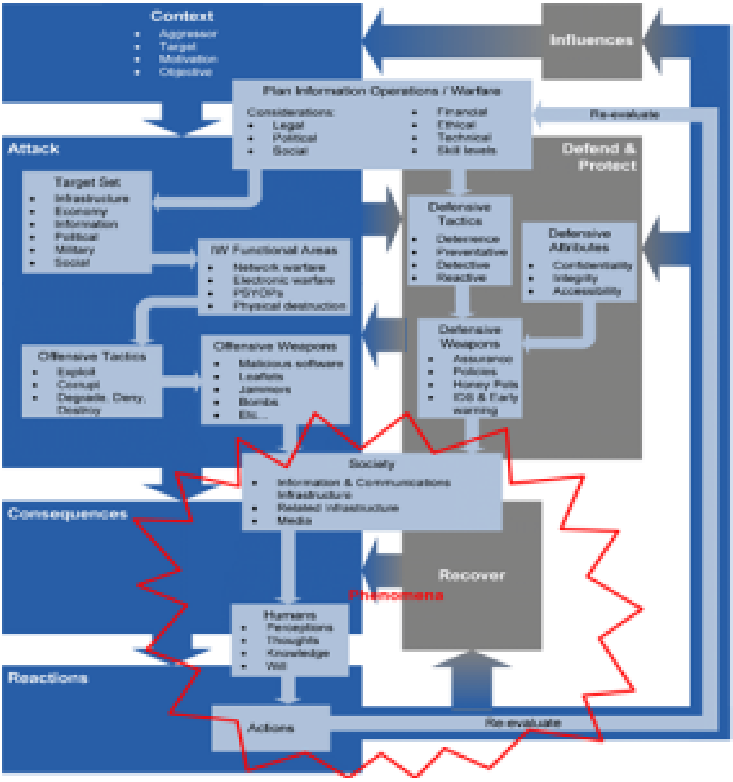
Later in the century, new technologies started to emerge, eventually leading to what is now commonly known as the internet. Names such as Compuserve, Usenet led to the introduction of GENie (General Electric Network for Information Exchange) and Listserv platforms of electronic mail lists, which started to rapidly gain popularity as the price and acceptance of connected technology led to ubiquitous acceptance. As the 1990s came and went, the first "Chatrooms" and employment sites such as the Palace, Friendster and LinkedIn were introduced and surged in popularity. By 2004 Facebook began to commercialize, quickly followed by YouTube, Twitter, and 100's of others. (McFadden, 2020) Information warfare had evolved from a prehistoric display of cave art to an instant communication method, capable of being instantly and globally disseminated on a peer-to-peer or peer-to-billions basis.

SOCIAL MEDIA TODAY -- INSTANT, PERSONAL, GLOBAL

What is Social Media? According to Merriam-Webster Dictionary, Social Media is "forms of electronic communication (such as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (such as videos)" (Merriam-Webster, 2020) For our examination Social Media is not a stand-alone concept or technology; instead, it exists as part of a class of information dissemination referred to as Information and Communications Technology ("ICT"). According to Van Niekerk, Pillay, & Maharaj, ICT is "traditional mass media, online media, including social networks, and communications technologies such as mobile telephones." (Van Niekwek, 2011)

ICT in the digital age is ubiquitous, affordable, and widely accepted. Even in the most remote and impoverished corners of the globe, the concept of connectivity via computer, smartphone, or other connected technology is a reality for most. Accordingly, the ability to control the access to, quality of, or the accuracy of the information has never been more critical when discussing Information Warfare ("IW"). In a military setting, information warfare is "a class of techniques, including collection, transport, protection, denial, disturbance, and degradation of information, by which one maintains an advantage over one's adversaries." (Burns, 1999)

Figure 9.3 "Traditional" Information Warfare Lifecycle (Van Niekwek, 2011)



Dan Kuehl of the National Defense University provided another more succinct definition, who described IW as the “conflict or struggle between two or more groups in the information environment.” (Stupples, 2015)A close examination of Figure 9.3, created in 2011, reveals it is devoid of any substantive reference to Social Media and its role in Information Warfare.

In mid-December 2010, a phenomenon known as the “Arab Spring” began in Tunisia. Essentially the “Arab Spring” consisted of an amalgam of disaffected youth, ethnic minorities, political outcasts, and academia engaging in demonstrations, protests, and ultimately revolutions. They were mainly protesting repression, censorship, lack of economic opportunity, and human rights violations in governments throughout North Africa and the Middle East. This movement was fueled in large part by leveraging the power and scope of mobile social media. The campaign almost immediately spread virally through real-time mobile phone video, tweets, hashtags, Facebook, and other social media tools. The governments of Tunisia, Egypt, Libya, and Yemen were left overthrown in its wake, with numerous others still embroiled in various unrest and even civil war stages. The speed with which the Arab Spring grew is a testament to mobile social media’s power and its ubiquitous instant access. Borders, oceans, and continents were no longer barriers to the transmission and viewing of live, first-hand accounts and media depicting the movement’s rapid growth and its efficacy in toppling governments. (Van Niekwek, 2011)

The power of mobile social media continues to be felt far beyond the Middle East and North Africa. The influence of mobile social media will be felt long after the Middle East and North Africa events. In 2015 the murders of Journalists Allison Parker and Adam Ward were streamed online shortly after they occurred (Shear, 2016). The shooting of Michael Brown in Ferguson, Missouri, the subsequent protests almost instantly rocketed social media streaming to new heights, not only as a media reporting tool but also as an organization and command and control tool for social information operated by a diverse group of sources ranging from media reporters to citizen journalists, to activists. (Solsman, 2014)

Every corner of the globe began to feel the effects of social media as a tool of information warfare. Viewers saw live violence, political upheaval, and perhaps most tragically, actual death—those who wanted to terrorize orchestrated attacks to stream their final acts of horror to millions watching online. A few examples include the Livestream of a mosque shooting in New Zealand, The Bataclan Nightclub attack in France, and The Parkland High School shooting in Florida.

Figure 9.4 Christchurch New Zealand Mosques Shooter (Tighe, 2019)

What started as an idea to allow people to interact with each other on an easy to use, instant platform with global reach seemed like a great idea when Facebook hit its stride publicly in

2006. Soon Facebook started to understand its technology's power to collect data regarding its user's preferences, behaviors, and even darker sides. As did its social media brethren, it discovered that its platforms were excellent marketing tools since they already collected massive amounts of personal data about its users. This acquired knowledge of the users, in turn, allowed the media to market products to the users based upon their profiles and custom design what news and information they see in their information feed further to embed themselves into the lives of billions globally Many believe that today's Facebook marketing and influence model reflects Edward Bernays' teachings, who is referred to as the "father of public relations." (Gunderman, 2015)

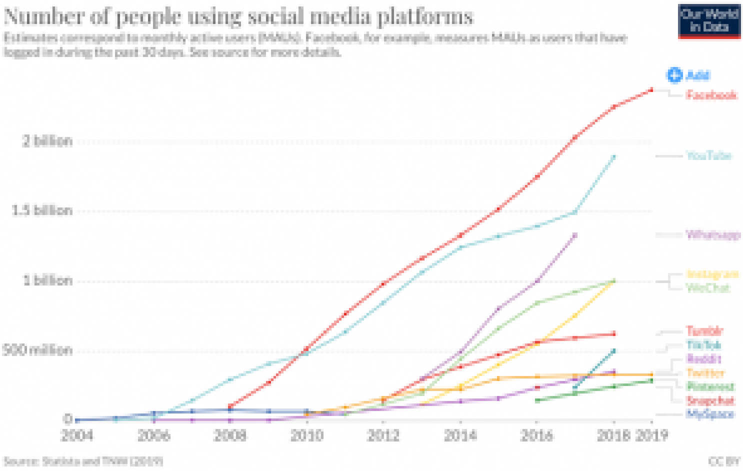
In his 1928 book "Propaganda," Benays wrote:

"The conscious and intelligent manipulation of the organized habits and opinions of the masses is an important element in democratic society. Those who manipulate this unseen mechanism of society constitute an invisible government which is the true ruling power of our country. We are governed, our minds are molded, our tastes formed, and our ideas suggested, largely by men we have never heard of.... It is they who pull the wires that control the public mind." (Bernays, 1928)

Perhaps no other technology has ever been able to mold the "habits and opinions" at the speed, scale, and individualized sophistication of social media. While other forms of communication such as print, broadcast radio, and television have undoubtedly expanded the ability to reach masses globally, no technology was ever as inexpensive, simple, ubiquitous, and always in the palm of our hands as social media.

Figure 9.5 Social Media Adoption 2004-2019

(Chaffey, 2020)

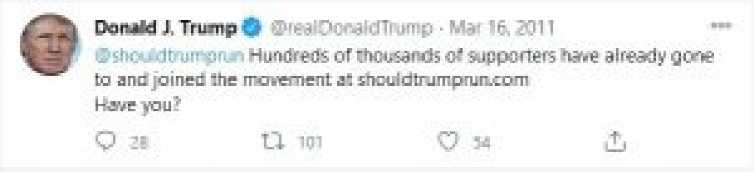


ENTER DONALD TRUMP – SOCIAL MEDIA DISRUPTOR

By 2015 it was apparent that social media was more than just a popularity contest where users could monetize pet tricks, extreme sports, memes, and other provocative content. With almost four billion users, social media represented entertainment and Donald Trump, a tool of disruption. In the final days of the Barack Obama administration, Donald Trump had become a vocal critic of its policies. While criticism of presidential administrations is nothing new, what was different about Trump was how he communicated his disagreement to the public. Previously critics or would-be presidential candidates would use television and radio appearances, write magazine or newspaper opinion pieces, or appear at events to help drive name recognition and following. Trump was different. On May 4, 2009, Donald Trump, or someone on his behalf, tweeted for the first time: "May 4, 2009, 01:54:25 PM Be sure to tune in and watch Donald Trump on Late Night with David Letterman as he presents the Top Ten List tonight!"

(Brown, 2020). In 2009, Trump was the host of his reality show “The Apprentice,” which was a huge success and was likely using Twitter and other Social Media to drive engagement and ratings. In 2011 he started to tack his use of Twitter by criticizing Obama and commenting on political issues of the day. In March of 2011, he began to discuss the prospect of entering the 2012
Presidential race. (Twitter, 2011)

Figure 9.6 Trump 2011 Election Tweet – (Courtesy Twitter @realdonaldtrump)



Donald J. Trump @realDonaldTrump · Mar 16, 2011

@shouldtrumprun Hundreds of thousands of supporters have already gone to and joined the movement at shouldtrumprun.com
Have you?

28 101 34

What followed was nothing short of amazing. Trump decided not to run in 2011 however chose to enter the fray in 2015, which eventually led to his defeat of former First Lady and Secretary of State Hillary Clinton in the 2016 United States presidential election. The fact that a political outsider could win the Presidency was not the story. In the past, candidates ranging from Andrew Jackson & Lincoln to Coolidge and Carter positioned themselves as political outsiders. However, most had some degree of governmental or political service on their resume. (WNYC, 2015) Donald Trump indeed was an outsider, a real estate and business mogul, and celebrity; he was even different than former actor Ronald Reagan who ascended to the presidency having first served as Governor of California.

While the broadcast media, who perceived him as a side-show and potential train wreck, during the Republican primary, it was only too quick to give Trump nearly unlimited press in the 2016 race.

To that end it was clear that Trump was a social media juggernaut. In a 2016 election post-mortem, Barbara Bickart, Susan Fournier and former New York Times digital, CEO Martin Nisenholtz wrote:

> "Big-seed" marketing beats viral. Duncan Watts, a principal researcher at Microsoft Research, has been studying the sociology of networks for decades. His notion of big-seed marketing suggests that a message can spread faster and more systematically if it is "seeded" among many people……….. Trump exploited Watts's theory at scale. He began with an enormous seedbed: Just before Election Day he had more than **19 million Twitter followers, 18 million Facebook fans, and nearly 5 million followers on Instagram.** The broadcast and cable networks — almost unwittingly — amplified Trump's network capabilities. Every time they reported on a tweet or posting, they effectively seeded the message among millions of viewers, many of whom, in turn, shared these messages. This offline/online complementarity helped Trump double his Twitter following during the campaign. Social and broadcast media work hand in hand, and Trump understood this better than his rivals, gaining by some estimates almost $2 billion in free air time through March 2016." (Bickart, 2017)

THE 2020 PRESIDENTIAL ELECTION: DISRUPTING THE DISRUPTOR

TAKE AWAY THE MICROPHONE

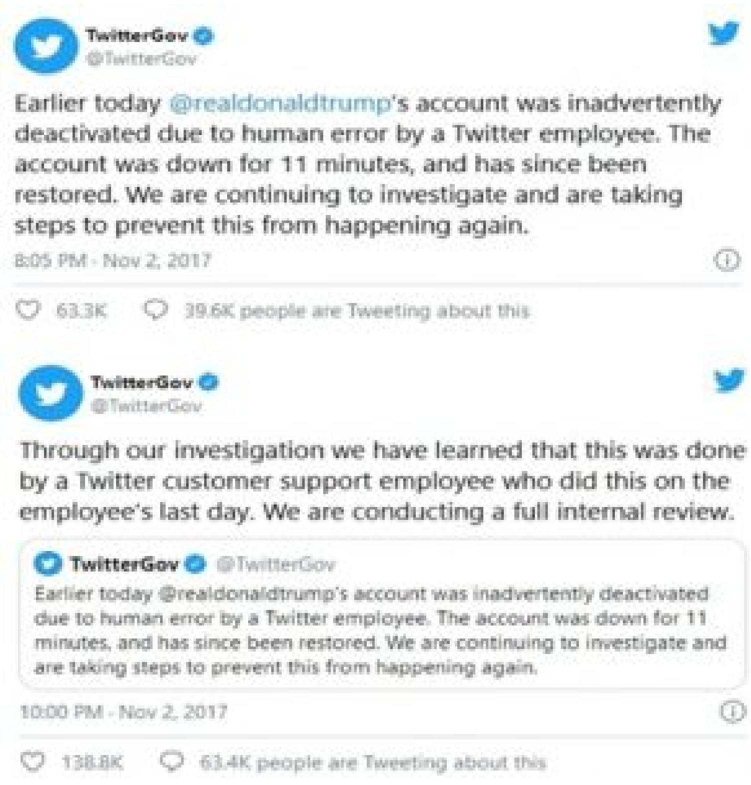
Stopping Trump from being re-elected would require non-traditional multi-faceted approach designed on the reality of how Trump totally disrupted the electoral process using social media as a primary tool to influence the coverage and behavior of traditional print and broadcast media. Before Trump is even inaugurated, the focus becomes clear, the 2020 United States Presidential Election would be less of a political campaign and more of an information warfare operation than even seen before in United States Politics.

In early November 2017, an "accident" occurred at Twitter when a technology journeyman by the name of Bahtiyar Duysak, a German citizen of Turkish descent was working on a work and study visa at Twitters Trust & Safety department received a “report” of an offensive or otherwise unpopular tweet coming from the account of one @realdonaldtrump. Duysak just happened to have formerly worked at Google and YouTube during the term of his visa and even more curiously this was to be his last day on the job at Twitter.

In an interview with Tech Crunch, shortly after the event when he returned to Germany, Duysak recalled the how the events transpired:

“His last day at Twitter was mostly uneventful, he says. There were many goodbyes, and he worked up until the last hour before his computer access was to be shut off. Near the end of his shift, the fateful alert came in. This is where Trump’s behavior intersects with Duysak’s work life. Someone reported Trump’s account on Duysak’s last day; as a final, throwaway gesture, he put the wheels in motion to deactivate it. Then he closed his computer and left the building.” (Lunden, 2017)

Figure 9.7 TwitterGov on Deactivation of @realdonaldtrump (Courtesy Twitter



TwitterGov
@TwitterGov

Earlier today @realdonaldtrump's account was inadvertently deactivated due to human error by a Twitter employee. The account was down for 11 minutes, and has since been restored. We are continuing to investigate and are taking steps to prevent this from happening again.

8:05 PM - Nov 2, 2017

63.3K 39.6K people are Tweeting about this

TwitterGov
@TwitterGov

Through our investigation we have learned that this was done by a Twitter customer support employee who did this on the employee's last day. We are conducting a full internal review.

TwitterGov @TwitterGov
Earlier today @realdonaldtrump's account was inadvertently deactivated due to human error by a Twitter employee. The account was down for 11 minutes, and has since been restored. We are continuing to investigate and are taking steps to prevent this from happening again.

10:00 PM - Nov 2, 2017

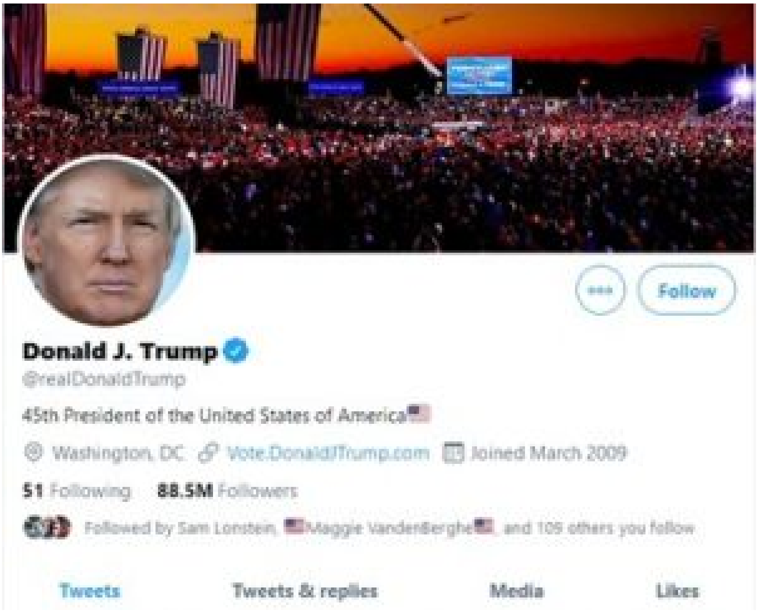
138.8K 63.4K people are Tweeting about this

The events surrounding the deactivation of the @realdonaldtrump Twitter might be a case of coincidence, even though, according to Statista, it employed almost 4000 people with additional labor coming from independent contractors and employees or vendors. (Statista, 2020) The curious circumstance where the employee happened to be leaving the company and country almost immediately may suggest a trial balloon about censoring Trumps' social media account. If "likes" are an indicator of reaction, it was undoubtedly positive since over 200,000 people liked the tweets.

CREATE A BOTTLENECK

What is clear is that Trump's supporters, opponents, and neutrals all recognized his deft implementation of social media as a tool to end-run, traditional media. Opponents became fixated on penetrating Trump's "Silicon Curtain" of individual communication with many millions of followers and foes alike.

Figure 9.8 Twitter Account @realdonaldtrump December 29, 2020



Donald J. Trump

@realDonaldTrump

45th President of the United States of America🇺🇸

Washington, DC Vote.DonaldJTrump.com Joined March 2009

51 Following 88.5M Followers

Followed by Sam Lonstein, 🇺🇸Maggie VandenBerghe🇺🇸, and 109 others you follow

By the time, the 2020 presidential election season had arrived, Trump's Twitter account had an incredible 85.5 million followers who could instantly be accessed by his tweets. In contrast, according to the Neilson Company, the average combined viewership of the major broadcast and cable news channels in

December 2020 was approximately 26.7 million viewers. (Schneider, 2020) [1]

According to George Lakoff, an emeritus professor at the University of California at Berkeley, and an expert in cognitive science and linguistics, "Trump uses social media as a weapon to control the news cycle. It works like a charm. His tweets are tactical rather than substantive," "He is as good as it gets [at using social media]," "He is not ranting, that is strategic. Even when he is ranting, it's strategic. (Buncombe, 2018)

The disruptive use of technology is nothing new when it comes to the presidency. In May of 1862, Abraham Lincoln, an apparent fan of technology, adopted widespread use of the Telegraph to message Union troops rapidly and efficiently in the field, administration officials, and to the public. In a 2012 opinion piece in the New York Times, Tom Wheeler wrote, " As he put down the message, Grant (General U.S.) laughed out loud and exclaimed to those around him, "The President has more nerve than any of his advisors." He was correct, of course, but more important than the message was the media: he held in his hands Lincoln's revolutionary tool for making sure that neither distance nor intermediaries diffused his leadership." (Wheeler, 2012) As we will see later on, technology is only useful as long as information transmission is uninterrupted.

"THE SECRET OF WAR" LIES IN THE COMMUNICATIONS"

Napoleon Bonaparte

On August 3, 2020, a group calling itself the Transition Integrity Project issued a report entitled "Preventing a Disrupted Presidential Election and Transition." The first paragraph reads:

"In June 2020, the Transition Integrity Project (TIP) convened a bipartisan group of over 100 current and former senior government and campaign leaders and other experts in a series of 2020 election crisis scenario planning exercises. The results of all four table-top exercises were alarming. We assess with a high degree of likelihood

> that November's elections will be marked by a chaotic legal and political landscape. We also assess that President Trump is likely to contest the result by both legal and extra-legal means, in an attempt to hold onto power. Recent events, including the President's own unwillingness to commit to abiding by the results of the election, the Attorney General's embrace of the President's groundless electoral fraud claims, and the unprecedented deployment of federal agents to put down leftwing protests, underscore the extreme lengths to which President Trump may be willing to go in order to stay in office." (Transition Integrity Project, 2020)

Almost immediately upon its release, the media gave the report extensive coverage. One of its authors, notably Rosa Brooks, spent the better part of late summer of 2020 discussing her fears of a Rogue Trump losing the 2020 election by a narrow margin and how he might attempt to cling to power. Although carefully crafted as a "bipartisan" group of experts, in reality, the project members and its war-game participants were either democrats, former Bush and Obama Administration officials, or, as the term goes, "Never Trump" republicans. (Gerber, 2020) Former George W. Bush Press Secretary Ari Fleisher was even more concerned about the Transition Integrity Project's dangerous narrative.

"It strikes me in the era of Trump to be one of the most irresponsible statements I've ever heard," said Fleischer, who was not part of the war games. "I'm perfectly willing, and I do so often, to criticize Donald Trump, but this is pernicious. This is beyond the call. You talk about being divisive. "He called the suggestion that Trump might not accept election results "dangerous." "Where's the evidence that this is what Trump is going to do according to his accusers? If the results are clear, the results are clear," Fleischer said. (Garrison, 2020)

In the age of social media, it has never been clearer that communication is not analogous with or necessarily intended to present facts or truth. Remember, as Bernays wrote, "We are governed, our minds are molded, our tastes formed, and our ideas suggested, largely by men we have never heard of.... It is they who pull the wires that control the public mind" (Bernays, 1928) Social Media has become the wires used in that process. It is hard to separate truth from fiction online, not to mention whether the content posted emanated from a person, a nation, an organization, or a machine. Suppose the public is unable to self-authenticate the legitimacy and credibility of the author of online content. In that case, it's undoubtedly going to be a challenge to verify the content they post as accurate or factual. A 2018 editorial on the Investor's Business Daily website distilled the issue in a fashion that leads back to the only way to determine truth and accuracy is doing it ourselves.

"As the Weekly Standard's Mark Hemingway explained: "It's basically a way for a bunch of reporters with no particular expertise to render pseudoscientific judgments on statements from public figures that are obviously argumentative or otherwise unverifiable. Then there's the matter of them weighing in with thundering certitude — pants on fire! — on complex policy debates they frequently misunderstand." In the end, the best way to judge the veracity of claims being tossed around is to become better informed about the issues, not contract out that job to people who aren't necessarily qualified to do for you." (Investors Business Daily, 2018)

According to Paul Horner, an individual who enriched himself during the 2016 presidential election, Hemingway is correct. We have identified the fake news enemy, and it is us! In an interview with the Washington Post in November 2017, Horner blamed the reader's laziness and bias for the proliferation of "fake news." Essentially he accurately believes if someone tells you are right, you are much less likely to fact check them than someone who criticized you.

"Honestly, people are definitely dumber. They just keep passing stuff around. Nobody fact-checks anything anymore — I mean, that's how Trump got elected. He just said whatever he wanted, and people believed everything, and when the things he said turned out not to be true, people didn't care because they'd already accepted it. It's real scary. I've never seen anything like it. (Dewey, 2016)

In this environment, it is easier to conduct information warfare using social media (which is now often picked up and repeated by broadcast and print media) to further a narrative throughout society rapidly and at scale. People read it, like the content, believe it, and often spread it.

MARGINALIZE THE MESSAGE – TOXIFICATION OF THE CONSUMER

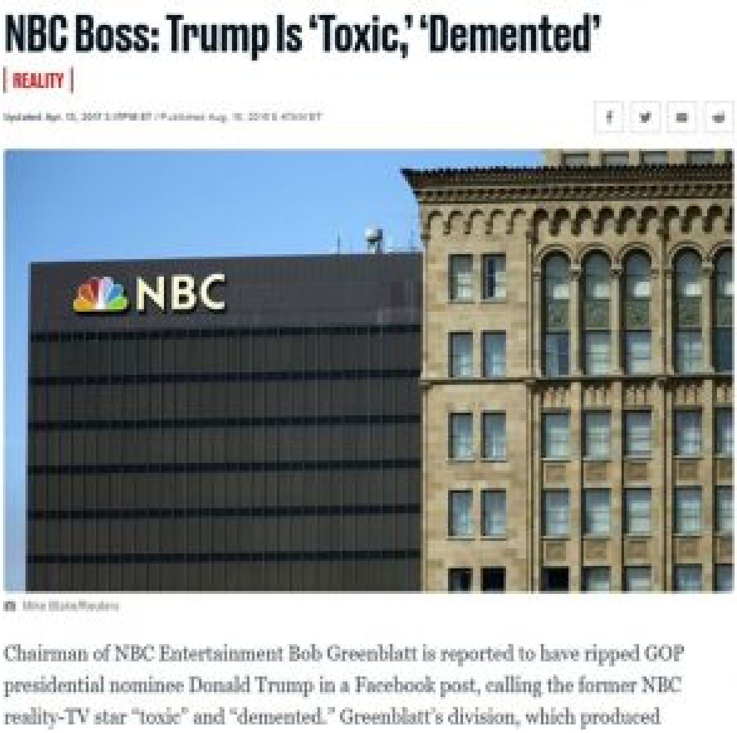
In October of 2020, the University of California, Berkeley, through its Othering & Belonging Institute, published an online book entitled "Trumpism and its Discontents," a compilation of content by various authors who drill home the same theme. The forward, written by Professor John A Powell, Director of the Othering & Belonging Institute, contained the following statement: "If the rise of Donald Trump is not grappled with critically, we will not release ourselves from the **social corrosion** we are all acutely experiencing. The work will be difficult—for many reasons, the least of which is not that it demands a look inward. We must reconsider who we are and who we think we are and think more carefully about how we have tried to answer those questions through the creation and exploitation of other beings instead of by searching for ourselves in relationship with those believed to be the "other." If we are to together forge a society in which a Trump phenomenon would not be possible, the

conversation must be contextualized on these terms." (Obasogie, Osagie K, 2020)

The marginalization can be seen in hundreds of examples of literal claims of toxicity of Trump and his followers in the media here are a few:

"NBC Boss: Trump Is Toxic, "Demented" April 13, 2017 Daily Beast (Daily Beast, 2017)

Figure 9.9 Trump Is Toxic – Demented (April 13, 2017 Courtesy Daily Beast)



NBC Boss: Trump Is 'Toxic,' 'Demented'

| REALITY |

Updated Apr. 13, 2017 3:09PM ET / Published Aug. 16, 2016 4:47AM ET

Mike Blake/Reuters

Chairman of NBC Entertainment Bob Greenblatt is reported to have ripped GOP presidential nominee Donald Trump in a Facebook post, calling the former NBC reality-TV star "toxic" and "demented." Greenblatt's division, which produced

LET THE BATTLE BEGIN

Caveat: Though this chapter mainly focuses on Twitter because they have, in the author's opinion, been the most aggressive in taking remedial action for what it deems disinformation, violence, or other content of concern to it, it does not mean that it has taken steps other social media platforms have not. Facebook, Google, and YouTube streaming services, and many others have also engaged in and been subject to both praise and criticism for censoring, warning, or otherwise protecting what they feel is a public interest when it comes to content posted on their platforms.

After a tumultuous four years of the Trump presidency, the plan was now clearly crystallizing, given the breadth of the president's popularity, and following on social media. Leverage his following through a three-step process could be successfully implemented to defeat his reelection. In 2019, Park Advisors prepared a report for the United States Department of State, entitled "Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age."

Figure 9.10- Social Media Weaponization (Courtesy Daily Times.PK)

Although the report's focus was on the use of social media disinformation by Foreign States or their proxies, in reality, it laid out the roadmap of how to use the popularity of social media against one of its biggest stars to effectively silence his message.

Spreading false narratives on social media relies on three main premises:

1. **The medium – the platforms on which disinformation**

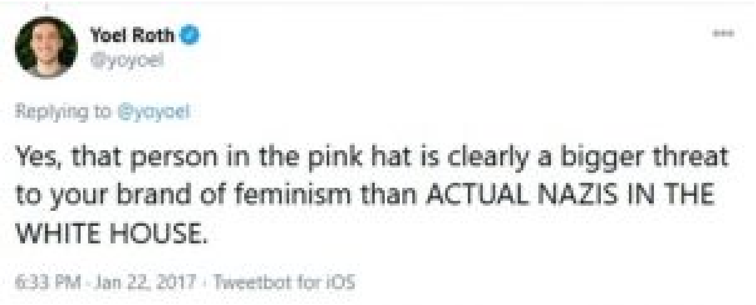
flourishes;

2. **The message – what is being conveyed through disinformation; and**

3. **The audience – the consumers of such content.** (Park Advisors, 2019)

Recall the events of November 2, 2017, when fate struck and a Twitter worker in his last hour of work gets an abuse report for a tweet from the president and disables his Twitter account for 11 minutes. Is a simulated attack replete with penetration testing? Was it even possible to judge reactions to the occurrence to predict actual long-term censorship or disabling of President Trump's Twitter account? Perhaps. Other operations directed at the Presidents access to social media were ongoing since before his inauguration in 2017. On January 22, 2017, shortly after Trumps inauguration an individual by the name of Yoel Roth Tweeted as follows:

Figure 9.11 Yoel Roth Tweet January 22, 2017 (courtesy Twitter @yoyyoel)



Yoel Roth
@yoyoel

Replying to @yoyoel

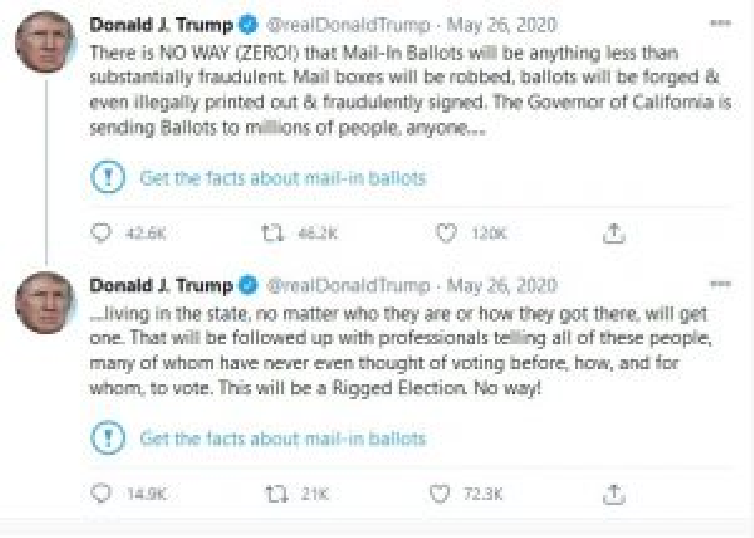
Yes, that person in the pink hat is clearly a bigger threat to your brand of feminism than ACTUAL NAZIS IN THE WHITE HOUSE.

6:33 PM · Jan 22, 2017 · Tweetbot for iOS

While accusing the President of the United States of being a Nazi is distasteful for the office, it becomes especially problematic when the person tweeting happens to be a part of the same Trust and Safety Team as Bahtiyar Duysak. They "mistakenly" deactivated the President's Twitter account in November of 2017. In fact, during the 2020 election, Roth was the Head of Site Integrity at Twitter. (LinkedIn, 2020)

In May of 2020, Twitter escalated its battle against what it called disinformation when for the first time, it placed a warning message on the President's tweet regarding the issue of fraud and mail-in election ballots.

Figure 9.12 Trump Tweet, May 26, 2020 (Courtesy Twitter @realdonaldtrump)



Donald J. Trump @realDonaldTrump · May 26, 2020

There is NO WAY (ZERO!) that Mail-In Ballots will be anything less than substantially fraudulent. Mail boxes will be robbed, ballots will be forged & even illegally printed out & fraudulently signed. The Governor of California is sending Ballots to millions of people, anyone...

Get the facts about mail-in ballots

42.6K 46.2K 120K

Donald J. Trump @realDonaldTrump · May 26, 2020

...living in the state, no matter who they are or how they got there, will get one. That will be followed up with professionals telling all of these people, many of whom have never even thought of voting before, how, and for whom, to vote. This will be a Rigged Election. No way!

Get the facts about mail-in ballots

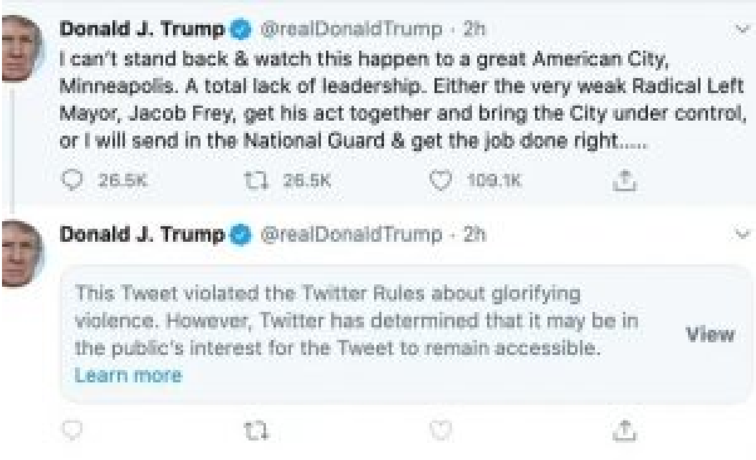
14.9K 21K 72.3K

Three days later, Twitter took a more aggressive stance when it hit a tweet from President Trump behind a warning. Twitter took this unprecedented action because it claimed:

"This tweet violates our policies regarding the glorification of violence based on the historical context of the last line, its connection to violence, and the risk it could inspire similar actions today.

"We've taken action in the interest of preventing others from being inspired to commit violent acts but have kept the tweet on Twitter because it is important that the public still be able to see the tweet given its relevance to ongoing matters of public importance." (TwitterComms, 2020)

Figure 9.13 Trump Tweet, May 29, 2020 (Courtesy Twitter @realdonaldtrump)



Donald J. Trump @realDonaldTrump · 2h

I can't stand back & watch this happen to a great American City, Minneapolis. A total lack of leadership. Either the very weak Radical Left Mayor, Jacob Frey, get his act together and bring the City under control, or I will send in the National Guard & get the job done right.....

26.5K 26.5K 109.1K

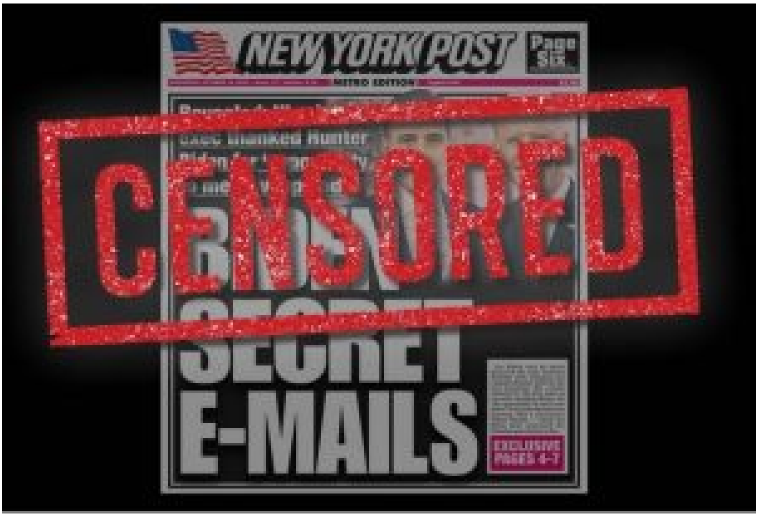
Donald J. Trump @realDonaldTrump · 2h

This Tweet violated the Twitter Rules about glorifying violence. However, Twitter has determined that it may be in the public's interest for the Tweet to remain accessible. Learn more

Perhaps the most telling salvo of the censorship war being waged by online and traditional media against the Trump campaign occurred on October 14, 2020, a mere three weeks before the Presidential election. According to the New York Post, it obtained a laptop believed to be owned by and dropped off for repair at a Delaware computer repair shop by Hunter Biden, son of then-candidate Joe Biden. Upon examining the computer, the repairmen found what he felt were critical national security emails. He sent the laptop to the FBI after being unclaimed for many months and being treated as abandoned. Not hearing back from the FBI and knowing the contents of the computer were of critical national interest to the nation in light of ties between Hunter Biden and the Ukrainian, Russian and Chinese governments and businesses, the repairmen provided a copy of the hard drive he had made to presidential attorney Rudolph Giuliani.[2]

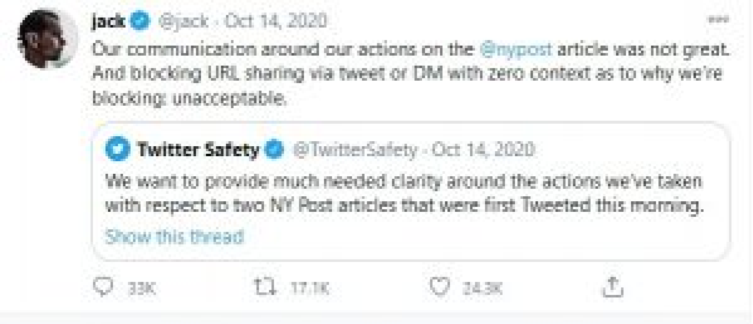
Giuliani and the Trump campaign then provided the hard drive image to the New York Post for confirmation and reporting. When the New York Post reported the story, it was big news. Almost immediately, the Posts' Twitter account was banned, and Facebook, Twitter, and YouTube restricted sharing of the story, and broadcast media largely ignored the story.

Figure 9.14 New York Post October 14, 2020 (Courtesy NY Post)



Almost immediately, the Trump campaign and many print and online media outlets protested this unprecedented act of censorship, and Jack Dorsey, Twitter's CEO, had to eat crow and admit that Twitter's "actions" surrounding the New York Post article "were not great." (Twitter, @jack Twitter, 2020)

Figure 9.16 Twitter Apology New York Post October 14, 2020 (Courtesy Twitter)



jack @jack · Oct 14, 2020

Our communication around our actions on the @nypost article was not great. And blocking URL sharing via tweet or DM with zero context as to why we're blocking: unacceptable.

Twitter Safety @TwitterSafety · Oct 14, 2020

We want to provide much needed clarity around the actions we've taken with respect to two NY Post articles that were first Tweeted this morning.

Censorship was not the only weapon in the Information Warfare campaign during election 2020. In 2020 the term "disinformation" became widely used to suggest social media or online content contained much falsehood which, relates to many claims regarding the 2016 Presidential Election. See; Russia's Pillars of Disinformation and Propaganda Report.. (United States Department of State, 2020) Case in point, in the early summer of 2020, the Biden-Harris team launched an online pressure campaign targeting Facebook claiming,

"Facebook.... It continues to allow Donald Trump to say anything — and to pay to ensure that his wild claims reach millions of voters. SuperPAC's and other dark money groups are following his example. Trump and his allies have used Facebook to spread fear and misleading information about voting, attempting to compromise the means of holding power to account: our voices and our ballot boxes." (Biden for President, 2020)

This tactic relied upon classifying the message and the messenger to drive a narrative to the masses that Trump's social media statement was, in fact, disinformation. This tactic's objective was to create an assumption that all Trump posting *was* disinformation and, therefore, untrustworthy. After the election in January 2021, citing a violent protest at the United States Capitol, both Facebook and Twitter permanently banned the social media accounts of Donald Trump. Mission accomplished. . (Twitter, 2021) (Zuckerberg, 2021)

HOW WILL LAW, POLICY AND MARKETS REACT?

As of January 1, 2021, Joseph Biden has been declared the 2020 US Presidential election winner. Unfortunately, the issues we have examined in this chapter have led many Trump supporters to believe that big technology companies, broadcast, print, and social media placed a hand on the scales of fairness. Trump and his supporters claim that electronic voting technology, mail-in ballots, and early voting created a "perfect storm" of election fraud.

They also claim sizeable financial assistance from social media companies and their executives negatively impacted his campaign in six "battleground" states where the margins of victory were very tight. To date, none of these claims have been proven in or accepted by a Court of Law. (Sheck, 2020)

Many on both sides of the aisle suggest that social media companies enjoy unwarranted protection from liability for their actions under Section 230 of the Communications Decency Act. (Cornell Law School Legal Information Institute, 2020) While reform of this law may bring some relief to those who claim injury caused by social media company activity, it certainly is under pitched debate in Congress. Still, it would fail to address social media companies outside the United States.

Others say there needs to be legislation enacted which affords individual and companies the same protections afforded them under the First Amendment to the United States Constitution. (United States Courts, 2020). By analogy, this type of oversight finds justification under the same theories which allow Public utility regulation. In 2018 Professor Anjana Susarla of Michigan State University was quoted as saying:

"It is both an open platform for free expression of diverse viewpoints and a public utility on which huge numbers of people

— and democracy itself — rely for accurate information.......... It's true that overregulation does run the risk of censorship and limiting free expression. But the dangers of too little regulation are already clear, in the toxic hate, fake news and intentionally misleading propaganda proliferating online and poisoning democracy. In my view, taking no action is no longer an option." (Susarla, 2018)

Recently a Justice Minister in Poland introduced legislation that would impose hefty fines on social media companies who wrongfully censor legal speech, (PolandIn, 2020) and Senator Mike Lee of Utah introduced the PROMISE ACT (Promoting Responsibility Over Moderation In the Social Media Environment Act). (Davidson, 2020) While each of these regulatory adjustments may hold promise, in reality, in the heat of a campaign or while running a private business, being censored by social media can be disastrous, and merely waiting for new legislation or filing lawsuits may not prevent irreparable harm.

The new reality is that social media censorship, primarily based upon opaque policies of conduct and arbitrary enforcement standards, amounts to the equivalent of a Distributed Denial of Service (DDoS) attack.

The internet company Cloudflare defines a DDoS attack as:

"A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices. From a high level, a DDoS attack is like an unexpected traffic jam clogging up the highway, preventing regular traffic from arriving at its destination." (Cloudflare, Inc., 2020)

When it comes to social media and its 4 billion users, simply censoring information or de-platforming individual posters or users can have the same effect as a DDoS attack. When conducted independently or in coordination with the most significant social media networks, it creates de facto censorship of dissenting voices.

Internet libertarian and free speech advocate John Gilmore once wrote, “The Internet interprets censorship as damage and routes around it.” In 2020 Brian Krebs, a noted cybersecurity expert, found his website taken offline when a massive DDoS attacked targeted his domain. His internet service provider informed him that the attack compromised their systems and customers, and therefore the website must remove its network. Krebs described the situation this way:

“Censorship can in fact route around the Internet.” The Internet can’t route around censorship when the censorship is all-pervasive and armed with, for all practical purposes, near-infinite reach, and capacity. I call this rather unwelcome and hostile development the “The Democratization of Censorship.”

Figure 9.15 the Democratization of Censorship (Courtesy Brian Krebs)

What Krebs described in 2016 was eerily similar to what occurred to the Trump reelection campaign in 2020. The difference was that censorship and de-platforming were at the request of an internet service provider or Content Distribution Network (CDN); it was being waged actively and passively by social, broadcast, and print media companies.

As you can see, there are many potential risks to using social media to conduct a political campaign, run a business, and conduct government operations. We now turn to countermeasures, risk mitigation, and related strategies to address this growing challenge to many people and entities maintaining an online or social media presence.

COUNTER-CENSORSHIP- SOCIAL MEDIA RESILIENCY STRATAGIES AND TECHNOLOGY

P.A.C.E., what is it and why does it matter?

PACE communications planning is a military-inspired concept designed to ensure a robust ability to effectively communicate during times when the unexpected happens so that panic, fear, and confusion do not compromise an organization's operational readiness. According to the Puget Sound Healthcare Emergency Communications Systems;

"Developing comprehensive PACE plans will not ensure perfect communications in a disaster but helps to clear some of the fog and friction found in every emergency situation. Developing comprehensive PACE plans will not ensure perfect communications in a disaster but helps to clear some of the fog and friction found in every emergency situation." (Puget Sound Healthcare Communications Systems, 2018) citing (Ryan, 2013)

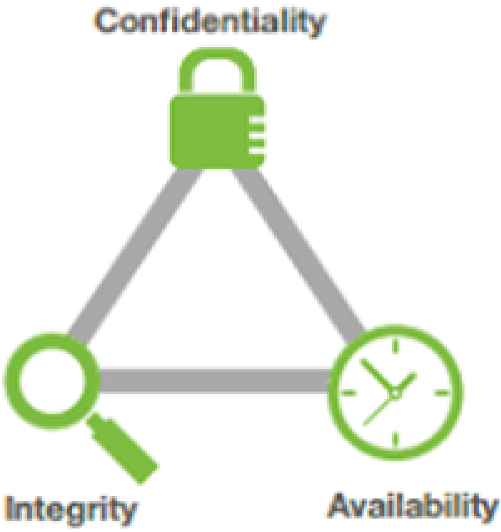
- **Primary: The main form of communication.**
- **Alternate: If the primary fails, this is your secondary form of communication**
- **Contingency: Tertiary method of communication**
- **Emergency: If all else fails, this is the worst-case option.** (Fire Watch Solutions, 2018)

The implications of a loss of communications are widely known, whether it be a military operation where command and control are lost, and aircraft are losing radio contact with ground controllers and other aircraft, or merely finding your internet service down. The first two are potentially fatal, the third a nuisance, but all three demonstrate without communication, it is challenging to function effectively in a data-driven world.

Figure 9.17 PACE Planning (Courtesy Chris Littlestone, Life is a Special Operation)

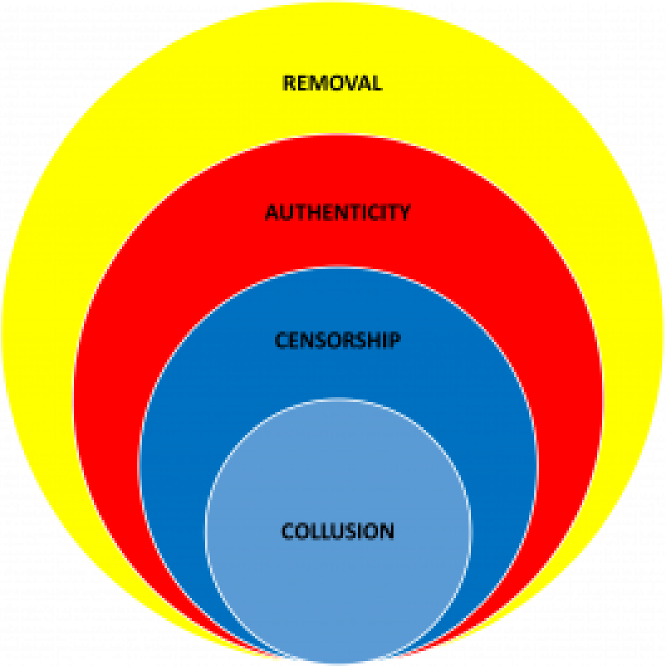
Cyberspace makes the challenge of communication protection even more difficult. To have a practical strategy, students must consider some of the lessons learned in primary information security education, particularly the CIA Triangle. The CIA Triangle, in its traditional form, has three legs, Integrity, Availability & Confidentiality.

Figure 9.18 CIA Triangle (Courtesy Infrosecuritybuzz.com)



Students will undoubtedly face challenges relating to the successes and failures of the 2020 Presidential election for years to come. As we have seen in the earlier parts of the chapter, it is relatively easy to weaponize social media in multiple ways and different combinations depending upon the objective.

Figure 9.19 Social Media RACC Threat Matrix (Courtesy VFT Solutions, Inc.)



Removal from a social media platform can have a devastatingly significant effect upon a campaign, a business, or an operation that leverages one platform far over the others. The result can be an imbalance where the removal from the platform of choice, in 2020 for President Trump it was Twitter can result in multiple hardships from merely communicating with supporters to redirect them to alternative media in time to avoid significant disruption and confusion.

Toxification is a method to make all content posted online by a source to be suspicious and assumed to be untrue. The tactic can be more effective and less noticeable to the audience than outright censorship or removal from a platform because it is very passive and operates like a subliminal message. As the Nazi Propaganda Minister Joseph Goebbels is reputed to have said;

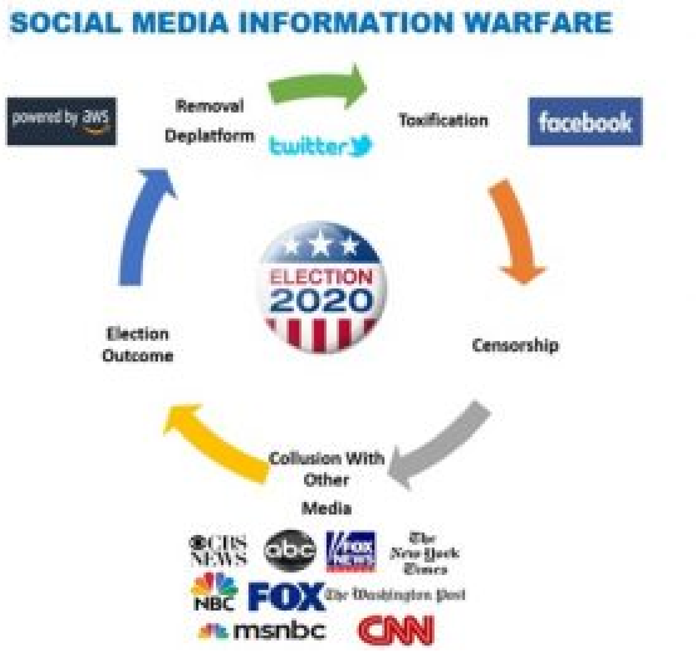
"If you tell a lie big enough and keep repeating it, people will eventually come to believe it. The lie can be maintained only for such time as the State can shield the people from the political, economic and/or military consequences of the lie. It thus becomes vitally important for the State to use all of its powers to repress dissent, for the truth is the mortal enemy of the lie, and thus by extension, the truth is the greatest enemy of the State." (Holocaust Education & Archive Research Team, 2010)

On the other hand, disinformation posted online can have equally significant value since it can create damaging narratives that are difficult if not impossible to recover. A perfect example of this would be the 2017 "Dossier," which allegedly detailed collusion between Russia and the 2016 Trump campaign. This narrative persisted through the entire first four years of the Trump presidency and though proven demonstrable false, still is used as a useful tool to fuel false narrative**s**.[5]

Censorship on social media is a complex issue. The platforms claim to be the sole judges of the content posted on their media since they are private businesses. Usually, the platform will tailor its Terms of Service to allow for them to decide what can and what cannot be posted and to change the rules without notice. As we discussed earlier, Section 230 of the Communications Decency Act, at least in the United States, allows them to do so with impunity.

Collusion, either overtly or *de facto*, has proven to be a devastatingly effective tool. When one social media platform uses its "Fact Checkers" to support content censorship, the adage strength in numbers applies. While there are many unknowns about Election 2020, for now the following Social Media Information Warfare Cycle (Figure 9.20) appears accurate.

Figure 9.20 Social Media Information Warfare Lifecycle



Suffice it to say that the challenges presented by social media are varied and will likely impact most student's careers in one way or another. There are no definitive answers; however, to help address the challenge, the following steps may serve as Best Practices to minimize, if not secure online operations from social media risks mentioned above with impunity

- Rapidly identify trending content that may be relevant to a particular stakeholder's interest. Understand that push notifications can make posts go viral in seconds, and live social media streams to go from one to over one million viewers in a minute. As Churchill once said, "There are a terrible lot of lies going about the world, and the worst of it is that half of them are true." (British Broadcasting Company, 2015)

- Develop overlapping, multiple social media accounts on as many platforms as possible. When it comes to social media live streaming, this task has become much simpler with stream casting technology. A single live or recorded stream can be simultaneously broadcast on multiple platforms, decentralizing a portion of RACC risk. Some technologies which can easily support this function include restream.io, Camera Fi, and melonapp, to name a few. See Figure 9.21.

Figure 9.21 (Courtesy restream.io)

Restream

Create Perfect Live Streams to 30+ Social Platforms

Set up high-quality live streams right in your browser and broadcast to multiple channels at once.

30+ social platforms

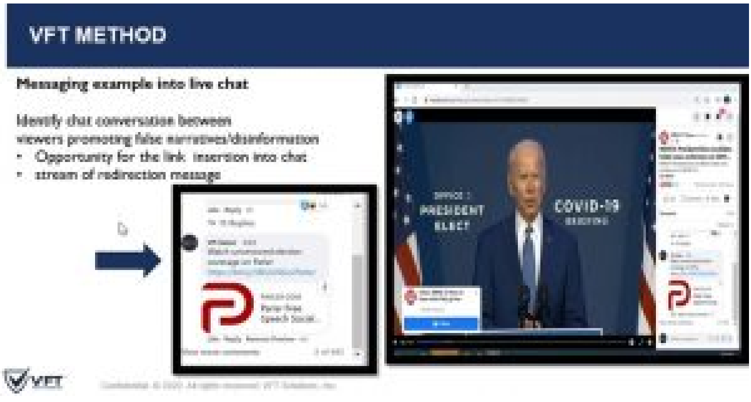
3M+ streamers worldwide

300M+ viewers engaged monthly

- Standalone mirror platform. A standalone mirror platform is simply a proprietary asset owned by the stakeholder, which has all the features of a traditional social media platform. The difference is that content is curated, controlled, and owned by the stakeholder. Inexpensive live streaming and video on demand technology are now extremely affordable and straightforward to rapidly integrate into a website. This standalone should have a URL listed in the description of all social media accounts operated by the stakeholder as well as be reachable through SMS "text to" technology (i.e., Text CENSOR to 555221)

- Employ live message insertion technology. Live message insertion technology is a patented process whereby all social media is scraped in real-time using various search and recognition technologies to identify relevant content. After that, an automated or manual message is inserted on multiple social media streams simultaneously. This process redirects viewers away from disinformation to legitimate and accurate content. And they were coupled with a reverse distribution; this countermeasure can be deployed in a remote, distributed fashion globally, override and compete with other individuals, or collective censorship attacks. See Figure 9.22.

Figure 9.22 Live Social Media Message Insertion (Courtesy VFT Solutions, Inc.)[4]



VFT METHOD

Messaging example into live chat

Identify chat conversation between viewers promoting false narratives/disinformation
- Opportunity for the link insertion into chat
- stream of redirection message

Parler Free Speech Social...
PRESIDENT ELECT
COVID-19
VFT
Confidential © 2020. All rights reserved. VFT Solutions, Inc.

CONCLUSIONS

Technology changes at a rapid pace; social media technology seems to change at the speed of light. This chapter's content exposes students to a brief overview of the scope and breadth of how social media has changed and disrupted our lives. What may true today may be outdated or incorrect one hour from now; the key is for students to understand the rapidly shifting landscape and how such shift can impact personal inconvenience or benefit to global change or conflict. Technologists, security specialists, and other professionals would do well to stay abreast of this emergent technology, currently in individual use by over one-half of the world population.

QUESTIONS TO CONSIDER

1. You are the global marketing president for Tesla Automobiles. As a popular automobile brand in the age of technology, green energy, and social awareness you learn the companies Chairman Elon Musk has made a politically unpopular statement regarding his fondness for eating foie gras. In response PETA (People for the Ethical Treatment of Animals) calls for a boycott of all Tesla products as well as a delisting and censorship of all content and advertisements on social media. What steps would you take in order to mitigate risk to your global business, respond to the story, maintain social media contact with your loyal customer base? What steps would you take to protect if other nations who were pro-duck decided to block all social media companies doing business in their nation which allowed pro foie gras content to be posted?

2. As part of your position as social media director of the local mayoral campaign, you are told to present a plan to create social media messaging to make your candidate look as if he supports gun control while painting the opponent as a supporter of full concealed carry weapons rights in public places including schools. How would you address the opponent's ten thousand social media followers? Would you post on his social media platforms? How would you fact check the information you intended to post? Would you post content that could not be 100% verified as accurate? What contingency plans would you create in case as a result of your postings, your candidate was de-platformed across social media?

References

@realdonaldtrump. (2020, May 26). *Twitter @realdonaldtrump*. Retrieved from Twitter: https://twitter.com/realDonaldTrump/status/1265255835124539392

Agrawal, G. (2019, January 19). *CIA Triad in Details… Looks Simple but Actually Complex*. Retrieved from MRCISSP: https://mrcissp.com/2019/01/09/cia-triad-in-details-looks-simple-but-actually-complex/

Bastian, M. N. (2019, Fall). Information Warfare and Its 18th and 19th Century Roots. *FALL 2019|5 THE CYBER DEFENSE REVIEW* , 31-38.

Bernays, E. (1928). *Propaganda*. Brooklyn: IG Publishing.

Bickart, B. F. (2017, March 1). *What Trump Understands About Using Social Media to Drive Attention*. Retrieved from Harvard Business Review: https://hbr.org/2017/03/what-trump-understands-about-using-social-media-to-drive-attention

British Broadcasting Company. (2015, April 9). *50 Sir Winston Churchill Quotes to Live By*. Retrieved from BBC: https://www.bbcamerica.com/blogs/50-churchill-quotes–49128

Brown, B. (2020, December 22). *Trump Twitter Archive*. Retrieved from The Trump Archive: https://www.thetrumparchive.com/?results=1

Buncombe, A. (2018 , January 17). *Donald Trump one year on: How the Twitter President changed social media and the country's top office*. Retrieved from The Independent: https://www.independent.co.uk/news/world/americas/us-politics/the-twitter-president-how-potus-changed-social-media-and-the-presidency-a8164161.html

Burns, M. (1999). *Information Warfare: What and How?* Retrieved from Carnegie Mellon School of Computer Science: https://www.cs.cmu.edu/~burnsm/InfoWarfare.html

Chaffey, D. (2020, August 3). *Global social media research summary August 2020*. Retrieved from Smart Insights: https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/

Cloudflare, Inc. (2020, December 27). *What is a DDoS Attack?* Retrieved from Cloudflare: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

Cornell Law School Legal Information Institute. (2020, December 30). *Protection for private blocking and screening of offensive material*. Retrieved from Legal Information Institute: https://www.law.cornell.edu/uscode/text/47/230

Crane, C. (2019). *A Return to Information Warfare*. Carlisle : Historical Services Division, U.S. Army Heritage and Education Center.

Daily Beast. (2017, April 13). *NBC Boss: Trump Is 'Toxic,' 'Demented'*. Retrieved from Daily Beast: https://www.thedailybeast.com/cheats/2016/08/16/nbc-boss-trump-is-toxic-pompous

Davidson, L. (2020, December 9). en. Mike Lee pushes bill to punish Facebook, Twitter if they show anti-conservative bias. *Salt Lake Tribune*.

Dewey, C. (2016, November 17). *Facebook fake-news writer: 'I think Donald Trump is in the White House because of me'*. Retrieved from The Washington Post: https://www.washingtonpost.com/news/

the-intersect/wp/2016/11/17/facebook-fake-news-writer-i-think-donald-trump-is-in-the-white-house-because-of-me/

Fire Watch Solutions. (2018, July 6). *Emergency Communications: What is a PACE Plan?* Retrieved from Medium: https://medium.com/firewatch-solutions/emergency-communications-what-is-a-pace-plan-694f14250bd2

Garrison, J. (2020, August 6). *Experts held 'war games' on the Trump vs. Biden election. Their finding? Brace for a mess.* Retrieved from USA Today: https://www.usatoday.com/story/news/politics/elections/2020/08/06/election-2020-war-games-trump-vs-biden-race-show-risk-chaos/5526553002/

Gerber, S. D. (2020, September 22). *A president has the constitutional right to contest results of election.* Retrieved from The Hill: https://thehill.com/opinion/white-house/517519-a-president-has-the-constitutional-right-to-contest-results-of-election

Gunderman, r. (2015, July 9). *The manipulation of the American mind: Edward Bernays and the birth of public relations.* Retrieved from The Conversation: https://theconversation.com/the-manipulation-of-the-american-mind-edward-bernays-and-the-birth-of-public-relations-44393

Hannigan, D. (2020, October 29). *America at Large: Golfers guilty of legitimizing Trump's toxic regime.* Retrieved from The Irish Times: https://www.irishtimes.com/sport/golf/america-at-large-golfers-guilty-of-legitimising-trump-s-toxic-regime-1.4393196

Hannigan, D. (2020, October 2020). *America at Large: Golfers guilty of legitimizing Trump's toxic regime.* Retrieved from The Irish Times: https://www.irishtimes.com/sport/golf/america-at-large-golfers-guilty-of-legitimising-trump-s-toxic-regime-1.4393196

Investors Business Daily. (2018, August 2). *Who Is Fact Checking The Fact Checkers?* . Retrieved from Ivestors Business Daily: https://www.investors.com/politics/editorials/fact-checkers-big-media/

Krebs, Brian. (2016, September 25). *The Democratization of Censorship.* Retrieved from Krebs on Security:

https://krebsonsecurity.com/2016/09/the-democratization-of-censorship/

LinkedIn. (2020, December 31). *Yoel Roth – LinkedIn*. Retrieved from LinkedIn: https://www.linkedin.com/in/yoelroth/

Littletone, C. (2020, December 30). *Life is a Special Operation*. Retrieved from YouTube Life Is A Special Operation: https://www.youtube.com/watch?v=52W-aoichfw

Lunden, I. H. (2017, November 29). *Meet the man who deactivated Trump's Twitter account*. Retrieved from Tech Crunch: https://techcrunch.com/2017/11/29/meet-the-man-who-deactivated-trumps-twitter-account/

McFadden, C. (2020, July 2). *A Chronological History of Social Media*. Retrieved from Interesting Engineering: https://interestingengineering.com/a-chronological-history-of-social-media

Merriam-Webster. (2020, December 16). *Merriam-Webster Dictionary*. Retrieved from Merriam-Webster.com: https://www.merriam-webster.com/dictionary

Metcalf, M. (2017, February). Deception Is the Chinese Way of War. *United States Naval Institute Magazine*.

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/

New York Post. (2020, October 14). *Twitter, Facebook censor Post over Hunter Biden exposé*. Retrieved from New York Post: https://nypost.com/2020/10/14/facebook-twitter-block-the-post-from-posting/

Obasogie, Osagie K. (2020). *Trumpism and its Discontents*. Berkeley: Berkeley Public Policy Press.

Park Advisors. (2019). MARCH 2019WEAPONS OF MASS DISTRACTION: *Foreign State-Sponsored Disinformation in the Digital Age*. Washington, DC: Park Advisors.

PolandIn. (2020, December 18). *Justice Minister announces online* *freedom of speech bill*. Retrieved from PolandIn: https://polandin.com/51388314/justice-minister-announces-online-freedom-of-speech-bill

PressureUA/iStock. (2019, September 19). *Social Media Apps Logotypes Printed on a Cubes stock photo*. Retrieved from iStock.com: https://www.istockphoto.com/photo/social-media-apps-logotypes-printed-on-a-cubes-gm1173494837-325964650

Puget Sound Healthcare Communications Systems. (2018, December 30). *PACE for Healthcare Emergency Communications Planning*. Retrieved from PUSHECS Council: https://pushecs.org/resources/ideas_concepts/pace/

Raza, Z. (2020, July 18). *Rhizomatic speed of Social media evolves to warfare tools*. Retrieved from Daily Times: https://dailytimes.com.pk/642477/rhizomatic-speed-of-social-media-evolves-to-warfare-tools/

Restream. (2021, January 1). *Restream*. Retrieved from Restream: https://restream.io/

Ryan, M. M. (2013, Summer). *A SHORT NOTE ON PACE PLANS*. Retrieved from Infantry Magazine: https://www.benning.army.mil/infantry/magazine/issues/2013/Jul-Sep/pdfs/Ryan.pdf

Schneider, M. (2020, December 28). *Year in Review: Most-Watched Television Networks — Ranking 2020's Winners and Losers*. Retrieved from Variety: https://variety.com/2020/tv/news/network-ratings-2020-top-channels-fox-news-cnn-msnbc-cbs-1234866801/

Shear, M. e. (2016, August 26). *Ex-Broadcaster Kills 2 on Air in Virginia Shooting; Takes Own Life*. Retrieved from New York Times: https://www.nytimes.com/2015/08/27/us/wdbj7-virginia-journalists-shot-during-live-broadcast.html

Sheck, T. H. (2020, December 8). *How Private Money From Facebook's CEO Saved The 2020 Election*. Retrieved from NPR: https://www.npr.org/2020/12/08/943242106/how-private-money-from-facebooks-ceo-saved-the-2020-election

Shixin, G. (2002). *Essentials of Sun Zu's Art of War and Submarine Operations*. Beijing: Military Science Press.

Solsman, J. S. (2014, August 26). *How Ferguson brought live streams into the mainstream.* Retrieved from CNET: https://www.cnet.com/news/how-ferguson-brought-live-streams-into-the-mainstream/

Statista. (2020, December 29). *Number of Twitter employees from 2008 to 2019.* Retrieved from Statista: https://www.statista.com/statistics/272140/employees-of-twitter/#:~:text=The%20statistic%20provides%20the%20number%20of%20employees%20of,and%20of%20a%20white%20ethnicity%20with%2043.5%20percent.

Stupples, D. (2015, November 26). The next war will be an information war, and we're not ready for it . London, United Kingdom.

Sun Tzu's The Art of War. (2020, December 29). Retrieved from https://suntzusaid.com/: https://suntzusaid.com/book/10/3/

Susarla, A. (2018, August 17). *Facebook shifting from open platform to public utility.* Retrieved from UPI: https://www.upi.com/Top_News/Voices/2018/08/17/Facebook-shifting-from-open-platform-to-public-utility/1721534507642/

Tighe, M. S. (2019, March 15). *Facebook, YouTube face ire over live streaming of Christchurch attack .* Retrieved from Business Standard: https://www.business-standard.com/article/international/facebook-youtube-face-ire-over-live-streaming-of-christchurch-attack-119031500493_1.html

Transition Integrity Project. (2020). *Preventing a Disrupted Presidential Election and Transition.* Washington, DC: Transition Integrity Project.

Twitter. (2011, March 16). *Twitter.* Retrieved from https://twitter.com/realDonaldTrump/status/48100699418005504?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E48100699418005504%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.thetrumparchive.com%2F%3Fresults%3D1

Twitter. (2017, January 22). *@yoyoel.* Retrieved from Twitter: https://twitter.com/yoyoel/status/823312771416588288

Twitter, @. (2020, October 14). *@jack Twitter*. Retrieved from Twitter: https://twitter.com/jack/status/1316528193621327876

Twitter, @. (2020, October 14). *@jack Twitter*. Retrieved from Twitter: https://twitter.com/jack/status/1316528193621327876

TwitterComms. (2020, May 29). *Twitter@twittercomms*. Retrieved from Twitter: https://twitter.com/twittercomms/status/1266267447838949378?lang=en

Tzu, S. (1971). *The Art of War. Translated by Samuel B. Griffith. New York*. New York: Oxford University Press.

United States Courts. (2020, December 29). *What Does Free Speech Mean?* Retrieved from United States Court's: https://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does

Van Niekwek, P. &. (2011). Analyzing the Role of ICTs in the Tunisian and Egyptian Unrest. *International Journal of Communication*, 1406.

VFT Solutions, Inc. (2020). *VFT Counter Social Media Censorship Strategies*. Ellenville, NY: VFT Solutions, Inc.

Voice of America. (1957, February 25). President Eisenhower Speaking at VOA. Washington, DC, USA.

Weaver, C. (2020, October 9). *'To be near Trump is toxic': Covid-19, chaos and the election*. Retrieved from Financial Times: https://www.ft.com/content/f2b6873c-b274-4f25-b319-847ea5303bf2

Wheeler, T. (2012, May 24). The First Wired President. *New York Times*.

WNYC, S. (2015). A Brief History Of The Political "Outsider" [Recorded by J. Brenneman]. New York, New York, United States of America.

[1] Citing SOURCE: NIELSEN, NPM (12/30/2019.12/06/2020, LIVE+7 AND 12/07/2020-12/22/2020, LIVE+SD VS. 12/31/2018-12/08/2019, LIVE+7 AND 12/09/2019.12/24/2019, LIVE+SD) MON-SAT 8PM-11PM/SUN 7PM-11PM, AD-SUPPORTED AND PREMIUM PAY NETWORKS. NAT GEO MUNDO BASED ON NPM-H. RANKED BY 2020 YEAR-TO-DATE.

[2] To date the author is unaware of any denial by the Biden family or campaign that the laptop at issue was in fact owned & dropped off by Hunter Biden or that any of the reported contents of its hard drive were not correct.

[3] https://apnews.com/article/7b7d698b9a660997f5e755d92b775d98 Robert Mueller's report debunks Russia dossier

[4] In the interest of full transparency, VFT Solutions is the owner of patented social media scraping and messaging technologies and patents. Author Wayne Lonstein is a principal of VFT Solutions

[5] https://apnews.com/article/7b7d698b9a660997f5e755d92b775d98 Robert Mueller's report debunks Russia dossier

10. Bioterrorism and Advanced Sensors [Sincavage & Carter]

"*History has shown us repeatedly, in terms of both human suffering and economic loss, that the costs of preparedness through vigilance are far lower than those needed to respond to unanticipated public health crises.*" ~ RL Berkelman, RT Bryan, MT Osterholm, JW LeDuc, JM Hughes

Student Learning Objectives – What Questions Will Be Answered

1) How have pathogens shaped our history and will determine our future?

2) What / why are biological weapons (BW) used by terrorists?

3) What general taxonomy of BW is used by LEO / DHS in the field?

4) What is the current bioterrorism defense for the U.S. homeland?

5) What could be the long-term implications of compromised DNA data?

6) How can nanotechnology impact the global BW threat landscape?

BIOLOGICAL TERRORIST AGENTS (BTA)

Biological terrorist agents (BTA) which are prima facia for development of biological weapons (BW) include any microorganism or toxin found in nature or derived from living organisms to produce death or disease in humans, animals, or plants. (Burke, 2017) (DrPH & Shiel, 2020). They are odorless, tasteless, and colorless if released in a biological cloud by terrorists.

All biological agents (BA) have an incubation period, which will allow the terrorist time to escape before onset of symptoms. Anthrax, plague, and other BA are readily available in biological supply houses around the world outside the US. (Burke, 2017) There are good and bad bacteria naturally present in the environment and living organisms. The bad bacteria are referred to as pathogens because they cause death to a living organism. Disease-causing microorganisms (pathogens) are classified as 6.2 infectious substances under the U.N,. / DOT hazard class system.[1] Toxins that are chemical poisons produced by microorganisms or plants are classified under the U.N. /DOT hazard class system 6.1 poisons. [See end note & reference (Evers & T.J. Glover, 2010)] There are other systems of classifications for specific audiences, ex LEO. [2]

The biological threat agent can be introduced in the environment via asymmetric war or terrorist attacks. The threat of advanced biological warfare agents will continue to present challenges to developing effective strategies for defense and countermeasures (vaccines, medicine, etc.) to combat the next level in 21st-century warfare. For those in the business of BW defense a solid reference for counterterrorism is by Burke. (Burke, 2017)

Biological Weapons – A Historical Primer

During medieval times, bodies diseased with plague were catapulted over walls protecting enemy forts and castles. Once inside, the disease would spread throughout the enclosed walls. Diseased bodies were also placed upstream from compounds, and the residents would drink the water full of deadly microorganisms. In the American Civil War confederate troops placed corpses of livestock into ponds and lakes, contaminating the water supply, which delayed the advance of Union troops. (Burke, 2017)

During World War I, Germany used biological weapons on animals to impact Romania, Spain, Norway, the United States, and Argentina (Wheelis, 1998). The German biological weapons program produced bacterial and pathogen bioweapons of Anthrax, glanders, and cholera.

France followed Germany with the development of its own bioweapons program in 1921, weaponizing the potato beetle.

In 1928, The Soviet Union had one of the most powerful bioweapons programs during the cold war. They created the next level of weapon using genetically modified agents (Tucker, 1998). The U.S.S.R. created antibiotic-resistant strains for gland, anthrax, plague, and tularemia. There are three categories of Soviet bioweapons strategic, operational, strategic-operational. The Soviets decided to develop biological weapons because their research showed them to be more efficient than toxic weapons. Biological weapons in massive amounts can create very high concentrations over a vast area. It is *believed* between 1988 and 1989; all Soviet bioweapons were destroyed on Vozrozhdeniye Island by Colonel Shcherbakov (Tucker, 1998).

Japan was the only country to use biological weapons during World War II. The Japanese program began in 1933, testing biological warfare out on women (pregnant or not) and men, ranging from any age, from their population of prisoners, handicapped, and homeless. The Japanese lab, Manchuria Detachment "Unit 731", tested many agents (ex: plague, anthrax, gonorrhea, syphilis) on prisoners of war. Prisoners were exposed aerosolized anthrax and died. Their bodies were dissected to determine the effects of anthrax. Reports indicate that as many as 3,000 prisoners might have died in BW research. It is also believed that the Japanese used BTA on Chinese soldiers and civilians in WWII. Bubonic plague, cholera, anthrax, and other diseases were released, killing tens of thousands of Chinese. (Burke, 2017) By the end of WWI, the Japanese had stockpiled 400 kilograms of anthrax to be used in specifically designed fragmentation bombs. (Burke, 2017)

From World War I, the United States began research and development of biological weapons. The official start of the U.S. biological weapons program was authorized in 1943 by President Roosevelt. During World War II, the United States had an advanced bioweapons program that included both offensive and defensive components. During that time, The United States could mass-produce pathogens such as anthrax and test spreading the bacteria in the form of a cluster bomb or anti-crop agent. Pathogens were weaponized at Fort Detrick in Maryland, then transported to the dugway proving grounds in Utah we're open-air testing of the biological weapons took place (Nuclear Threat Initiative (NTI), 2015). After World War II, the United States expanded its biological warfare research based on information learned from Japan's units 731 (Imperial Japanese Army's covert biological and chemical warfare research and development unit). However, the early U.S. BW program was created because of the anticipated German biological warfare threat rather than the Japanese. (Burke, 2017) The medical defensive BTA program in the U.S. continues today as the U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID). (Burke, 2017)

During the Korean War, the United States was accused of using bioweapons, but it was proven to the World Peace Council; the allegations were Chinese government propaganda. Accusations followed in 1962 by the Cuban government. It was believed the United States used bioweapons against poultry and tobacco industries in Cuba. Cuba could not prove the allegations. In 1969 President Nixon abolished all U.S. offensive biological weapon capabilities but retained the BTA defensive program. (watchdog -USAMRIID)

After World War II, Disarmament Discussions began to be addressed in the United Nations. This included biological and chemical weapons. In 1968 the nuclear nonproliferation treaty was put into place. This Treaty's focus was mainly on chemical weapons and did not address the core of the biological weapons race. After negotiations by the U.S. and USSR, the biological weapons convention was written in 1971. It was formally signed in 1972. At the signing event, Minister of State for Foreign and Commonwealth Affairs, David Ennals, stated, "The Biological Weapons Convention is significant as the first measure, reached since the Second World War, involving the destruction of existing weapons. Biological warfare was potentially the most frightening method of armed conflict. Today, over 40 states are parties to this Convention and have both renounced this entire class of weapons and undertaken to prevent their future development by appropriate national measures. All governments for whom this Treaty formally enters into force today should gain satisfaction from having taken a step which will reduce the possibility of biological weapons being used in some future conflict." (United Nations, 2021).

During the mid-1990's, the Aum Shinri Kyo Cult terrorist organization in Japan dispersed aerosols of anthrax and botulism throughout Tokyo on at least eight occasions. The attacks failed. John Hopkins Center for Civilian Biodefense studies found that given the right weather and wind conditions, about 110 pounds of anthrax released from an aircraft could spread nearly 12 miles downwind. The cloud would be colorless, odorless, and invisible. No warning systems would be activated until patients showed up in hospitals. (Burke, 2017) [3] During the fall of 2001, Biological terrorism struck U.S. letters postmarked Trenton, NJ, to various news organizations and political figures. The most potent of the letters went to the Senate with a highly refined dry powder consisting of 1 gram of nearly pure anthrax spores. Twenty-two people developed anthrax infections. Five Died. [4] (Burke, 2017)

First Bioterrorism Attack in the United States

The 1984, the Rajneeshee bioterror attack that impacted the Pacific Northwest of the U.S. The Rajneesh cult (Osho followers) conducted the first documented bioterror incident in the U.S. (CDC Emerging Infectious Diseases, 2003). The cult had been planned to influence the county election results by infecting residents with salmonella on election day. They first started to test their attack by contaminating salad bars at ten restaurants with S. Typhimurium (typhoid fever) on different occasions before Election Day (CDC Emerging Infectious Diseases, 2003). It came to light the cult was to blame when Osho fled the commune and voiced his concern about the leader Anand Sheela's fascist beliefs. The FBI found a bioterrorism lab containing salmonella cultures and documentation for manufacturing and using explosives and biowarfare.

Dark Winter

On June 22nd and 23rd, 2001, the Johns Hopkins Center for civil biodefense strategies collaborated with other institutional institutions in a bioterrorism exercise, Dark Winter. The event simulated pandemic smallpox, focusing on the challenge's policymakers would face if confronted with a bioterrorist attack. Dark winter was intended to bring awareness to the threat posed by biological weapons among senior national security experts (Tara O'Toole, April 2002). Dark winner simulated attacks involving smallpox on shopping malls in three different states resulting in 3000 people becoming infected (Foley, 2017). The exercise resulted in:

- 16,000 smallpox cases reported in 25 states
- 1000 people had died
- The health care system could not meet the patient load
- Ten countries reported smallpox outbreaks, and Canada and Mexico had closed their borders (Foley, 2017).
- The vaccine stockpiles for smallpox ran out with a month's wait to replenish.
- Food supplies we're running low
- Countries put travel restrictions in place the economy was

weak.

What were the lessons learned from Dark Winter? Why was a similar simulation running again in the U.S.? Remember after September 11, 2001, eyes turned to the United States and the use of biodefense. Shortly after 9/11, the United States encountered an anthrax attack against government officials (described supra). Since the tragic historical event, the FBI create a specialized branch to focus on chemical, biological radiological, nuclear, and explosives. (Figure 10.1) Later in 2006, it became the Weapons of Mass Destruction Directorate (WMDD). The branch links intelligence scientific and operational components to detect and disrupt the acquisition of WMDD against America.

Between 2014 in 2016, the lessons of dark winter *were not applied*, and the nation faced the Ebola crisis. When the outbreak began in West Africa, the world watched as it spread quickly through West African countries. 10,000 people were infected with the Ebola virus, and more than half of that number died. It became a United States national security top priority, sending troops to assist with the $400 million humanitarian effort. When the virus reached The U.S. borders, it was not met with any sort of barrier requirements. The personal protective equipment could not protect against the pathogen, causing patients to be isolated. Quick reaction by the government and the medical community The United States suffered only 11 cases, which resulted in two deaths and nine survivors. Following the Ebola crisis, the House of Representative's subcommittees examined pandemic /biological terrorist attack preparedness. U.S. presidential Directive (PPD)-39 outlined the responsibilities of five federal agencies regarding WMD exercises (Foley, 2017). The directive had assigned specific tasks to each of the five agencies. It did not provide a plan for a coordinated response to a biological attack

Also, PDD-39 was at the federal funding level and did not account for the states (Foley, 2017). From 2004 leading up to the Ebola crisis, the U.S. government spent over $78.8 billion in biodefense. When examining the expenditures further, the majority was spent on multi-hazard programs, and only 17% went towards true biodefense (Foley, 2017). Biodefense continues to struggle through the budget from year to year. For example, the 2014 budget was $47.7 million less than the 2013 budget (Foley, 2017). Since 2017 several of the programs under the Weapons of Mass Destruction Directorate (WMDD) were eliminated or reassigned to another division. The red team who conducted drills and assessments to help federal and local officials detect threats were eliminated. A part of the homeland unit that performs its exercises related to Weapons of Mass Destruction at all levels was reduced. And international cooperation division that worked with foreign counterparts and the United Nations nuclear watchdog agency was disbanded. The goal of this partnership was to stop and track the smuggling of nuclear materials. There was a cut in funding to mobile units that protected large public events by detecting biological threats.

Figure 10.1 FBI WMD Investigation (Federal Bureau of Investigation, 2021)

The U.S. is one of the largest contributors to the G8 global partnership against the spread of weapons and materials and mass destruction. This partnership with 29 other countries is critical in preventing the illegal trafficking of weapons mass destruction materials, dismantle and decommission nuclear submarines, and improve biosecurity. In 2004, the U.S. was a cosponsor for the United Nations Security Council resolution 1540. The resolution, "to prevent states from supporting non-state actors and development of weapons of mass destruction including biological weapons" (Nuclear Threat Initiative (NTI), 2015). In the United States, biological weapons programs are created, restructured, expand, and disbanded at the hands of different government administrations. In October 2019, a House Homeland Security Committee subcommittee held a hearing entitled "Defending the Homeland from Bioterrorism: Are We Prepared?" The answer was a resounding no (Rutschman, 2019).

PATHOGENS

There are several types of BTA (pathogens) used for biological weapons. Biological agents can be divided into several related groups (See Table 10.1). These include bacteria and rickettsia, viruses, and toxins. Bacterial and viral agents cause disease and can multiply and spread beyond the initial attack.[5] Toxins are poisonous substances produced by living things, some of which are extremely lethal. Toxins are not contagious. Some of the bacteria that cause disease include anthrax, plague, cholera, diphtheria, tuberculosis, typhoid fever, typhus, Legionnaire's disease, Lyme disease, and strep infections. Other bacteria produce toxins that are chemical poisons, such as botulinum. *More bacteria exist in a handful of soils or in a person's mouth than all the people who have ever lived on earth. When someone sneezes, over a million bacteria can be disseminated. Over 90% of all feces is made up of bacteria.* More bacterial cells than human cells exist in your body. From 300,000 to 1,000,000 different types of bacteria exist on Earth. The majority of common bacteria is not pathogenic nor parasitic. Some have mutated and learned to invade other cells and cause disease. Bacterial organisms have a nucleus, intracellular nonmembrane bound organelles (a specialized cellular part that resembles an organ) , and a cell wall. (Burke, 2017)

Table 10.1 Comparison of Biological Agent Characteristics
(Burke, 2017)

Disease	Likely Method of Dissemination	Infectious person to person	Infectious dose	Incubation Period	Duration of illness	Lethality
Anthrax	Spores in aerosol	No except cutaneous	8 to 10,000 spores	1 to 5 days	3-5 days usually fatal	High
Cholera	Sabotage (food & water)	Rare	>106 organisms	12 hours to 6 days	>1 week	Low when treated, high without
Plague	Aerosol	High	<100 organisms	1 to 3 days̀	1 to 6 days, usually fatal	High if not treated w/i 12 – 24 hours
Tularemia	Aerosol	No	1 to 50 organisms	1 to 10 days	>2 weeks	Moderate
Q Fever	Aerosol, sabotage (food supply)	Rare	10 organisms	14 to 26 days	Weeks	Very low
Ebola	Direct contact, aerosol	Moderate	1 to 10 plague units	4 to 16 days	Death between 7-16 days	High Zaire strain; moderate Sudan
Smallpox	Aerosol	High	Assumed low	10-12 days	4 weeks	High to moderate
VEE	Aerosol	Low	Assumed low	1 to 6 days	Days to weeks	Low
Botulinum toxin	Aerosol	No	0.001 g/ kg is LD50 [6]	Variable (hours to 24 to days)	Death in 72 hours; lasts months if not fatal	High without respiratory support

Bacteria and rickettsia are single-celled microscopic organisms that can cause disease in plants, animals, and humans.

Rickettsia are pleomorphic (varying sizes) parasitic microorganisms that live in the cells of the intestines of arthropods (invertebrates and man, such as insects, spiders, and crabs, which have segmented bodies and jointed limbs. Some are pathogenic to man, where they are known to cause the typhus group of fevers. Rickettsia are smaller than bacteria but larger than viruses. Like viruses, rickettsia are obligate (they cannot exist on their own or in any other form); they are considered intra-cellular parasites. (Burke, 2017)

Viruses are very small submicroscopic organisms, smaller than bacteria and unable to live on their own. They must invade the host cell and make use of its reproductive mechanism to multiply. Many of the biological toxins are much more toxic than any of the chemical agents classified as chemical weapons (CW). See Table 10.2 Lethality of Selected Toxins and Chemical Agents in Laboratory Mice (Burke, 2017)

Table 10.2 Lethality of Selected Toxins and Chemical Agents in Laboratory Mice (Burke, 2017)

Agent	LD50 (g/kg)	Source
Botulinum toxin	0.001	Bacterium
Shiga toxin	0.002	Bacterium
Tetanus toxin	0.002	Bacterium
Abrin	0.04	Plant (Rosa Pea)
Diphtheria toxin	0.10	Bacterium
Maitotoxin	0.10	Marine Dinoflagellate
Palytoxin	0.15	Marine soft coral
Ciguatoxin	0.40	Marine Dinoflagellate
Texilotoxin	0.60	Elapid snake
C.perfringes toxins	0.1 to 5.0	Bacterium
Batrachotoxin	2.0	Arrow-Poison frog
Ricin	3.0	Plant (Castor beans)
Alpha-Conotoxin	5.0	Cone snake
Tiapoxin	5.0	Elapid snake
Tetrodotoxin	8.0	Puffer fish
Alpha-Tityustoxin	9.0	Scorpion
Saxitoxin	10.0	Marine Dinoflagellate
	Inhalation 2.0	
VX	15.0	Chemical agent
SEB	27.0	Bacterium
Anatoxin-A	50	Blue-green algae
Microcystin	50	Blue-green Algae
Soman (SD)	64	Chemical agent
Sarin	100	Chemical agent
Aconitine	100	Plant (Monkshood)
T-2 Toxin	1200	Fungal Mycotoxin

Bacterial Agents

Bacteria are single-celled organisms that range in size and shape from cocci (spherical cells) with a diameter of 0.5-1.0 m (micrometer) to long rod-shaped organisms – bacilli – which can be from 1.5 m in size. Chains of bacilli have been known to exceed 60 m in size. Some bacteria have the ability to change into spores. In this form, the bacteria are more resistant to cold, heat, drying, chemicals, and radiation than the bacterial form. When in spore form, the bacteria are inactive, or dormant, much like seeds of a plant. When conditions are favorable, the spores germinate just like seeds. (Burke, 2017)

Bacteria has two methods by which it can cause disease in humans and animals. The first is by attacking the tissues of the host living thing. Secondly, all living organisms produce waste. Bacteria may produce a toxic or poisonous waste material that causes disease in the host. Some bacteria attack by both methods. When a terrorist selects a BTA, he wants the organism to survive under varied conditions and produce certain desired results from dissemination into the population. Genetic engineering may be used to create BTA from otherwise harmless bacteria.

Bacteria can be created to be resistant to known antibiotics, extreme weather conditions, or aerosol dissemination losses.

For a BTA to be effective, it must produce a specific effect: illness, disability, death, or damage to food chains. It must be produced in large amounts, and remain stable while manufactured, during storage, when weaponized, and during transportation. It must be easy to easy and effective to disperse and remain stable once disseminated. It should have a short reliable gestation period and should be persistent. (Burke, 2017)

Bacillus anthracis is the cause of anthrax, used by Robert Koch in 1877 to develop a theory of disease (Bruce Budowle, 2020). DNA is used to study bacteria's evolution, giving the scientist the ability to identify different strands of viruses. As of 2018, 412 strains of anthrax have been identified, allowing a scientist to understand the bacteria for cures or weaponization (Bruce Budowle, 2020). The increase in

DNA study using whole-genome sequencing of data has provided great insight into pathogens such as the plague. In 2002 two tourists visiting New York became ill with the first case of bubonic plague. Scientists were able to determine within a day the couple had been, in fact, it by bites from fleas in their backyard in New Mexico. The use of DNA leading to the progression of genotyping and analysis of a bacterial pathogen increases the chances of determining bio crimes. As with the good, there is the bad the advances in DNA study also increase the potential of an effective bioweapon.

Anthrax is a good example of a BTA. Its medical courses is instructive. There are three ways to die from anthrax. Most commonly the disease appears on the hands and forearms of people working with infected animals. Symptoms as a result of cutaneous exposure include:

- Intense itching, followed by carbuncle formation
- Formation of carbuncles (inflammation of hair follicles and surrounding tissue)
- Swelling at the location of the infection
- Scabs form over the lesions and turn black as coal[7]

The mortality rate for untreated cutaneous anthrax is 20%. Inhalation exposure symptoms are flu-like:

- Chills and mild fever
- Malaise
- Nausea and swelling of the lymph nodes
- Fatigue
- Myalgia (muscle pain)
- Dry cough
- Feeling of pressure in chest

Victims feel better (known as anthrax eclipse) but in a few days the victim will get much worse with major pulmonary involvement.

Mortality rate is nearly 100%.

Anthrax can also be ingested. Symptoms resulting from ingestion exposure to anthrax include:

- Abdominal pain
- Acute inflammation of the intestinal tract
- Nausea
- Loss of appetite
- Vomiting
- Fever
- Abdominal pain
- Vomiting of blood
- Severe diarrhea

Approximately 25-60 % of those victims will die.

All the pathogens in Tables 10.1 & 10.2 are medically described in detail in (Burke, 2017). Further properties -especially for LEO- are listed in (Evers & T.J. Glover, 2010).

Viruses / Viral Weapons

Viruses are the simplest type of microorganism and the smallest of living things. They are much smaller than bacteria and range in size from 0.02 – 1.0 m (1m = 1,000 mm). One drop of blood can contain over 6 billion viruses! [8] Every living entity is composed of cells except for viruses. They are inert until they come into contact with a living host. The infection point created from a virus occurs at the cellular level. Once the virus invades the cell, it can kill it. Common examples of viral agents include measles, mumps, meningitis, influenza, HIV -AIDS, HBV, HBC, and the common cold. (Burke, 2017)

Most likely virus candidates for terrorist agents would include

Venezuelan equine encephalitis (VEE), *smallpox, and the class called hemorrhagic fevers. The latter group includes Ebola, Marburg, arenaviridae, Lassa fever, Argentine and Bolivia, Congo-Crimean, Rift Valley, yellow fever, and dengue.* (Burke, 2017)

Viruses are infectious agents that require a host for propagation, a trait that has caused them to excel at finding new hosts (Clare E. Rowland, 2016). Whereas many of the weaponized bacteria are not as effective in transmission from person to person, viruses are the pathogens that generate pandemics (Clare E. Rowland, 2016). The CDC has classified multiple viral agents as potential weapons of mass destruction or agents for biologic terrorism (Bronze, 2002). Viruses are significant; they are quickly produced and spread (i.e., Ebola, coronaviruses, smallpox). In 2009, the U.S. government launched USAID PREDICT to search for unknown viruses that can cross from animals to humans resulting in a pandemic. The PREDICT program identified nearly 1,000 new viruses, including a new strain of Ebola; trained roughly 5,000 people worldwide to identify new diseases; worked with 31 countries, and improved or developed 60 research laboratories (Global Biodefense Staff, 2020).

In China, PREDICT detected a novel coronavirus clustering with the SARS-like coronaviruses in Rhinolophus bats from Guangdong. Further characterization of this Beta Coronavirus is underway, including sequencing of the spike protein, to determine if it has the potential to infect other hosts. USAID PREDICT in 2017 and 2018 reported on the cross-contamination of coronaviruses among bats, camels, and livestock. In 2019, USAID PREDICT had reached the end of its ten-year funding and was scheduled to be disbanded in March 2020. On November 21, 2019, Senator Angus S. King wrote Mark green, the administrator for the United States Agency for International Development, questioning the closure of PREDICT, questioning if other agencies would inherit the project's initiatives, and asked if Congress would be consulted before decisions were made regarding the reassignment of PREDICT Initiatives. On January 30, 2020, Senate representatives, including senator King wrote mark green again and wrote Homeland Security requesting updates on the coronavirus and USAID PREDICT response. April 1, 2020, the USAID PREDICT project was extended by six months. On May 7, 2020, the United States Agency for International Development announced USAID PREDICT project replacement, STOP Spillover. The $100 million replacement project was awarded to Tufts University to implement STOP Spillover with a consortium of universities worldwide. STOP Spillover is a critical next step in the evolution of USAID's work to understand and address the risks posed by zoonotic diseases that can "spillover" – or be transmitted (USAID , 2020). A member of the debunked USAID PREDICT, Kevin Olival is a disease ecologist at the EcoHealth Alliance, expressed, "…what is needed is detailed knowledge of local ecology, maps of species distributions, an understanding of people's behavioral interactions with other species and an awareness of the cultural and economic drivers of the animal trade."

Galveston National Laboratory

Galveston National Laboratory is one of the most extensive active biocontainment facilities on a U.S. academic campus. On March 23, 2013, GNL reported a vial of the GUANARITO virus missing from the secure research lab. Guanarito virus, a rat-borne pathogen that can infect humans, could potentially be weaponized as an aerosol spray causing hemorrhagic fever. Similar to Ebola, the virus causes bleeding under the skin, and internal organs were from body orifices like math eyes or ears, a 33% chance of death. The virus is typically contracted in South America, specifically Venezuela. GNL maintains there was no breach to the facilities and no indication that wrongdoing was involved. The lab believes the vial had been accidentally dropped on the floor then destroyed in the incinerator, but there is no record.

Biological Toxins / Toxic Weapons

Biological toxins are defined as any toxic substance occurring in nature produced by an animal, plants, or microbe (pathogenic bacteria) such as bacteria, fungi, flowering plants, insects, fish, reptiles, or mammals. They are classified as poisons under U.N./DOT 6.1. Unlike chemical agents such as sarin, cyanide, or mustard, toxins are not man-made. (Table 10.3)

Table 10.3 Comparison of Chemical Agents and Toxins (Burke, 2017)

Toxins	Chemical Agents
Natural Origin	Man-made
Difficult small-scale production	Large scale industrial operations
None volatile	Many volatile
Many are more toxic	Less toxic than many toxins
Not dermally active *	Dermally active
Legitimate medical use	No use other than many toxins (except murder)
Odorless and tasteless	Noticeable odor and taste
Diverse toxic effects	Fewer types of effects
Many are effective immunogens **	Poor immunogens
Aerosol delivery	Mist/droplet/aerosol delivery
*Exceptions are trichothecene mycotoxins, lyngbyatoxin, and some blue-green algae. Cause dermal injury to swimmers.	**The human body recognizes them as foreign material and makes protective antibodies against them

Toxins are unlike chemical agents in that they vary widely in their mechanism of action. (Table 10.4) Length of time from exposure to onset of symptoms also varies significantly. In battlefield scenarios, preparations can be made for treatments and preventive measures. However, in a terrorist threat, preparation is not as easy, because it is unknown when or where the terrorist will strike, or which agent would be used. (Burke, 2017)

Table 10.4 Comparison of Chemical Nerve Agent, Botulinum Toxin, and Staphylococcal Enterotoxin B Intoxication following Inhalation Exposure (Burke, 2017)

	Chemical Nerve Agent	Botulinum Toxin	Staphylococcal Enterotoxin B
Time to symptoms	Minutes	Hours (12-48)	Hours (1-6)
Nervous	Convulsions, Muscle twitching	Progressive paralysis	Headache, muscle aches
Cardiovascular	Slow heart rate	Normal rate	Normal or rapid rate
Respiratory	Difficult breathing, airway constriction	Normal then progressive paralysis	Non-productive cough; severe cases: chest pain, difficult breathing
Gastrointestinal	Increased motility, pain, diarrhea	Decreased motility	Nausea, vomiting, diarrhea
Ocular	Small pupils	Droopy eyelids	Red eyes, conjunctival injection
Salivary	Profuse watering saliva	Normal but difficult swallowing	Slight increased quantities of saliva
Death	Minutes	2-3 days	unlikely
Response to Atropine / 2PAM-CL	Yes	No	Atropine may reduce gastrointestinal symptoms

Toxins, produced by living organisms, are materials that can be connected to several types of industrial operations and bioterrorism. Unlike the other bioweapons, toxic weapons are not contagious. The toxin ricin is a natural byproduct creating Castor oil from Castor beans. Castor beans are processed worldwide, resulting in millions of tons readily available. In 1978 during the Cold War, Bulgarian dissident Georgi Markov was assassin by a poke of an Umbrella that contained tiny pellet ricin. It was reported during the Iran Iraqi war that ricin might have been used. Ricin has also been detected in the mail received at the U.S. Senate office complex in 2004

In general, governments have found BTA unsatisfactory as battlefield weapons because they are difficult to deliver efficiently while protecting their own troops and because of treaties and conventions signed among participants. However, they may be more attractive to terrorists because they have a potential to cause casualties, and to instill fear and panic in a general population. (Evers & T.J. Glover, 2010) BTA is definitely a global phenomenon. Table 10.5 Biological agents (BTA) as a function of global development / use. (Clare E. Rowland, 2016)

.

Table 10.5 Biological Threat Agents as a function of global development / use (Clare E. Rowland, October 2016)

AGENT	COUNTRY OR ORGANIZATION (1)	INCIDENTS (aggressor, target, year) (2)	TRANSMISSION MODE (3)	GREATEST CONCERN
BACTERIA				
		Germany; Allies; WWI; (4)		
Bacillus anthracis (anthrax)	US, UK, Canada. USSR, Iraq, Germany, Japan, Aum Shinrikyo	USSR; Sverdlovsk; 1979, Aum Shinrikyo, Japan, 1993; **Not Determined**; US; 2001.	**Inhalation,** *ingestion, cutaneous*	Aerosol Dispersion
Yersinia pestis (plague)	US, USSR, Japan	**Japan; China; WWII**.	**Inhalation**, *animal* vectors	High fatality rate, secondary transmission
Francisella tularensis (tularemia)	US, USSR, Japan	**USSR; German troops**; **WWII** (5)	*Ingestion*, **inhalation,** contact, animal vectors	Infectivity, difficult diagnosis, antibiotic resistance
Coxiella burnetti (Q *fever)*	US, USSR	**USSR; German troops; WWII** (5)	**Inhalation**, animal vectors	Infectivity, stability, secondary infection from animal vectors
Brucella species (brucellosis)	US	**Germany; Allies; WWI;** (4)	**Inhalation,** *ingestion, contact*	Aerosol dispersion
Burkholderia mallei (glanders)	Germany, Japan, US, USSR	**Japan; China and Manchuria; WWII; USSR; Afghanistan; 1982–4 (5)**	**Inhalation,** contact	Infectivity, high morbidity

Salmonella typhimurium (salmonella)	Japan	**Japan; China; WWII** **Rajneeshee cult; Oregon; 1984**	*Ingestion*	Incapacitation
VIRUSES				
Variola major (smallpox)	USSR, Japan	USSR; Aralsk; 1971	**Inhalation,** contact	Secondary transmission;
Viral hemorrhagic fevers (Ebola, Marburg, etc.)	US, USSR, Japan		**Inhalation,** contact	high mortality Secondary transmission;
TOXINS				
Mycotoxins (including aflatoxin, T-2 toxins)	USSR; Iraq	**USSR; Laos;** 1975-81	**Contact,** inhalation, *ingestion*	Incapacitation
Clostridium botulinum toxin (botulism)	USSR; Iraq, USSR, Germany, Japan, Aum Shinrikyo	**Aum Shinrikyo; 1990-95**	**inhalation,** *ingestion*	Extreme toxicity; aerosol dispersion
Ricin	US, UK, USSR, Iraq, Al Qaeda	**Soviet assassin; Georgi Markov; 1978**	**inhalation**, *ingestion*, intramuscular	Widespread availability
Staphylococcal enterotoxin B (SEB)	US		**inhalation**, *ingestion*	incapacitation
(1) Partial list of	States or groups	Involved in researching	Or weaponizing the	The agent
(2) Accidental releases	Are in plain text.	Attempted use shown	In italics. Successful attacks in	Bold
(3) Common natural	Transmission mode	Shown in italics & Red	Transmission mode posing greatest	Threat in bold
(4) Against livestock	Rather than	Human targets		

(5) suspected use

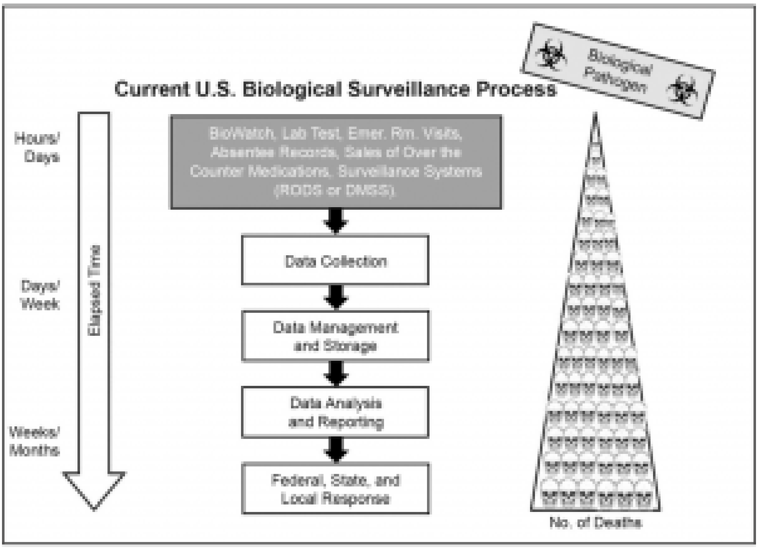
Biological attacks using bacteria or viral agents are likely to escape detection for a time period corresponding to the incubation period for the disease they cause, anywhere from hours to weeks. Toxins typically act much faster. Doctors' offices and emergency rooms are considered most likely to be the "first responders" in case of a bacterial or viral attack. (Evers & T.J. Glover, 2010)

Law enforcement officers (LEOs) are most likely to encounter attacks with toxins. They will be at more risk of exposure to bacterial or viral agents when investigating suspicious activities or where terrorists were observed or caught in the process of disseminating the agent. (Evers & T.J. Glover, 2010)

Existing U.S. Biodefense – BioWatch

Post 9/11, the United States created the BioWatch program. BioWatch is slow and cannot provide comprehensive attribution information, which leaves the U.S. population vulnerable to deadly biological agents and contributes to the nation's overall biological unpreparedness and vulnerability (Mojidi, 2019). (See Figure 10.2) This surveillance system uses more than 600 sensors in over 30 major cities across the U.S., including throughout city transport systems (Mojidi, 2019). The samples are obtained by monitoring the air quality via a specialized filter (Mojidi, 2019). The filter is tested for pathogens using the Polymerase Chain Reaction, which directly identifies pathogenic genes from a list of predetermined highly infectious diseases (Mercer, 2016).

Figure 10.2 U.S. Biological Surveillance Process (Mojidi, 2019)


Current U.S. Biological Surveillance Process
Biological Pathogen
Hours/ Days
Days/ Week
Weeks/ Months
Elapsed Time
BioWatch, Lab Test, Emer. Rm. Visits, Absentee Records, Sales of Over the Counter Medications, Surveillance Systems (RODS or DMSS)
Data Collection
Data Management and Storage
Data Analysis and Reporting
Federal, State, and Local Response
No. of Deaths

It can take from days to weeks before the U.S. government can coordinate an effective interagency response to bioterror events through the unsecured BioWatch portal. BioWatch program reported between 2003 to 2011 having 56 false alarms. Thus, putting the credibility of the BioWatch program in question. The U.S. started development on a Generation-3 system

Figure 10.3 BioWatch Gen 2 Aerosol Collector (Mercer, 2016)

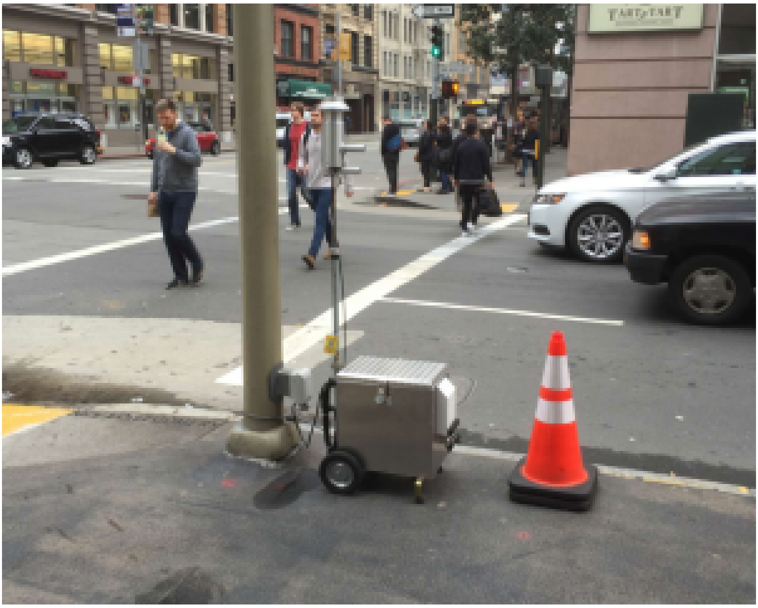


Figure 10.4 BioWatch Gen 2 Aerosol Collector (Mercer, 2016)

Biowatch Gen 2 detection capabilities consist of outdoor aerosol collectors whose filters are manually retrieved for subsequent analysis in a State or county public health laboratory that is a member of the CDC Laboratory Response Network. The results are generally received 8-10 hours after sample delivery to the laboratory. Biowatch Gen 2 is labor-intensive, and products may not be available until 12-36 hours after a biological agent's release has occurred. (See Figures 10-3 & 10.4)

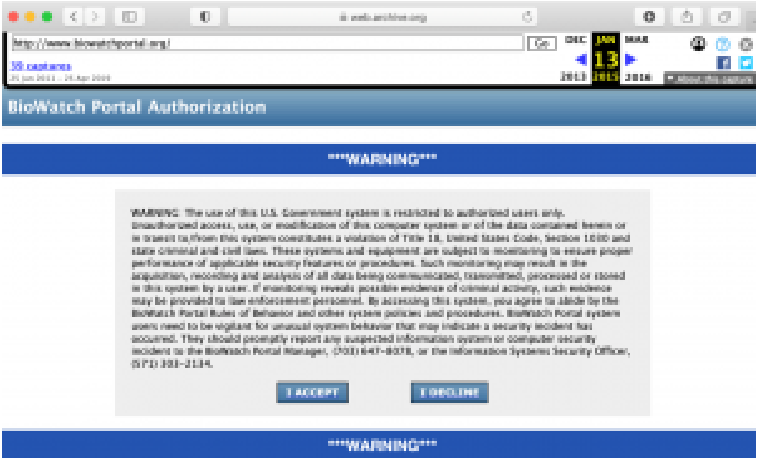
Biowatch Gen 3 was canceled in 2014 when the Government Accountability Office reported the program's upgraded capabilities from Gen 2 were not worth the investment price. In 2011 the U.S. Committee on Effectiveness of National Biosurveillance Systems said, “Generation 3 involves improvements that include replacing the existing air samplers, which require manual retrieval and laboratory analysis of filters, with automated detectors capable of onsite sample analysis and an anticipated expansion of the BioWatch system’s coverage. Over the next decade, such upgrades will more than double the program’s direct cost to $200 million on an annualized basis. The expansion of coverage mainly drives the higher cost. As shown by comparing the Generation 2 scenario to a scenario in which the Generation 3 technology is used without expanding the number of jurisdictions or deployed detectors, the cost of acquiring and fielding new technology is largely offset by the cost savings associated with automated analysis of the detector samples” (Institute of Medicine (US) and National Research Council (US) Committee on Effectiveness of National Biosurveillance Systems, 2011). Biowatch Gen 3 was to operate 24 hours a day year-round, continuously monitoring the air for agents and expanding to other areas. The BioWatch program is the only U.S. initiative in place for bio surveillance.

In the private sector, when an audit is conducted internally or if a third party and critical items are identified, the offender needs to have an immediate mitigation plan and resolve the issue in a reasonable amount of time. We can see this across the financial health care and retail sector with the enforcement of different federal regulations that must be compliant for the business to remain in business without incurring a fine or completely shut down. A security audit completes in 2017 found the BioWatch website to be critical in high risk of vulnerabilities, including weak encryption that made the website susceptible to online attacks. The website was also noted not to have any protective monitoring. The data on that website included some of the Biowatch air samplers’ locations, which are installed throughout the United States. The results of the Biowatch air samplers and possible pathogens they detect in response plans were available on the website. The website was run by a private company, Logistics Management Institute (LMI), and was considered a (dot)org versus (dot) gov website. James

McDonnell, assistant secretary of Homeland security counter countering weapons of mass destruction office, stated the data was housed outside the secure government firewall and were not significant enough to cause a national security threat (Baumgartner, 2019). A security scan found Up to 41 vulnerabilities and attempted access to the portal by unauthorized users. The website was retired in May 2019; however, at the time of this writing, with the Wayback machine, image captures return a positive result except for the final capture taken in April 2019. (Figure 10.5)

At the House Homeland Security Committee subcommittee hearing fall of 2019, experts testified that our biodefense system has been vulnerable and outdated over the past ten years (Rutschman, 2019).

Figure 10.5 BioWatch Portal Snapshots Remain (by Author)



WARNING: The use of this U.S. Government system is restricted to authorized users only. Unauthorized access, use, or modification of this computer system or of the data contained herein or in transit to/from this system constitutes a violation of Title 18, United States Code, Section 1030 and state criminal and civil laws. These systems and equipment are subject to monitoring to ensure proper performance of applicable security features or procedures. Such monitoring may result in the acquisition, recording and analysis of all data being communicated, transmitted, processed or stored in this system by a user. If monitoring reveals possible evidence of criminal activity, such evidence may be provided to law enforcement personnel. By accessing this system, you agree to abide by the BioWatch Portal Rules of Behavior and other system policies and procedures. BioWatch Portal system users need to be vigilant for unusual system behavior that may indicate a security incident has occurred. They should promptly report any suspected information system or computer security incident to the BioWatch Portal Manager, (703) 647-8078, or the Information Systems Security Officer, (571) 331-2134.

NEXT GENERATION – DNA to GENOME

In 1997, the JASON group (a group of academic scientists who advise the U.S. government in science and technology), focused on genetically engineered pathogens and biological weapons. The group came up with six potential threats: binary biological weapons, designer genes, weaponized gene therapy, stealth virus-host swapping diseases, and designer diseases. At the time of their study, some of the technology existed to produce such threats.

Science evolved, presenting commercial opportunities to collect consumers' DNA to help complete the puzzle of family members' heritage. The consumer agreed to the fine print ,in the excitement to find out their origin, but also surrendered their personal (private) data to be used for research. As a result, DNA is used by several different industries to profit from the information available from the DNA data collected. The marketing industry launched large-scale consumer advertising companies such as Airbnb© and Spotify©. They use collected DNA datasets to attract customers. The genetic data can give creative strategies to leverage customers' requirements(and company profits) based on their genomes. [9] [10]

DNA collection can occur for medical reasons. DNA data can live on the physical computer systems of the lab, a medical professional or their gloves, treatment center/hospital, health care company, university, and in some cases, a state. It was confirmed in 2017 by news reports that Asian based firms have obtained U.S. DNA data and plan to collect additional Americans DNA through commercial and medical means (Javers, 2017). Since that report, several healthcare companies, facilities, and organizations have suffered data breaches. [11]

Genomic data can be digitized. With quantum computing,[12] we can understand the genetic development of living organisms, how they are vulnerable to diseases, and how they would respond to drugs and treatments. Genomic research has increased the development of medicines and vaccines dramatically. For example, a vaccine was created in less than three months for the mutated flu virus strain H7 N 9. This converging technology also poses a BW threat when it is used to identify harmful genes or DNA sequences.

There are risks and benefits to dual use DNA collection. The primary concerns are the amount of data being collected; who collects and filters /categorizes the data; who owns the data; where is it stored; and can it be resold. Another issue is can the collected databases be hacked. Data collected by Cambridge Analytics through social media for elections was weaponized and published.

DNA can lead to a designer bioweapon, to affect genocide. Our DNA data can be used to understand how our mind and body will react. Synthetic viruses or genes combined with the use of quantum dots, nanoparticles, and 3D printer materials to create a bioweapon / biodefense agent to target a population or protect that same population. DNA technologies are disturbing and will have a future impact on the airline, marine and most definitely the defense industries.

Nanowire

In 2005, research was completed on the concept of using nanowires, as ultrasensitive electronic sensors to detect biological and chemical agents (Fernando Patolsky, 2005). Dr. Charles Lieber and Professor Fernando Patolsky discuss the creation of a sensor that's configured with nanowire with the natural oxide coding. The aforementioned receptor construction is more efficient than the current modification of glass or a Silicon oxide to create the sensor (Fernando Patolsky, 2005). When a virus particle binds to an antibody receptor on a nanowire device, the conductance of that device will change from the baseline value. When the virus unbinds again, the conductance will return to the baseline value (Fernando Patolsky, 2005). When the nanowire encounters influenza the nanowire reflects accurate characteristics that are consistent with influenza viruses. The sensor is able to produce optical and electrical data it receives from the nanowire as the virus diffuses near the nanowire device (Fernando Patolsky, 2005). The Harvard team was able to determine the difference in distance of spacing the nanowires over different size areas when the sensor could encounter and detect two other viruses. Dr. Charles Lieber and Professor Fernando Patolsky concluded that nanowire sensors could be key for virus sensing devices for the medical community and used to detect bioterrorism (Fernando Patolsky, 2005).

Advances in nano-biosensor technology offer the ability to alert LEO / DHS to a biological weapons attack. This early warning system permits enactment of countermeasures such as containment. Dr. Jing Wang of the Swiss Federal Laboratories for Materials Science and Technology (Empa, ETH Zurich) and Zurich University Hospital was tasked with creating a sensor to detect SARS-COV-2. In January 2020, the team began testing sensors to see if they could differentiate bacteria and viruses transmitted in the air (Global Biodefense Staff, 2020). The goal of the sensor was to be used in places like train stations or hospitals. It would measure the virus concentration in the air in real-time (Global Biodefense Staff, 2020). Doctor Wang and his team developed a sensor that combines two different methods to detect viruses using optical and thermal means. The sensor is based on tiny structures of gold nanoislands on a glass substrate (Global Biodefense Staff, 2020) . Artificially produced DNA receptors that match specific coronavirus sequences of SARS CoV-2 are grafted onto the nanoislands (Global Biodefense Staff, 2020). The coronavirus virus genome does not consist of the DNA double-strand as in living organisms. The virus has the DNA of a single strand (Global Biodefense Staff, 2020). Therefore, the receptors on the sensor can identify the virus. The optical component, localized surface plasmon resonance (LSPR), can be used to measure whether the sample contains RNA strands of SAR-CoV-2 or SARS-COV. The thermal component, plasmonic photothermal (PPT), can detect whether the DNA strand is single or double using localized heat produced by a laser of a specific wavelength (Global Biodefense Staff, 2020). The sensor is in the early phase of development and not ready for measurement of

COVID-19. When the sensor is completed testing it could be applied to two other viruses. Dr. Wang's sensor was featured as part of the science -Switzerland April – May 2020 report, sponsored by Swissnex. (Fernando Patolsky, 2005)

Conclusions

- Pathogens are continuing to grow and disembogue into the human population
- Biodefense is essential in defending the U.S. from adversaries and preservation of American lives. It represents a significant Disturbing Technology for all three theaters: Airline, Marine and Defense. (Mauroni, 2014)

- Funding for the scientific community is essential for further discovery, tracking, understanding, and constructing countermeasures against pathogens.
- Lessons can be learned from past reductions in funding for bioterrorism.[13]
- Nanotechnologies are the next generation of technology that can contribute significantly to several different fields, including medical and bioterrorism defenses.
- Cybersecurity plays a critical role in preventing bioterrorism. There needs to be an understanding of adversarial use of the data collected in the public and private sector and stored and transmitted securely.

Post Analysis from a Terrorist Point of View

Terrorists like *Disturbing Technologies* because they make their mission / goals of population disruption manageable. Biological agents and toxins are the most likely terrorist weapons for the future. They are inexpensive, do not require a great deal of technical expertise or equipment to manufacture, and can be produced without creating a lot of attention. Biological agents have the best potential as weapons of mass destruction or disruption. They have the ability to inflict extremely high levels of casualties on a target population. It has been estimated by WHO that 50 kilograms of aerosolized anthrax spores dispensed 2 kilometers upwind of a population center of 500,000 unprotected people in an ideal meteorological condition, would travel greater than 20 kilometers downwind, and kill / incapacitate up to 125,000 humans in the path of the biological cloud. It is estimated by the Defense Department that the amount of anthrax equal to a five-pound bag of sugar in size would be enough to kill half the population of Washington, DC. (Burke, 2017)

To be effective against large numbers of people, biological agents must be properly disseminated. Conventional explosives could be used for this purpose, along with common agricultural and home garden spraying equipment modified to generate the smaller particle size of biological materials. Motorized vehicles, boats, and airplanes could also provide effective dissemination. Spray devices would need nozzles in the 1- 10-micron range for optimum dissemination. Weather conditions are critical for the effective deployment of biological agents as aerosols. The ideal weather would occur during the early morning or evening hours. (Burke, 2017)

The federal government has clamped down on the sale and use of biological agents in research facilities. A program has been developed to control the "Transfer or Receipt of Select agents." (Burke, 2017)The Anti-Terrorism and Effective Death Penalty Act of 1996 requires regulation of shipment and receipt of certain microorganisms and toxins. Regulations are detailed in Appendix E of (Burke, 2017) This reference also give over 20 pages of resources, websites, agency contacts, notifications to gain more information or report an incident. (Burke, 2017)

References

Baumgartner, E. (2019, August 25). *It was sensitive data from a U.S. anti-terror program – and terrorists could have gotten to it for years, records show*. Retrieved from La Times: https://www.latimes.com/science/sciencenow/la-sci-biowatch-20190402-story.html

Bronze, M. S. (2002). Viral agents as biological weapons and agents of bioterrorism. *The American journal of the medical sciences*, 323(6), 316–325.

Bruce Budowle, S. E. (2020). *Microbial Forensics.* London: Academic Press.

Burke, R. (2017). *Counterterrorism for Emergency Responders, 3rd edition.* Boca Raton, FL: CRC.

CDC. (2021, January 16). *Infection Control Considerations for High-Priority (CDC Category A) Diseases that May Result from Bioterrorist Attacks or are Considered to be Bioterrorist Threats.* Retrieved from www.cdc.gov/: https://www.cdc.gov/infectioncontrol/guidelines/isolation/appendix/bioterror-precautions.html

CDC Emerging Infectious Diseases. (2003, January 17). *Rajneeshee Bioterror Attack*. Retrieved from Homeland Security Digital Library (HSDL): https://www.hsdl.org/c/tl/rajneeshee-bioterror-attack/

Clare E. Rowland, C. W. (October 2016). Nanomaterial-based sensors for the detection of biological threat agents. *Materials Today*, V19, No. 8: 464-477.

DrPH, E. H., & Shiel, W. C. (2020, October 16). *What Is the Biological Warfare?* . Retrieved from eMedicineHealth: https://www.emedicinehealth.com/biological_warfare/article_em.htm

Evers, D., & T.J. Glover, T. M. (2010). *Pocket Partner for Law Enforcement, 5th edition.* Littleton, CO: Sequoia Publishing.

Federal Bureau of Investigation. (2021, January 12). *Weapons of Mass Destruction.* Retrieved from FBI: https://www.fbi.gov/investigate/wmd

Fernando Patolsky, C. M. (2005, April). Nanowire Nanosensors. *Materials Today*, pp. 21-28.

Fish, J., & R.N. Stout, &. E. (2011). *Practical Crime Scene Investigations for Hot Zones.* Boca Raton, FL: CRC.

Foley, J. B. (2017). *A Nation Unprepared: Bioterrorism and Pandemic Response.* Fort Leavenworth: Arthur D. Simons Center for Interagency Cooperation.

Global Biodefense Staff. (2020, April 21). *A New Optical Biosensor for the COVID-19 Virus.* Retrieved from Global Biodefense: https://globalbiodefense.com/2020/04/21/a-new-optical-biosensor-for-the-covid-19-virus/

Global Biodefense Staff. (2020, February 2020). *Shutdown of PREDICT Infectious Disease Program Challenged by Senators Warren and King.* Retrieved from Global Biodefense: https://globalbiodefense.com/2020/02/04/shutdown-of-predict-infectious-disease-program-challenged-by-senators-warren-and-king/

Google. (2021, January 16). *Current Global death toll and cases reported for COVID-19* . Retrieved from www.google.com: www.google.com

Institute of Medicine (US) and National Research Council (US) Committee on Effectiveness of National Biosurveillance Systems. (2011). *Biowatch and the Public Health System. Biowatch and Public Health Surveillance: Evaluating Systems for the Early Detection of Biological Threats: Abbreviated Version.* Washington D.C.: National Academies Press (US).

Javers, E. (2017, March 14). *Official: American DNA info at risk for theft by foreign powers.* Retrieved from CNBC: https://www.cnbc.com/2017/03/14/us-official-american-dna-info-at-risk-for-theft-by-foreign-powers.html

Mercer, B. (2016, January 28). *SFGATE.* Retrieved from That mysterious Homeland Security box plugged into an SF utility pole is a..: https://www.sfgate.com/superbowl/article/That-mysterious-Homeland-Security-box-plugged-6790510.php

Mojidi, H. (2019). Advancing Bio Detection with Biosensors and

Nanotechnology for Rapid Interagency Response. *InterAgency Journal* Vol. 10, No. 2, 44.

Nuclear Threat Initiative (NTI). (2015). *Biological*. Retrieved from Nuclear Threat Initiative (NTI): https://www.nti.org/learn/countries/united-states/biological/

Rutschman, A. S. (2019, November 17). *Salad bars and water systems are easy targets for bioterrorists – and America's monitoring system is woefully inadequate*. Retrieved from The Conversation: https://theconversation.com/salad-bars-and-water-systems-are-easy-targets-for-bioterrorists-and-americas-monitoring-system-is-woefully-inadequate-126079

Schmidt, C. (2020, April 3). *Scienctific America*. Retrieved from Why the Coronavirus Slipped Past Disease Detectives: https://www.scientificamerican.com/article/why-the-coronavirus-slipped-past-disease-detectives/

Tara O'Toole, M. M. (April 2002). Shining Light on "Dark Winter". *Clinical Infectious Diseases*, *Volume* 34, *Issue* 7, 972–983.

Tucker, J. B. (1998, November 6). *Biological Weapons in the Former Soviet Union: Am Interview with Dr. Kenneth Alibel*. Retrieved from nonproliferation.org: https://www.nonproliferation.org/wp-content/uploads/npr/alibek63.pdf

United Nations. (2021, January 7). *History of the Biological Weapons Convention*. Retrieved from United Nations: https://www.un.org/disarmament/biological-weapons/about/history/

USAID . (2020, September 30). *USAID ANNOUNCES NEW $100 MILLION PROJECT TO ANTICIPATE THREATS POSED BY EMERGING INFECTIOUS DISEASES*. Retrieved from USAID: https://www.usaid.gov/news-information/press-releases/sep-30-2020-usaid-announces-new-100-million-project-threats-emerging-infectious

USAID. (2021, January). *USAID PERDICT*. Retrieved from USAID: https://www.usaid.gov/sites/default/files/documents/1864/predict-global-flyer-508.pdf

Wheelis, M. (1998). First shots fired in biological warfare. *Nature*, 395.

Zastrow, M. (2019, October 15). *Why Japan imported Ebola ahead of the 2020 Olympics.* Retrieved from Nature.com: https://www.nature.com/articles/d41586-019-03103-4

[1] The HAZARD Classification System divides dangerous goods into nine classes of materials for purposes of transportation, identification, and placarding: Class 1- explosives; Class 2 -gases; Class 3-Combustable liquids; Class 4-Flamable solids & water reactive; Class 5- Oxidizing substances; Class 6- Toxic & Infectious substances; Class 7 – Radioactive materials; Class 8 – Corrosive substances & Class 9 – Miscellaneous Hazardous materials. The entire system is further divided into compatibility groups (letters) and special placarding restrictions on all DOT or vehicles in DOT jurisdiction must comply. If it moves it falls under these restrictions. See (Evers & T.J. Glover, 2010)

[2] Center for Disease Control (CDC) Taxonomy for LEO of Biological Weapons – Along with the HAZMAT U.N. DOT classification system, there are other classification systems. CDC uses a general system for LEOs (Evers & T.J. Glover, 2010) where:

CDC Category A

These organisms pose a risk to national security because they can be easily disseminated or transmitted from person to person. They result in high mortality rates and have the potential for major public health impact and might cause public and social disruption. They require special action for public health preparedness.

CDC Category B

These are moderately easy to disseminate and result in moderate morbidity rates and low mortality rates. They require specific enhancements of CDC's diagnostic capability and enhanced disease surveillance.

CDC Category C

These agents include emerging pathogens that could be engineered for mass dissemination in the future because of availability, ease of production and dissemination, potential for high morbidity

and mortality rates, and major health impact.

Type

B= Bacteria

V= Virus

T= Toxin

R = Rickettsial

Precautions

Consult with current CDC guidelines. (CDC, 2021) Also, Chapter 4 on BTA from (Burke, 2017) discusses precautions and protective equipment in detail.

Dissemination

Dissemination is most likely by aerosol; some could also be used as food or water contaminants; Inhalation is the mist deadly route of exposure in all cases. (Evers & T.J. Glover, 2010)

More official information about biological hazards falls under DOT HAZMAT Guide 153 available in (Evers & T.J. Glover, 2010). From a LEO, forensics, protective gear perspective, one can consult Practical Crime Scene Investigations for Hot Zones. (Fish & R.N. Stout, 2011)

Table 10.2 shows the Biological agents as a function of global development / use.

[3] The James Bond movie *Goldfinger* had toxins released from crop dusters on Fort Knox troops.

[4] There is a detailed discussion of this incident in (Burke, 2017).

[5] It can be argued and there is corroborative Open-Source evidence to support the theory that COVID-19 was in 2020 a human-engineered / developed bioweapon (BW) in a Chinese Lab in Wuhan, China The postulate is that it escaped its containment apparatus and spread to the world causing unintended grievous harm and death. Whether this BW theory true, partially true,

negligence or intentionally delivered does not really matter because as of this writing (1/16/2021) 92,775,578 cases have been reported with 1,986,842 COVID-19 deaths. About 29% of reported cases are attributable to North America with 569,333 lost souls. This is a solid example of what a BW can do if not contained or breached countermeasures. (Google, 2021)

[6] LD50 of as toxin, radiation, or pathogen is the dose required to kill half the members of a tested population after a specified test duration. LD50 figures are frequently used as a general indicator of a substance's acute toxicity. A lower LD50 is indicative of increased toxicity. (Evers & T.J. Glover, 2010)

[7] Anthrax is the Greek word for coal

[8] Virus is Latin for "poisonous slime."

[9] Think movie *Minority Report* where Tom Cruise replaces his eye to bypass biometric security controls and as he passes optical readers at a mall, the stores pitch him for their goods based on the wrong profile.

[10] Recognize that the government and LEO all have access to this data. LEO does use DNA data responsibly to solve outstanding felony cases. However, it is up for grabs whether we believe that the government is so attentive and responsible with our private data.

[11] There is little definitive proof that the breaches were related to the DNA data thefts.

[12] Quantum computing is in its infancy. There is plenty of research money and a few startups making a run for this technology. There is lots of hype but not much "commercial beef."

[13] For example, USAID PREDICT received approximately $200 million over ten years, a fraction of the $2 trillion in emergency-

relief spending authorized by Congress as a response to COVID-19 as of March 2020 (Schmidt, 2020).