

5-9-2022

## DRONE DELIVERY OF CBNRECy – DEW WEAPONS Emerging Threats of Mini-Weapons of Mass Destruction and Disruption (WMDD)

Randall K. Nichols

*Kansas State University - Polytechnic Campus*

Suzanne Sincavage

Hans Mumm

Wayne Lonstein

Candice Carter

*See next page for additional authors*

Follow this and additional works at: <https://newprairiepress.org/ebooks>



Part of the [Aerospace Engineering Commons](#), and the [Aviation and Space Education Commons](#)



This work is licensed under a [Creative Commons Attribution-Share Alike 4.0 License](#).

---

### Recommended Citation

Nichols, Randall K.; Sincavage, Suzanne; Mumm, Hans; Lonstein, Wayne; Carter, Candice; Hood, John Paul; Mai, Randall; Jackson, Mark; Monnik, Mike; McCreight, Robert; Slofer, William; and Harding, Troy, "DRONE DELIVERY OF CBNRECy – DEW WEAPONS Emerging Threats of Mini-Weapons of Mass Destruction and Disruption (WMDD)" (2022). *NPP eBooks*. 46.

<https://newprairiepress.org/ebooks/46>

This Book is brought to you for free and open access by the Monographs at New Prairie Press. It has been accepted for inclusion in NPP eBooks by an authorized administrator of New Prairie Press. For more information, please contact [cads@k-state.edu](mailto:cads@k-state.edu).

---

## Authors

Randall K. Nichols, Suzanne Sincavage, Hans Mumm, Wayne Lonstein, Candice Carter, John Paul Hood, Randall Mai, Mark Jackson, Mike Monnik, Robert McCreight, William Slofer, and Troy Harding

# **DRONE DELIVERY OF CBNRECY DEW WEAPONS EMERGING THREATS OF MINI-WEAPONS OF MASS DESTRUCTION AND DISRUPTION (WMDD)**



---

**Nichols • Sincavage • Mumm • Lonstein  
Carter • Hood • Mai • Jackson  
Monnik • McCreight • Slofer**

---

DRONE DELIVERY OF CBNRECy – DEW  
WEAPONS Emerging Threats of Mini-Weapons of  
Mass Destruction and Disruption ( WMDD)



Copyright © 2022 Randall K. Nichols, Suzanne Sincavage, Hans C. Mumm, Wayne D. Lonstein, Candice M. Carter, John-Paul Hood, Randall Mai, Mark J. Jackson, Mike Monnik, Robert McCreight, William Slofer, and Troy Harding

Cover design by Suzanne Sincavage and Brenda Andrews

New Prairie Press,  
Kansas State University Libraries  
Manhattan, Kansas

Electronic edition available online at:  
<https://newprairiepress.org/ebooks/46/>

This work is licensed under a  
[Creative Commons](https://creativecommons.org/licenses/by-nc-sa/4.0/) Attribution-NonCommercial-ShareAlike  
4.0 International License  
<https://creativecommons.org/licenses/by-nc-sa/4.0/>



ISBN-: 978-1-944548-44-5

NEW prairie PRESS  
*open access scholarly publishing*



DRONE DELIVERY OF  
CBNRECy – DEW  
WEAPONS Emerging  
Threats of Mini-Weapons of  
Mass Destruction and  
Disruption ( WMDD)

*RANDALL K. NICHOLS; DR SUZANNE  
SINCAVAGE; DR HANS C. MUMM; WAYNE  
LONSTEIN; CANDICE CARTER; CPT  
JOHN PAUL HOOD; RANDALL MAI; DR  
MARK JACKSON; MIKE MONNIK; DR  
ROBERT MCCREIGHT; AND WILLIAM  
SLOFER*

NEW PRAIRIE PRESS  
MANHATTAN, KS



DRONE DELIVERY OF CBNRECy – DEW WEAPONS *Emerging Threats of Mini-Weapons of Mass Destruction and Disruption ( WMDD)* by Randall K. Nichols is licensed under a [Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-nc-sa/4.0/), except where otherwise noted.

**Copyright © 2022 Nichols, R. K., Sincavage, S., Mumm, H.C., Lonstein, W.D., Carter, C., Hood, J.P, Mai, R., Jackson, M., Monnik, M., J., McCreight, R., Slofer, W.**

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

# Contents

|  |       |
|--|-------|
| Title Page   | ix    |
| Copyright / Publication Page                                     | xii   |
| Books also by Professor Randall K. Nichols & the<br>Wildcat Team | xiii  |
| Dedications  | xv    |
| Disclaimers  | xx    |
| Foreword   | xxii  |
| Preface  | xxiv  |
| Acknowledgements   | xxix  |
| List of Series Contributors                                      | xxxiv |
| Abbreviations and Acronyms                                       | lxv   |
| Table of Contents -Detailed                                      | 1     |
| Table of Figures   | 19    |
| Table of Tables  | xxix  |
| Table of Equations   | xxxii |

Part I. Section I: Chemical, Biological, Radiation,  
Nuclear, Explosive (CBRNE) Weapons and  
Payloads

|  |    |
|--|----|
| 1. Drones Capabilities to Deliver Weapons of Mass<br>Destruction / Disruption (WMDD) | 37 |
| 2. Chemical Weapons  | 58 |
| 3. Biological Weapons  | 80 |

|  |     |
|--|-----|
| 4. Radiological, Electromagnetic, Drone & Metaverse Risks and Issues | 93  |
| 5. Nuclear Weapons   | 127 |
| 6. Explosives Delivered by Drone                                     | 143 |
| 7. Deception   | 169 |

Part II. Section 2: Directed Energy Weapons (DEW) and Payloads

|                                    |     |
|------------------------------------|-----|
| 8. DEW Primer                      | 211 |
| 9. DE Weapons, Projectiles, Damage | 236 |
| 10. DE Weapons, MASERS/LASERS      | 279 |
| 11. DE Weapons & Microwaves        | 320 |
| 12. Hypersonic Drone Missiles      | 358 |
| 13. Acoustic Weapons               | 410 |
| 14. Satellite Killers              | 465 |
| 15. Cyber Weapons and CBRNE        | 485 |

Part III. Section 3 Risk Assessment and Policy Considerations

|  |     |
|--|-----|
| 16. Assessing the Drone Delivery Future WMDD and DEW Threats/Risks                                   | 523 |
| 17. Unique Challenges of Responding to Bioterrorism & Chemical Threats & Attacks Delivered by Drones | 548 |
| 18. Practical Crime Scene Investigation (CSI) Using Autonomous Systems                               | 565 |
| 19. Navigation Spoofing and ECD  | 588 |

Part IV. Section 4: Social Networks and Tools of  
the Trade

|  |     |
|--|-----|
| 20. Social Network Implications for WMDD | 633 |
| 21. Tools of the Trade                   | 646 |





# Books also by Professor Randall K. Nichols & the Wildcat Team

Nichols, Randall K.; Sincavage, S.; Mumm, Hans. C.; Lonstein, Wayne D.; Carter, Candice M.; Hood, John-Paul; Mai, Randall; W Jackson, M.; Monnik, M.; McCreight, R. & Slofer, W. **DRONE DELIVERY OF CBNRECy – DEW WEAPONS Emerging Threats of Mini-Weapons of Mass Destruction and Disruption (WMDD)** (2022) Copyright 2022, All Rights Reserved. NPP eBooks. #46/  
<https://newprairiepress.org/ebooks/46/>

Nichols, Randall K.; Sincavage, S.; Mumm, Hans. C.; Lonstein, Wayne D.; Ryan, Carter, Candice M.; Hood, John-Paul; Jackson, M., Mai, Randall W.; & Shields, B. **Disruptive Technologies With Applications In Airline, Marine, Defense Industries** (2021) Copyright 2021, All Rights Reserved. NPP eBooks. 38.  
<https://newprairiepress.org/ebooks/38/>

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 **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 38 years, Montine, and children Robin, Kent, Phillip (USA Army), Diana (USA Army), and Michelle who have lived with a Dragon and survived; to our 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.

In addition, in 2017, 17 sailors died because of two separate collisions involving US Navy warships in the South China Seas, the USS Fitzgerald and the USS John S. McCain. In my professional opinion, the US Navy's official response was insufficient as to real causes. Since 2017, I have dedicated my research to giving purpose, closure, truth, and voice to the families of these Honorable sailors. God grant them peace.

I dedicate my writing to the Ukrainian people suffering and fighting with such bravery against overwhelming Russian savagery in a war they did not choose.

Lastly, my deepest gratitude to my wonderful, talented Wildcat writing team. It has been a real Honor. My chapter on this earth is closing, and I have been truly blessed to work with you. My cup runneth over.

## **From Dr. Suzanne Sincavage:**

I want to dedicate my research to the men and women who are devoted to biodefense intelligence and the non-proliferation of WMDs; To Professor Randall Nichols for his leadership, mentorship, integrity, and significant contributions to the field of unmanned systems, I'm honored to be a part of your amazing

team; To my sons Trevor Muehlfelder, Cole Muehlfelder and David Sincavage III for their loving encouragement and support; To Dr. Steve Herrick, who changed the trajectory of my life, To Candice Carter, a true friend and co-author, her devotion to biodefense research are invaluable; and Brenda A. Andrews, renowned art professor and colleague for her insights and support in transforming the digitization of data into visual art forms.

**From Dr. Hans C. Mumm:**

I dedicate this work to my students and colleagues and all those innovators, those dreamers who race against time as they create an ever-changing and evolving future 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, Sam, extended family and co-workers, and co-authors from whom I have learned so much. To all those brave souls who have made the ultimate sacrifice serving this nation and 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 become a more peaceful and harmonious place for all.

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

I dedicate this work to my husband, Dan, and my students, who have taught me so 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 succeed in asymmetric warfare and 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 Gwendolyn, and my extended family. They 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 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 – to 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. Oswald 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 walk 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. My family has grown. To my blessed group comes

a granddaughter, Olivia Jeannine Oswald. My cup runneth over. And lastly, Professor Nichols has become a valued mentor and true friend. He has helped me 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, and 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 know that. I could not have done any of this without them. It has been long and difficult, and unfortunately, I am still in transition, but thankfully, it will be ending soon.

**From Robert McCreight:**

I dedicate my chapter to all US service personnel who fought in, or supported, combat operations with unflagging thanks to their families for the sacrifice that cannot be measured. Honorable military service must be acknowledged and respected as a tireless effort to keep our nation safe and secure tomorrow's peace as a sacred duty.

There are sincere thanks to serious professional and dedicated members of law enforcement whose daily routine involves our first line of domestic security and societal stability. These unselfish warriors and police never get the full thanks and gratitude they genuinely deserve. Thanks, and a salute from a grateful nation.

**From Mike Monnik:**

I dedicate this work to my team, who give me purpose and fulfillment. I thank my wife Fedora for her infinite trust and Dr. Lei Pan for his guidance and wisdom. The coming years will be a stark reminder of our work in this field and for that, I have the utmost appreciation for Professor Nichols and his vision. Finally, to



all DroneSec customers who live and breathe this problem set on a daily basis – you are writing the future.

**From William Slofer:**

I would like to give thanks to God for giving my parents the wisdom and discernment to consistently send me to the library to find answers to my endless parade of questions they could not answer. I also want to give a special thanks to my daughter who continued to encourage me through my journey as a life-long learner and the few friends that have been by my side through thick and thin. That support and encouragement has truly made the difference.

Thank you one and all.

# Disclaimers

The authors have obtained the information contained in this work from sources believed to be accurate and reliable. However, neither New Prairie Press, Professor Randall K. Nichols (Managing Editor / Author / Publisher), Kansas State University, nor its authors guarantee the information's accuracy or completeness. Neither the parties mentioned above nor its authors shall be responsible for any errors, omissions, or damages arising from using this information.

This work examines *inter alia* technical, legal, and ethical dimensions of behavior regarding unmanned vehicles in the air and underwater / drone delivery of chemical threats, biological threat agents, radiation threats, nuclear threats, cyberwar, 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 the services of a lawyer authorized to practice in the appropriate jurisdiction. All scenarios discussed in this work are hypothetical and not to be taken or construed as actual occurrences.

The authors, publishers, and associated institutions represent that all reasonable steps and special review protocols have been taken to ensure that all information contained herein is OPEN sourced from the public domain. 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 information above by any party or intentionally disseminated to any third party or parties for any illegal or improper purpose is expressly forbidden.

The authors and publisher have also strived to attribute and cite all third-party sources of information and content to the greatest extent possible where available permission has been sought for all such content, including figures, data, and tables. In many instances, sources from which the authors seek permission have not replied to requests or no longer have contact information. Should we have missed citing any source, we welcome them contacting the Managing Editor, Professor Randall K. Nichols, who will ensure that any such oversight is corrected.

# Foreword

When I first met Randall Nichols in 2014, he had just retired from Utica College as a Professor in Cybersecurity. At the time, I was a Professor in Computer Systems Technology on the Kansas State University Salina campus. K-State Salina had already established one of the first UAS degree programs in the United States and had built a strong UAS research program. Professor Nichols approached K-State Salina to discuss the need to integrate cybersecurity education into our UAS programs and raise awareness of the security implications of UAS technology. Shortly after our first meeting, K-State hired Professor Nichols to do just as he suggested. Randall Nichols has established himself as one of the world's foremost cybersecurity experts in UAS/CUAS/UUV and related technologies.

This textbook is the sixth in a series covering UASs & UUVs from Randall Nichols and his team of experts. It is an ambitious project demonstrating just how far drone technology and its uses have come. I have been fortunate enough to be on the team's communication channel as they share the latest news and viewpoints and discuss chapter content. The 2022 Russian invasion of Ukraine began midway through the writing of this book. It has been amazing to see how this dedicated team of authors reworked their chapters to incorporate the latest use cases happening in real-time. As you read the book, I hope you appreciate the amount of research behind it and the team's ability to distill that information into a digestible format.

Though the idea of using drones to deliver weapons may not be the image that the industry wants to cultivate, it is nevertheless a fascinating and essential subject. The authors do an excellent job of describing how the same drone technology that can navigate urban landscapes to deliver packages to our houses can potentially deliver DEW and CBRNE weapons. The same drone technology that

provides an efficient means of spraying an agricultural field could spray a deadly chemical or biological weapon. Artists may use drone swarm technology to create beautiful light shows, while terrorists might use it to deliver a multiprong, multiweapon attack on a target. Of course, this book would not be complete without discussing the detection and mitigation of such attacks. You will learn about drone navigation, sensor, communication, and software technologies and their vulnerabilities.

So far, I have only given you a glimpse of the true scope of the book. There is so much more here for you to discover. The book includes the history of the different weapon and drone technologies, descriptions of how they work, and various use cases and applications. You will delve into policy considerations and even peek into the tools of the trade. Furthermore, there are chapters on emerging technologies such as hypersonic drone missiles and satellite killers.

To fully understand any technology, you need to know the full scope of how people might apply it. It is not enough to only look at how a set of technologies might make our lives more convenient or profitable. We need to understand the other side of the coin. We need to know how people might use those same technologies to wreak havoc and destroy lives or, on the flip side, use them to fight back against a more powerful invader. I expect that this book will provide an excellent resource for your journey into this critical and fascinating arena.

Best wishes,

Troy Harding

Department Head and Professor

Integrated Studies

Kansas State University Salina

Aerospace and Technology Campus

# Preface

**Drone Delivery of CBNRECy – DEW Weapons: Emerging Threats of Mini-Weapons of Mass Destruction and Disruption (WMDD)** is our sixth textbook in a series covering the world of UASs & UAVs. Other textbooks in our series are **Disruptive Technologies with applications in Airline, Marine, Defense Industries; 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**. Our previous five titles have received considerable global recognition in the field. (Nichols et al., 2021) (Nichols R. K. et al., 2020) (Nichols R. et al., 2020) (Nichols R. et al., 2019) (Nichols R. K., 2018) [\[1\]](#)

Our sixth title is a new purview for UAS / CUAS / UAV (drones). We are concerned with the future use of these inexpensive devices and their availability to maleficent actors. As I write this Preface, we are on the 56th day of the savage invasion of Ukraine by Russia under President Putin. The Russian drone fleet numbers are above 500. They have had five years to grow their fleet. It currently uses them for domestic security, Syrian operations, and defense. (Facon, 2016) In the conflict, Russian troops seriously outnumber Ukrainian forces. However, on February 8, 2022, a Forbes report stated that Ukraine used 20 Turkish TB-2 drones to hit Russian targets and offset some of Russia's enormous military advantages. (Malsin, 2022) According to Fox News, on February 27, 2022, President Putin ordered nuclear deterrent forces status raised to "special combat readiness" (Colton, 2022)

News like this in just one conflict suggests that UASs in air and underwater will be the future of military operations. They can deliver a huge punch for a low investment and minimize human

casualties. Our team believes that China is watching both the United States' Neville Chamberlain appeasement strategy and the aggressive nature of Russia in its full-scale invasion of its neighbor. This portends that Taiwan is the next meal on the global plate. Unfortunately, two other state actors have season tickets: Iran and North Korea. Iran's drone fleet is impressive and has caused other Gulf states' inventories to escalate (UAE, Kingdom of Saudi Arabia, Egypt, Iraq, Jordan, Israel) (Barrie, 2021). North Korea (NK) lies about its air power. However, one report states that NK will have drones with stealth capability. (Choi, 2021) Maybe. According to Datablog, the US has the most drones and is best equipped for warfare. China, of course, might dispute these statistics. (DATABLOG, 2012)[\[2\]](#)[\[3\]](#) However, carrying a big stick doesn't count anymore in the UAS's future military play without the will to use it.

Our Wildcat team is composed of some impressive SMEs. We divided the work into four sections. Section 1 covers Chemical, Biological, Radiation, Nuclear, Explosive (CBRNE) weapons and payloads delivered by unmanned vehicles. Here we look at the technologies and damage delivered by drones as mini weapons of mass destruction and disruption. Chapter 7 concentrates on Deception and how drones can be used in PSYOPS and INFOWAR. Section 2 concentrates on Directed Energy Weapons (DEW), projectiles payloads, satellite killers, port disrupters, and cyberweapons against CBRN assets. Section 3 looks at policy considerations, risk assessments of threats and vulnerabilities of drone-based WMDD / DEW, practical crime scene investigations for hot zones, and unique challenges of responding to bioterrorism and chemical threats and attacks delivered by drones. Our final Section 4 concludes with social networking implications and DRONESEC security and tracking tools of the trade.

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



Best

Randall K Nichols, DTM

Professor of Practice

Director, Unmanned Aircraft Systems –

Cybersecurity Certificate Program

UAS / CUAS / UUV Series Managing Editor / Co-Author

Kansas State University Polytechnic Campus &

Professor Emeritus – Cybersecurity, Utica College

LinkedIn Profile:

[www.linkedin.com/in/randall-nichols-2222a691](https://www.linkedin.com/in/randall-nichols-2222a691)

Illi nunquam cedunt.

“We Never Yield”

## Bibliography

Barrie, D. (2021, July 1). *Iran's-drone-fleet*. Retrieved from [https://iranprimer.usip.org/blog: https://iranprimer.usip.org/blog/2020/aug/20/irans-drone-fleet](https://iranprimer.usip.org/blog:https://iranprimer.usip.org/blog/2020/aug/20/irans-drone-fleet)

Choi, D. (2021, March). *could-north-korea-soon-field-advanced-stealth-drones/*. Retrieved from [https://thediplomat.com/: https://thediplomat.com/2021/03/could-north-korea-soon-field-advanced-stealth-drones/](https://thediplomat.com/:https://thediplomat.com/2021/03/could-north-korea-soon-field-advanced-stealth-drones/)

Colton, E. (2022, February 27). *putin-orders-nuclear-deterrent-forces-be-put-on-high-alert*. Retrieved from [https://www.foxnews.com/world/: https://www.foxnews.com/world/putin-orders-nuclear-deterrent-forces-be-put-on-high-alert](https://www.foxnews.com/world/:https://www.foxnews.com/world/putin-orders-nuclear-deterrent-forces-be-put-on-high-alert)

DATABLOG. (2012, August 3). *drone-stocks-by-country*. Retrieved from [https://www.theguardian.com/news/datablog/: https://www.theguardian.com/news/datablog/2012/aug/03/drone-stocks-by-country](https://www.theguardian.com/news/datablog/:https://www.theguardian.com/news/datablog/2012/aug/03/drone-stocks-by-country)

Facon, I. (2016, May). *A-Perspective-on-Russia-Proliferated-Drones*. Retrieved from [http://drones.cnas.org/:](http://drones.cnas.org/)

<http://drones.cnas.org/wp-content/uploads/2016/05/A-Perspective-on-Russia-Proliferated-Drones.pdf>

Malsin, B. F. (2022, February 12). *ukraines-use-of-armed-drones-could-offset-some-of-russias-enormous-military-advantage*. Retrieved from <https://www.wsj.com/articles/https://www.wsj.com/articles/ukraines-use-of-armed-drones-could-offset-some-of-russias-enormous-military-advantage-11644676305>

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/>.

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

[1] NPP metrics as of 04/22/2022: 36,627 downloads (with additional files) for commercial, military, educational, government,

and small business organizations, 1,362 institutions, 163 countries, 10,143 metadata pages, 7,641 abstract views, 48 social media, 28,019 usage, and 337 referrers! Our books are averaging 1,000 + downloads /month. These figures do not include Amazon sales, Kindle, or Tablet versions.

[2] DATABLOG data is interesting but dated. Accurate numbers by certain countries are not generously reported or are CLASSIFIED.

[3] We have issued clear warnings about China's drone capabilities in all uses in our textbooks. The Chinese New Silk Road Land and Sea Strategy employs UASs in the air and UUVs underwater in the South China Seas. PLAN's success has been documented. China also uses drones to enforce its social policies and ISR capabilities. They export more drones than any other country. It would be foolish to discount China as a secondary player supporting Russia in its illegal operations in Ukraine.

# Acknowledgements

Books such as this are the products of contributions by many people, not just the authors' musings. *Drone delivery of CBNRECY – DEW Weapons Emerging Threats Of Mini-Weapons Of Mass Destruction And Disruption (WMDD)* (R. K. Nichols & et al., 2022) 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 / security / OVRP committees at KSU. Their contributions were especially helpful in not releasing protected information, CLASSIFIED, or “DEEMED EXPORTABLE” categories. We will name only a few and miss some special friends whose contributions were noteworthy. For this, we sincerely apologize in advance and beg their 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 Aerospace and Technology Campus (AT) – Salina, Kansas (KSU-AT): Dr. Richard Myers, retiring President KSU; Dr. Kurt C. Barnhart, prior Associate Dean of Research and Executive Director of the UAS Research Laboratory KSU-AT; Dr. Alysia Starkey, Dean & CEO of KSU-AT; Dr. Terri Gaeddert, Associate Dean for Academics & Success (AT); Professor Troy Harding, Director of Academics, School of Integrated Studies (SIS) KSU-AT; Dr. Donald V. Bergen, prior Director of Graduate Studies KSU-AT; Fred Guzek, Professor and current Director of Graduate Studies KSU-AT; Dr. Kurt Caraway, Executive Director UAS, Dr. Mark J. Jackson, Professor, SIS KSU-AT; Dr. Saeed Khan, Professor, SIS KSU-AT; Dr. Mark J. Pritchard, Sr., Dr. Katherine Jones, KSU-AT Research and Library; Dr. Emily Finch at New Prairie Press and Pressbooks, Joel Anderson, KSU OVPR and

Research Director; and Brenda Andrews, Visual Communications Specialist.

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, Utica College; Professor of Practice and Cybersecurity Director, Joe Giordano, Utica College; Professor Harold B. Massey, Executive Director of UAS Drone Port, UAS Pilot, Dr. Amit K Maitra, Chairman and Founder of Borders and Beyond, Inc.; Dr. Jeff Bardin, President of Treadstone 71, a superior intelligence firm; Richard Lescalleet, VP Sales & marketing, Airship Technologies Group; Dr. Julie J.C.H. Ryan, SME in Intelligence and INFOSEC plus previous Wildcat author; and Dr. Dan J. Ryan, experienced SME / lawyer in intelligence, cryptography, and global defenses.

We owe a gratitude to Phillip E. Nielsen, author of *Effects of Directed Energy Weapons*, for guidance in Chapters 8 & 9. (Nielsen, 1994). Similarly, we thank Dr. Manual Eichelberger for his brilliant solutions to spoofing attacks on GPS and aircraft signals in his textbook *Robust Global Localization Using GPS and Aircraft Signals*. (Eichelberger, 2019)

No one could be prouder of the textbooks that my KSU Wildcat team has produced between 2018-and 2022. (Nichols & Mumm, *Unmanned Aircraft Systems in the Cyber Domain*, 2nd Edition., 2019) (Nichols & Sincavage, *Disruptive Technologies with Applications in Airline, Marine, and Defense Industries*, 2021) *Counter Unmanned Aircraft Systems Technologies & Operations*. 2020) (*Unmanned Vehicle Systems & Operations on Air, Sea & Land*.2021) (Nichols, R. K., & Mumm, H. C. (2019) *Unmanned Aircraft Systems (UAS) in the Cyber Domain* 2018)

Next comes our expanded Wildcat writing team: Dr. Suzanne Sincavage, Co-Chair of the Foundation for Biodefense Research, which is devoted and dedicated to promoting the biodefense intelligence tradecraft and developing a stronger biodefense community with government, industry, academia professional organizations; 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 a leadership expert 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 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 the UAS field operations; Dr. Mark Jackson, SME in UUV, naval architecture, and nanotechnologies, MSgt Jeremy Shay, Dragon student, COVID-19 expert, RET USAF, Fabrication Production Manager, Spirit AeroSystems; Joel Coulter, President, Mobile Sciences Consortium, LLC; Bart Shields, Inventor and CTO of Olympus Sky, Inc; Mike Monnik, CEO of DRONESEC and his XO Arison Neo; Robert McCreight, a specialist in US Army Special Operations and National Security Expert in Defense programs associated with nuclear and biological defense matters; and William Slofer, Dragon and SME in radar and Hypersonic technologies. We were fortunate to have Brenda Andrews build our cover image with Dr. Sincavage and Professor Carter. Brenda is CEO of Ikonology Studios and an incredibly talented artist. Many others have helped our team write this important book. We appreciate all of their contributions.

The Wildcat team especially thanks Assistant Professor Dr. Emily Finch, Scholarly Communication Librarian, for her expert guidance on the New Prairie Press and Pressbooks publishing journey.

Professor Randall K. Nichols is Managing Editor/author/co-author with his Wildcat Team of twelve textbooks and developer of six master's and Certificate programs in Cybersecurity, Intelligence, Forensics, and UAS/CUAS/UUV at Utica College and Kansas State University. He has five decades of experience.

Finally, Mrs. Montine Nichols, my God-given Angel of 38 years, deserves a commendation for her help on the final drafts and copy edit work for our book and a living (surviving) this long with a real Dragon who hardly sleeps.

Randall K Nichols, DTM  
Professor of Practice  
NIST PSCR UAS 3.0 Technical Lead – Cyber Challenge  
ASSURE44 KSU UAS – Cybersecurity Technical Lead  
Director, Unmanned Aircraft Systems (UAS) – Cybersecurity  
Graduate Certificate Program  
Managing Editor / Author / Co-Author of UAS/CUAS/UUV  
Textbook Series  
Kansas State University Aerospace & Technology Campus, Salina,  
KS &  
Professor Emeritus – Graduate Cybersecurity & Forensics, Utica  
College

### Bibliography

Eichelberger, M. (2019). *Robust Global Localization Using GPS and Aircraft Signals*. ETH Zurich: Free Space Publishing – DISS ETH 26089.

Nichols, R. K. (2020). *Counter Unmanned Aircraft Systems Technologies & Operations*. Manhattan, KS: [www.newprairiepress.org/ebooks/31](http://www.newprairiepress.org/ebooks/31).

Nichols, R. K. (2022). *DRONE DELIVERY OF CBNRECy – DEW WEAPONS, Emerging Threats of Mini-Weapons of Mass Destruction and Disruption (WMDD)*. Manhattan, KS: New Prairie Press #TBA.

Nichols, R. K., & Mumm, H. C. (2019). *Unmanned Aircraft Systems in the Cyber Domain*, 2nd Edition. Manhattan, KS: [www.newprairiepress.org/ebooks/27](http://www.newprairiepress.org/ebooks/27).

Nichols, R. K., & Sincavage, S. M. (2021). *Disruptive Technologies*



*with Applications in Airline, Marine, and Defense Industries.* Manhattan, KS: New Prairie Press #38.

Nichols, R., & Ryan, J. M. (2020). *Unmanned Vehicle Systems & Operations on Air, Sea & Land.* Manhattan, KS: New Prairie Press #35.

Nielsen, P. E. (1994). *Effects of Directed Energy Weapons.* Dayton, OH: USAF.

# List of Series Contributors

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



Randall K. Nichols is a Professor of Practice in Unmanned Aircraft Systems (UAS) – Cybersecurity at Kansas State University Aerospace and Technology Campus 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 **eleven** best-selling textbooks. Nichols

has provided counsel to the United States government and is certified as a federal subject matter expert (SME) in cryptography and computer forensics. His most recent work involves creating masters 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, a public company acquired 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 Moo Duc Kwan Tae Kwon Do and a permanent rank of 2nd Dan Black Belt (D). In Corpus Christi, TX, he taught self-defense courses for women. In 1994,

Nichols was elevated to Ring Judge for the National Tae Kwon Do Championships held in San Antonio, TX.

Managing Editor / Co-author:

***Disruptive Technologies with Applications in Airline, Marine, Defense Industries (2021)***

Available as a free eBook at: <https://newprairiepress.org/ebooks/38/>

***Unmanned Vehicle Systems & Operations on Air, Sea, Land (2020)***

Available as a free eBook at: <https://www.newprairiepress.org/ebooks/35/>

***Counter Unmanned Aircraft Systems Technologies and Operations (2020)***

Available as a free eBook at: <https://www.newprairiepress.org/ebooks/31/>

***Unmanned Aircraft Systems in Cyber Domain: Protecting USA's Advanced Air Assets, 2nd Edition (2019)***

Available as a free eBook at: [https://www.newprairiepress.org/ebooks/27](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 [profkrnichols@ksu.edu](mailto:profkrnichols@ksu.edu).

\*Direct all inquiries about this book to Prof. Randall K. Nichols at [profkrnichols@ksu.edu](mailto:profkrnichols@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 of 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. He was 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." 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, including contracts for UAV research and creating an advanced multiple fuel system that 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

the 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](mailto:hans@hansmumm.com). [www.HansMumm.com](http://www.HansMumm.com)

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



Wayne Lonstein holds a Bachelor of Arts Degree in Political Science from Wilkes University, a Bachelor of Science Degree in Cyber Forensics and Information Security from Syracuse University – Utica College, A Master of Science Degree in Homeland Security with a concentration in Information Security from The Pennsylvania State University and a Juris Doctor Degree from Pace University School of Law. Additionally, he holds a CISSP Certification from The Pennsylvania State University. He is a member of the state bars of New York, New Jersey, Massachusetts, and Pennsylvania, as well as being admitted to over 30 United States District Court Bars, The Court of Veterans Appeals, the 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 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 is a member of Signal law PC, the Co-Founder, and CEO of VFT Solutions, a member of the Forbes Technology Council. He 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 / 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 at the U.S. National Defense University. Before that, she was tenured faculty at 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 an 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 a Military Intelligence Officer with the Defense Intelligence Agency. Upon leaving government service, she worked in various positions, including systems engineer, consultant, and senior staff scientist with Sterling Software, Booz Allen & Hamilton, Welkin Associates, and TRW/ESL, supporting various 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, focusing 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 counterterrorism, counterintelligence, and cybercriminal 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 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 Wilmington University. Ms. Carter holds an MSc in 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, working full time. He has provided editing skills for Professor Nichols for ten 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, and MBAA from Embry-Riddle Aeronautical University, and a Ph.D. in educational administration from Indiana State University.

Dr. Barnhart's Research plan focuses on aviation psychology and Human Factors and on integrating Unmanned Aircraft Systems into the National Airspace System. His industry experience includes working as an R&D inspector with Rolls Royce Engine Company. He worked on the RQ-4 Unmanned Reconnaissance Aircraft development program and served 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. 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, etc.

**CPT John-Paul Hood USA (Co-Author)**



CPT John-Paul Hood is a researcher focused on developing future counter unmanned aircraft technologies, theories, and best practices for government and civilian applications. CPT Hood has commanded in the US Army Field Artillery with a background specializing in coordinating and delivering conventional/smart munitions and achieving desired battlefield effects by integrating 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 of 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, an M.L.S. from the 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 the library director and associate professor in 2007 and 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 over 30 years of experience in the military, industry, and academia. He currently serves as Development Director for Kansas State University within the Office of Research Development (ORD). Before 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-and 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. 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 (FIU), and 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, and educational and operational environments.

His awards include the Defense Superior Service Medal; Bronze Star; Meritorious Service Medal with four gold stars instead of the 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 instead of the second award; Armed Forces Expeditionary Medal; Southwest Asia Service Medal with three stars instead of additional awards; Global War on Terrorism Service Medal; Sea Service Deployment Ribbon with three stars instead of additional awards; Overseas Deployment Ribbon with one device; Marine Security Guard Ribbon; Kuwaiti Liberation Medal (Saudi Arabia); Kuwaiti Liberation Medal (Kuwait).



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



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

Jeremy currently serves as a Senior Principal Manufacturing Engineer at Northrop Grumman. He recently retired from the United States Air Force as a Senior Master Sergeant with 26 years of service. 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 an I.C.I. prize for achievement, he studied for a degree in mechanical and manufacturing engineering at Liverpool Polytechnic. He spent periods in the 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. Subsequently, he was employed by Unicorn Abrasives' Central Research & Development Laboratory (Saint-Gobain Abrasives' Group) as a materials technologist, then technical manager, responsible for product and new business development in Europe university liaison projects concerned with abrasive process development. Doctor Jackson then became a 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 several research grants to develop innovative manufacturing processes. He was jointly awarded an Innovative Manufacturing Technology Centre from the Engineering and Physical Sciences Research Council in November 2001. In 2002, he became an 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 a 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 encyclopedia's first edition was published in 2009, and the second edition was published in 2018. In March 2017, the degree of Doctor of Science (D. Sc.) in mechanical engineering was conferred upon Dr. Jackson in absentia by the congregation for sustained contributions made in mechanical engineering and advanced manufacturing over 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 his great-grandfather established 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. He was also responsible for validating the Laboratory LIMS and Millenium32 software. The validation encompassed network security and disaster recovery.

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

**Kurt J. Carraway, Col, USAF (Ret) (Foreword)**



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, including 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. 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 before 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 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 a serial entrepreneur, long-time innovator, deeply technical product architect, and has over 25+ years of technical and engineering management. He has designed systems from concept to deployment for various verticals. Still, He 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 designed multiple MAC layer protocols, including designing and implementing a Wi-Max-like protocol (WCOPP) in the late 90s 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 engineering aspects, 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 designing and developing embedded systems, including mission and safety-critical systems. Bart has focused the past six years entirely on cybersecurity and solving many issues plaguing security today, with simple and elegant solutions built around his highly innovative technology, AKM.

**Dr. Suzanne Sincavage, (Co-Author)**



Executive Summary

On April 20, 2021, Dr. Suzanne Sincavage founded and Co-Chairs the **Foundation for Biodefense Research**, a non-profit 501 (c)(3) devoted and dedicated to promoting the biodefense tradecraft and developing a stronger biodefense community with government, industry, academia professional organizations, and



individuals who assess, develop, and apply biodefense intelligence research to address national security challenges.

From 2020- 2021, Dr. Suzanne Sincavage served as the Executive Director for the Institute for Biodefense Research (IBR). A nonprofit devoted to advancing the science of microbial forensics.

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

Dr. Sincavage received her Ph.D. in Public Health and Epidemiology with a 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, and oncology, hematology, urology, and immunology.

Dr. Sincavage is an SME for the National Institute of Science and Technology (NIST), 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, served as Executive Director of the La Jolla Symphony & Chorus.

Dr. Sincavage holds certifications:

SAM (CCR); SBA 8 (m)

DD 2345 Military Critical Technical Data Agreement

D

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

**Troy Harding Associate Dean (Foreword)**



Troy Harding is a Professor in computer systems technology and Department Head of Integrated Studies at Kansas State University Salina Aerospace and Technology Campus. Professor Harding earned a bachelor's degree in Chemistry and Computer Science from Bethany College and a master's degree in Chemistry from the University of Virginia. Before joining K-State, he worked as Technical Director at Aquarian Systems in Orange, VA, Programmer/Analyst and Network Coordinator at Associated Colleges of Central Kansas, and Director of I.S. at Kansas Wesleyan University. At K-State, he has received the Marchbanks Award for

Teaching Excellence, the McArthur Faculty Fellow Award, and the endowed McCune & Middlekauff Fellowship.

**Robert McCreight (Co-Author)**



Dr. McCreight spent 27 years in federal service and 23 years concurrently in US Army Special Operations, working on various national security projects and special defense programs associated with nuclear, chemical, and biological defense matters. He has supported and served as a periodic advisor on the Chemical Weapons Treaty and Biological and Toxin Weapons Convention during a career at the State Department, along with programs enabling satellite verification of arms control treaty compliance. He helped draft HSPD-10 and contributed to the issuance of HSPD-21, also serving as a contributing White House assistant on nuclear policy and strategy exercises. Upon retirement, he has published

on advanced weapons systems, WMD issues, crisis management, emergency response issues, and neuroscience topics. Periodically he has been a guest lecturer at NDU on future weapons systems and taught graduate school at seven different universities during the last 15 years in his designated areas of interest, on national security issues, CBRN matters, and emerging convergent technology threats.

**Brenda Alexandra Andrews (Visual Communications Specialist)**



Visual Communications Specialist / International Exhibition Artist

Led artistic direction, exhibition space planning, construction oversight, academic programming, and cross-functional teams. Developed programs, symposiums, lectures, and philanthropic ventures. She secured educational advancement and scholarships.

- Re-Envisioning, A World Beyond Borders (San Diego).  
Showcase Installation featuring real-time cell phone and

digital photo imagery from participants worldwide- over 5,000 entries. Images were transmitted wirelessly, uploaded to a global website, and showcased as an Art & Technology Installation at International Art Fair. Partners: QUALCOMM, SDUSD, UCSD, KPBS, Worldwide Community.

- Mapping Rockwell's World (Orange County). International project using Conextent technologies brings Rockwell International Family together in real-time video lectures. Culminated in the large-scale installation of painted map abstractions displayed a globally interconnected world. Installation became a corporate holiday card and annual report cover. Partners: Rockwell, Conextant, OCMA, and Visionaries.
- Art of the Book (Orange County | San Diego Founder of Artist in Residence Teaching Program for OCMA and Orange County high schools. Lectures and in-studio art projects. Culminating in Museum Exhibition practices, awards, and scholarship programs. Partners: OCMA, Dana Hills High School, Ryman Arts (Walt Disney Imagineering), various established Artists. Repeated in San Diego County- SDMA.
- Exhibition driven programming for OCMA, Orange County Museum of Art; SDMA: LACMA; Delaware Contemporary Museum, and numerous University Museum spaces. Focused on fundraising and grant support.
- International Exhibition Artist

**Mike Monnik (Co-Author)**



As CEO at DroneSec, Mike enables organizations to protect people and drones from malicious drones and people. National security roles have included the Australian Department of Defense and BAE Systems. He has lectured on Computer Crime & Digital Forensics at Deakin University and sits on the IT Advisory board. Mike crystallized his knowledge as a consultant conducting offensive technical cyber and physical security engagements. Mike has led high-performing teams in Red Team, Penetration Testing, Open-Source Intelligence, and Drone engagements in a variety of challenging environments.

Mike is a long-time global conference speaker and advocate for drone security and has presented to the FBI, INTERPOL, NSW Government, and European Commission at closed-door presentations. Mike has experience coordinating large teams, such as the Table-Top Threat exercise for the 2018 Commonwealth Games. He has several hall-of-fame contributions for protecting the technology and customers of organizations such as DJI, Parrot, AirData, Aloft, and Fortem Technologies.

Specializing in Red Team operations, Mike has used drones in

simulations against critical infrastructure, government buildings, and private facilities to highlight the potential threats and evaluate their response. Mike has trained hundreds of students in offensive and defensive drone security measures, counter-drone operations, and UAS Threat Intelligence gathering. Mike continues to lead DroneSec in building drone threat intelligence and drone security software to protect the future of mobility, delivery, and transport.

**William Slofer (Co-Author)**



Bill is an IT Project Management and security professional with over 30 years of IT and management experience. He holds PMP, Scrum, and Scaled agile certifications with expertise in application development, systems/infrastructure integration, high-speed video/data communications, and IT security. His technical and management expertise has been employed by federal, state, and local governments and various industries in the private sector. Bill's strong management, interpersonal, and communications skills have enabled him to lead high-impact teams nationally and in Europe, South/Central America, and Asia. Bill is a member of Infragard and has career accomplishments involving implementing corporate-wide fortifications for perimeter defense, Lateral Segmentation, and Data Loss Prevention measures to protect sensitive data assets.

Formal education includes:

- MS, Cybersecurity / Cyber Terrorism
- MS, Management, Management Information Systems

BS, Business Administration / Computer Science



# Abbreviations and Acronyms

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

|          |  |
|----------|--|
| ABM      | Anti-ballistic missile   |
| A/C      | Aircraft (Piloted or unmanned) also A/C  |
| ACOUSTIC | Detects drones by recognizing unique sounds produced by their motors.  |
| A/D      | Attack / Defense Scenario Analysis   |
| ADS      | Air Defense System (USA) / Area Denial System  |
| ADS-B    | Automatic Dependent Surveillance-Broadcast systems   |
| A/C FD   | Aircraft flood denial  |
| AFRL     | Air Force Research Lab   |
| A-GPS    | Assisted GPS   |
| AGL      | Above ground level   |
| AHI      | Anomalous Health Incidents   |
| 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) |
| AIS      | Automated Identification System for Collision Avoidance  |
| AMS      | Autonomous Mobile Sword (SCREAMER) uses sound to disrupt the brain before cutting the enemy to pieces.   |
| AO       | Area of Operations   |
| AOA      | Angle of Arrival of signals to GPS receivers / Angle of Attack   |
| APC      | Armored personnel carrier  |
| APDS     | Armor-piercing discarding sabot projectile   |

|                   |   |
|-------------------|---|
| APFSDS projectile | Armor-piercing fin-stabilized discarding sabot    |
| AR                | Augmented reality                                 |
| ARW               | Anti-radiation weapons                            |
| ATC               | Air Traffic Control / Air traffic Control Signals |
| ATSAW             | Air Traffic Situational Awareness                 |
| AUV               | Autonomous underwater vehicle                     |

B&B            Branch & bound

*Bandwidth* is 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 systems.

BC            Ballistic Coefficient

BEAR        Battlefield Extraction-Assist Robot

Black Swan    Black Swan Event- A black swan is an unpredictable event 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

BPAUV        Battlespace Preparation Autonomous Underwater Vehicle

BSL-4        Biosafety Level #

BTWC        Biological & Toxin Weapons Convention

BVLOS        Beyond Visual Line-of-Sight operations

BVR        Beyond visual range

BW        Biological weapons

BYOD        Bring your device

c            Speed of light ~ (3 x 10<sup>8</sup> m/s) [186,000 miles per sec]

in vacuum named after *Celeritas*, the Latin word for speed or velocity.

|          |  |
|----------|--|
| C-CLAW   | Combat Laser assault weapon  |
| cs       | speed of sound (344 m/s) in air  |
| C2 / C2W | Command and control / Command and Control Warfare  |
| C3       | Command, control, communications   |
| 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       |
| C5I      | Command, control, communications, computers, Collaboration & Intelligence  |
| CA       | Collision Avoidance / Clear Acquisition (GPS) / Cyber Assault (aka CyA)  |
| C/A      | Civilian acquisition code for GPS  |
| CAA      | Control Acquisition cyber attack   |
| CAS      | Close Air Support / Common situational awareness   |
| CBRN     | Chemical, Biological, Radiation & Nuclear critical infrastructure facilities   |
| CBRNE    | Chemical, Biological, Radiation, Nuclear & Explosives attacks critical infrastructure facilities or assets           |
| CBRNECy  | Chemical, Biological, Radiation, Nuclear, Explosives & Cyber-attacks on critical infrastructure facilities or assets |
| CBW      | Chemical, Biological Weapons   |
| CC&D     | Camouflage, Concealment, and Deception   |
| CCTV     | Closed Circuit Television  |
| CD       | Charge diameters   |

|           |  |
|-----------|--|
| Cd        | Drag coefficient   |
| CDC       | Center for Disease Control   |
| CDMA      | Code division multiple access  |
| <b>CD</b> | <b><i>Collective detection maximum likelihood localization approach</i></b> (Eichelberger, 2019) |
| CEA       | Cyber-electromagnetic activities   |
| CEP       | Circular error probable  |
| CETC      | Chinese Electronics Technology Group Corporation   |
| CEW       | Cyber electronic warfare / Communications electronic warfare                                     |
| CGA       | Coast Guard Administration – Singapore   |
| CHAMP     | Counter-Electronics High Power Microwave Advanced Missile Project                                |
| CIA       | Confidentiality, Integrity & Availability ( standard INFOSEC paradigm)                           |
| CI / CyI  | Critical Infrastructure / Cyber Infiltration   |
| CIA       | Confidentiality, Integrity, Availability / Central Intelligence Agency                           |
| CIS       | Critical Infrastructure Sector   |
| CJNG      | Cártel de Jalisco Nueva Generación   |
| CM / CyM  | <i>Countermeasure</i> / Cyber Manipulation   |
| CMADS     | China's Microwave Active Denial System   |
| C/NA      | Communication / Navigation Aid   |
| CNA       | Computer network attack  |
| CND       | Computer network deception   |
| CNE       | Computer network exploitation  |
| CNO       | Computer network operations  |
| CNS       | Central nervous system   |
| COMINT    | Communications intelligence  |
| COMJAM    | Communications Jamming   |
| COMINT    | Communications Intelligence  |
| COMSEC    | Communications Security  |
| CONOP(S)  | Concepts of Operations   |
| CONV      | Convergent Technology Dynamics   |

CONV-CBRN Convergent Technology Dynamics – Chemical, Biological, Radiation & Nuclear

|          |  |
|----------|--|
| COP      | Common operating picture                                     |
| COTS     | Commercial off-the-shelf                                     |
| CPS      | Cyber-physical systems                                       |
| CR       | Conflict Resolution / Close range / Cyber Raid (aka CyR)     |
| CSI      | Crime scene investigation                                    |
| CT       | Counter-Terrorism / Counter-Terrorism Mission                |
| CTN      | Course time navigation                                       |
| C-UAS    | Counter Unmanned Aircraft Systems (defenses/countermeasures) |
| CUAV     | Counter Unmanned Aircraft Vehicle (defenses/countermeasures) |
| CUES     | Code for unplanned encounters at sea                         |
| CW / CyW | Cyber Warfare  |
| CWC      | Chemical Weapons Convention                                  |
| CWMD     | Countering Weapons of Mass Destruction                       |

#### Community

CYBER WEAPON – Malicious Software and IT systems that, through ICTS networks,

manipulate, deny, disrupt, degrade, or destroy targeted information systems or

networks. It may be deployed via computer, communications, networks, rogue

access points, USBs, acoustically, electronically, and airborne/underwater

unmanned systems & SWARMS. Alternatively, cyber weapons:

1. A campaign that may combine multiple malicious programs for espionage, data theft, or sabotage.
2. A stealth capability that enables undetected operation within the targeted system over an extended time.
3. An attacker with apparent intimate knowledge of details for the workings of the targeted system.

4. A special type of computer code to bypass protective cybersecurity technology.

#### Danger Close

Definition [www.benning.army.mil/infantry/magazine/issues/2013/May-June/Myer.html](http://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 *fires* which indicates that friendly forces are within close proximity of the target.

|           |  |
|-----------|--|
| DARPA     | Defense Advanced Research Projects Agency                  |
| Dazzle    | Cause temporary blindness with Laser                       |
| DCPA      | Distance between vessels approaching CPA                   |
| D&D       | Denial & deception   |
| DDD       | Dull, dangerous, and dirty                                 |
| D/D/D     | Destruction, Disruption, Deception                         |
| DDOS      | Distributed Denial of Service cyber attack                 |
| DEFCON    | Defense condition  |
| DEW       | Directed energy weapons (also, DE)                         |
| DF        | Direction-finding  |
| DPRK      | Democratic People’s Republic of Korea                      |
| DTRA      | Defense Threat Reduction Agency                            |
| DUST      | Dual-use Science & Technology threat                       |
| EA        | Electronic Attack  |
| EBO       | Effects-based operations                                   |
| ECCM / EP | Electronic counter-countermeasures / Electronic Protection |
| ECD       | Dr. Manuel Eichelberger’s advanced implementation          |

of CD to detect & mitigate spoofing attacks on GPS or ADS-B signals (Eichelberger, 2019)

|       |   |
|-------|---|
| ECM   | Electronic countermeasures                      |
| ELINT | Electronic Intelligence                         |
| EM    | Electromagnetic waves                           |
| EMC   | Electromagnetic compatibility                   |
| EMD   | Electromagnetic deception                       |
| EMF   | Electromagnetic field                           |
| EMI   | Electromagnetic interference                    |
| EMP   | Electromagnetic pulse – electromagnetic energy. |
| EMR   | Electromagnetic radiation                       |
| EMS   | Electromagnetic spectrum                        |
| EO    | Electro-optical system                          |
| EW    | Electronic warfare                              |

[Legacy EW definitions: EW was classically divided into (Adamy D., EW 101 A First Course in Electronic Warfare, 2001):

- ESM – Electromagnetic Support Measures – the receiving part of EW;
- ECM – Electromagnetic Countermeasures – jamming, chaff, flares used to interfere with operations of radars, military communications, and heat-seeking weapons;
- ECCM -Electronic Counter-Counter Measures – measures are taken to design or operate radars or communications systems to counter the effects of ECM.[\[1\]](#)

Not included in the EW definitions were Anti-radiation Weapons (ARW) and Directed Energy Weapons (DEW).

USA and NATO have updated these categories:

- ES – Electronic warfare Support (old ESM) to monitor the R.F. environment;
- EA – Electronic Attack – the old ECM includes ASW and D.E. weapons; to deny, disrupt, deceive, exploit, and destroy adversary electronic systems.

- EP – Electronic Protection – (old ECCM) (Adamy D., EW 101 A First Course in Electronic Warfare, 2001) to guard friendly systems from hostile attacks.[\[2\]](#)

ES is different from Signal Intelligence (**SIGINT**). SIGINT comprises Communications Intelligence (**COMINT**) and Electronic Intelligence (**ELINT**). All these fields involve the receiving of enemy transmissions. (Adamy D., EW 101 A First Course in Electronic Warfare, 2001)

|             |   |
|-------------|---|
| FAA         | Federal Aviation Agency   |
| FHSS        | frequency-hopping spread spectrum   |
| FIRES       | definition (US DoD – JP 3-0) is the use of weapon systems to create a specific lethal or nonlethal effect on a target.  |
| FPS         | Feet Per Second   |
| GS          | Ground Station  |
| GCS         | Ground control station  |
| GPS         | Global Positioning System (US) <a href="#">[3]</a> (USGPO, 2021)  |
| GNSS        | Global Navigation Satellite System (GPS, GLONASS, Galileo, Beidou & other regional systems)   |
| GNU         | GNU / Linux Operating system  |
| GPS         | Global Positioning System / Geo-Fencing   |
| GPS/INS     | uses <a href="#">GPS</a> satellite signals to correct or calibrate a solution from an <a href="#">inertial navigation system</a> (INS). The method applies to any GNSS/INS system |
| GRU         | Russian military intelligence branch  |
| GSFD        | Ground station flood denial   |
| GSM         | Global system for mobile communications   |
| GTA         | Ground-to-Air Defense   |
| Hard damage | DEW complete vaporization of a target   |
| HAPS        | High Altitude Platforms (generally for wireless communications enhancements)  |
| HCM         | Hypersonic cruise missile   |
| HGV         | Hypersonic glide vehicle  |
| HEAT        | High-explosive anti-tank warhead  |
| HEL         | High energy Laser   |



|          |  |
|----------|--|
| HOW      | Hand-over-word satellite data timestamp defined in (IS-GPS-200G, 2013) |
| HTV      | Hypersonic test vehicle  |
| HUMINT   | Human Intelligence   |
| HVM      | Hostile vehicle mitigation   |
| IAEA     | International Atomic Energy Agency                                     |
| IC       | Intelligence community ~ 17 different agencies                         |
| ICBM     | Intercontinental ballistic missile                                     |
| ICS      | Internet Connection Sharing / Industrial control systems               |
| ICT      | Information & Communications Technology                                |
| ICTS     | Information & Communications Technology Services                       |
| ID       | Information Dominance / Inspection and Identification / Identification |
| IDEX     | International Defense Exhibition and Conference                        |
| IDS      | Intrusion detection system   |
| IED      | Improvised Explosive Device  |
| IFF      | Identify Friend or Foe   |
| IIIM     | International, Impartial, and Independent Mechanism                    |
| IMU      | Inertial Measurement Unit  |
| IND      | Improvised nuclear device  |
| INS      | Inertial navigation system   |
| INFOSEC  | <i>Information Security</i>  |
| IO /I.O. | Information Operations   |
| IoT      | Internet of things   |
| IIoT     | Industrial Internet of things  |
| IP       | Internet protocol  |
| IR       | Infrared   |
| IS       | Information security / Islamic State                                   |
| ISIS     | <i>Islamic State of Iraq and al-Sham (ISIS)</i>                        |
| ISR      | Intelligence, Reconnaissance and Surveillance UAS                      |
| Platform |  |

ISTAR Intelligence, surveillance, target acquisition, and reconnaissance

IT Information Technology

IT/OT Information Technology/ Operational Technology

ITE Installation, Training, Expense

IW Information Warfare

JIM Joint Investigative Mechanism

JSR Jamming-to-signal ratio

KE Kinetic energy

KEW Kinetic energy weapon

K'IHAP Short Shout in Tae Kwon Do

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 light sources in that it emits light [coherently](#), spatially, and temporally. [Spatial coherence](#) allows a laser to be focused on a tight spot, enabling laser cutting and lithography applications 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 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)

LaWS Laser weapon system

LLTR Low-level transit route

LM or L.M. Loitering munitions

LMM Lightweight Multi-role Missiles

LOS Line of sight

LPI Low Probability of Intercept

**LRAD Long Range Acoustic Device / Long-Range Area Denial [4]**

|           |   |
|-----------|---|
| Mach 1    | Speed of sound, 761.2 mph                           |
| MAD       | Mutually assured destruction                        |
| M-ATV     | Mine-resistant ambush-protected vehicle             |
| MAME      | Medium altitude medium endurance                    |
| MASER     | Microwave Amplification Stimulated Emission of      |
| Radiation |   |
| MAST      | Micro Autonomous Systems & Technology               |
| MEDUSA    | (Mob Excess Deterrent Using Silent Audio)           |
| MEMS      | micro-electro-mechanical systems                    |
| MIM       | Man-in-middle attack                                |
| MIRV      | Multiple independently targetable reentry vehicles  |
| ML        | Machine learning                                    |
| MLAT      | Multilateration System                              |
| MND       | Ministry of National Defense                        |
| MOA       | Minute of angle in degrees                          |
| MOPP      | Mission Oriented Protective Posture (MOPP) Gear     |
| MRVs      | Multiple Re-entry Vehicles                          |
| mTBI      | mild Traumatic Brain Injury                         |
| MTI       | Moving target indicator                             |
| MUM-T     | Manned-unmanned teaming (MUM-T)                     |
| NAS       | National Academy Of Sciences                        |
| NATO      | North Atlantic Treaty Organization                  |
| NEB       | New Economic Block soldier                          |
| NERC      | North American Electric Reliability Corporation     |
| NDM       | Navigation data modification spoofing attack        |
| NGO       | Nongovernmental organization                        |
| NIEHS     | National Institute of Environmental Health Sciences |
| NKW       | non-kinetic warfare                                 |
| NV        | Neurological vulnerability                          |
| OODA      | Observe, Orient, Decide, and Act decision loops     |
| OPCW      | Organization for the Prohibition of Chemical        |
| Weapons   |   |
| OPSEC     | Operational Security                                |
| OSINT     | Open-source intelligence                            |
| OTH       | Over-the-horizon                                    |

PETMAN      Humanoid robot developed for US Army -Protection  
Ensemble Test Mannequin

Phigital      Digital and human characteristics & patterns  
overlap

PII      Private identifying information and credentials

PLA      Peoples Liberation Army ( Chinese)

PLAN      Peoples Liberation Army & Navy (Chinese)

POV      Point of view

PRN      Pseudo-Random Noise

PSYOPS      Psychological warfare operations

RC      Radio communications signals

RCS      Radar cross-section

RDD      Radiological dispersion device

RF      Radio Frequency

RF-EMF      Radiofrequency – Electromagnetic field

RFID      Radio-frequency identification (tags)

RID      Remote identification of ID

RIMPAC      Tim of the Pacific

RN      Ryan-Nichols Qualitative Risk Assessment

RNRA      Ryan – Nichols Attack / Defense Scenario Risk

Assessment for Cyber cases

ROA      Remotely operated aircraft

ROC      Republic of China

ROV/ROUV      Remote operating vehicle / Remotely operated  
underwater vehicle

RPA      Remotely piloted aircraft

RPAS      Remotely piloted system

RPV      Remotely piloted vehicle

RSS      Received signal strength

RV      Re-entry vehicle

SA      Situational Awareness

SAA      Sense and Avoid

SAM      Surface to Air missile

SAR      Synthetic aperture radar

SATCOM      Satellite communications

|                 |  |
|-----------------|--|
| SBLM            | Submarine-launched ballistic missile                 |
| SCADA           | Supervisory Control and Data Acquisition systems     |
| SCS             | Shipboard control system (or station) / Stereo       |
| Camera System / | South China Seas                                     |
| SDR             | Software-defined radio                               |
| SEAD            | Suppression of enemy defenses                        |
| SECDEF          | Secretary of Defense (USA)                           |
| SIC             | Successive Signal Interference Cancellation          |
| SIGINT          | Signals Intelligence                                 |
| Signature       | UAS detection by acoustic, optical, thermal, and     |
| radio /radar    |  |
| SMART           | Strategic Arms Reduction Treaty                      |
| S/N             | S / N = is one pulse received signal to noise ratio, |
| dB:             | Signal to Noise ratio at HAPS receiver (also, SNR)   |
| Soft damage     | DEW disruption to a UAS computer                     |
| SOCOM           | U.S. Army Special Operations Command                 |
| SOLAS           | Safety of Life at Sea (International Maritime        |
| Convention)     | [safety conventions]                                 |

**Spoofing is A Cyber-weapon attack that generates false signals to replace valid ones. GPS Spoofing is an attack to provide false information to GPS receivers by broadcasting counterfeit signals similar to the original GPS signal or by recording the original GPS signal captured somewhere else at some other time and then retransmitting the signal. The Spoofing Attack causes GPS receivers to provide the wrong information about position**

**and time.** (T.E. Humphrees, 2008) (Tippenhauer & et.al, 2011)

Spoofing Alt Def: A Cyber-weapon attack generates false signals to replace valid ones.

SSBN Strategic nuclear-powered ballistic missile submarine

SSLT Seamless satellite-lock takeover spoofing attack

sUAS Small Unmanned Aircraft System

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

Taiwan ROC Taiwan is officially the Republic of China

|            |  |
|------------|--|
| TCAS       | Traffic collision avoidance system   |
| ToF        | Time of flight   |
| TTF        | Time to first fix (latency)  |
| TDOA       | time difference of arrival   |
| TEAM (UAS) | High-level, a 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. |
| TDOA       | Time difference of arrival   |
| TNT        | Trinitrotoluene  |
| TO         | Theater of Operations  |
| TOA        | Time of arrival  |
| TRANSEC    | Transmission security  |
| TTPs       | Tactic, Technique, and Procedures  |
| Tx         | Transmit signal  |
| UA         | Unmanned Aircraft (non-cooperative and potential intruder)   |
| UAM        | Urban Air Mobile (vehicle)   |
| UAS        | Unmanned aircraft system   |
| UAS-p      | UAS pilot  |
| UAV        | Unmanned aerial vehicle / Unmanned autonomous vehicle.   |
| UAV-p      | UAV pilot  |
| UCAR       | Unmanned combat armed rotorcraft   |
| UCARS      | UAV common automated recovery system   |
| UCWA / UA  | Unintentional cyber warfare attack   |
| UGCS       | Unmanned Ground Control Station  |
| UGS        | Unmanned ground-based station  |
| UGT        | Unmanned ground transport  |
| UGV        | Unmanned ground vehicle  |
| UHF        | Ultra-high frequency   |
| USV        | Unmanned Surface Vessel  |
| UUV        | Unmanned underwater vehicle  |
| VR         | Virtual reality  |
| VLOS       | visual line of sight   |

|      |  |
|------|--|
| VTOL | Vertical take-off and landing                          |
| VX   | Deadly nerve agent                                     |
| WFOV | Wide field of view                                     |
| WFUL | Wake Forrest University Laboratory                     |
| WLAN | Wide Local area network                                |
| WMD  | <b>Weapons of Mass Destruction</b>                     |
| WMDD | <b>Mini-Weapons of Mass Destruction and Disruption</b> |

## Special Definitions

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

This contrasts with *symmetric warfare*, where two powers have comparable military power and resources and rely on similar tactics, differing only in details and execution. (Thomas, 2010)

## Definitions [5]

Acquisition – Acquisition is the process in a GPS receiver that finds the visible satellite signals and detects the delays of the PRN sequences and the Doppler shifts of the signals.

Circular Cross-Correlation (CCC) – In a GPS classical receiver, the circular cross-correlation is a similarity measure between two vectors of length N, circularly shifted by a given displacement d:

$$C_{\text{xcorr}}(\mathbf{a}, \mathbf{b}, d) = \sum_{i=0}^{N-1} a_i \cdot b_{i+d \bmod N}$$

The two vectors are most similar at the displacement d, where

the sum (CCC value) is maximum. The vector of CCC values with all N displacements can be efficiently computed by a fast Fourier transform (FFT) in  $\mathcal{O}(N \log N)$  time. [6](Eichelberger, 2019)

Coarse-Time Navigation (CTN) is a snapshot receiver localization technique measuring sub-millisecond satellite ranges from correlation peaks, like classical GPS receivers. (IS-GPS-200G, 2013) [See also expanded definition above.]

Collective Detection (CD) is a maximum likelihood snapshot receiver localization method, which does not determine the arrival time for each satellite, but rather combines all the available information and decides only at the end of the computation. This technique is critical to the (Eichelberger, 2019) invention to mitigate spoofing attacks on GPS or ADS-B.

Coordinate System – A coordinate system uses an ordered list of coordinates to uniquely describe the location of points in space. The meaning of the coordinates is defined concerning some anchor points. The point with all coordinates being zero is called the origin. [ Examples: terrestrial, Earth-centered, Earth-fixed, equator, meridian longitude, latitude, geodetic latitude, geocentric latitude, and geoid. [7]

DEW Energy SPREAD and Loss in Propagation – There are two types of energy losses in propagation: *the spreading of energy such that it does not interact with the target and the wasting of energy in interactions with a physical medium, such as the atmosphere, through which it passes to destroy the target.* Type one occurs whether the weapon or target is located on earth or in the vacuum of space. Type two occurs primarily when a weapon or target lies within the atmosphere. (Nielsen, 2012)

DEW Propagation loss – There is always some loss of energy during propagation. The DEW must *deliver more energy than needed to damage the target to compensate for the loss along the way.* DE weapon design depends on the anticipated target, determining the energy required for damage. Second, the anticipated scenario (range, environment, time, etc. This determines how much energy



must be produced to ensure that adequate energy is delivered in the time available. (Nielsen, 2012)

**Fluence** is the energy per area or (Joules / cm<sup>2</sup>) necessary to damage a target. (Nielsen, 2012)

**Intensity** is the power per area (Watt / cm<sup>2</sup>) necessary to damage a target. (Nielsen, 2012)

**Localization** – Process of determining an object's place concerning some reference, usually coordinate systems. [aka Positioning or Position Fix]

**Microwave Weapon** – A device that damages a target by emitting focused microwaves. The critical word in the definition is “damage.” (Monte, 2021) **Navigation Data** is the data transmitted from satellites, including orbit parameters to determine the satellite locations, timestamps of signal transmission, atmospheric delay estimations, and status information of the satellites and GPS, such as the accuracy and validity of the data. (IS-GPS-200G, 2013) [8]

**Pseudo-Random Noise (PRN)** sequences are pseudo-random bit strings. Each GPS satellite uses a unique PRN sequence with a length of 1023 bits for its signal transmissions. aka as Gold codes, they have a low cross-correlation with each other. (IS-GPS-200G, 2013)

**Propagation** – delivery of energy to a DEW target.

**Snapshot GPS Receiver**– A snapshot receiver is a GPS receiver that captures one or a few milliseconds of raw GPS signal for a location fix. (Diggelen, 2009)

**DEW Weapon** – *Weapons may be understood as devices that deposit energy on targets. The energy that must be deposited to achieve a given level of damage is relatively insensitive to the type of weapon employed. Nuclear weapons may be characterized by megatons, bullets in terms of muzzle velocity, and particle beams in terms of amperes of current. Still, when reduced to common units for the energy absorbed by the target, similar levels of damage are achieved at similar levels of energy deposited.* (Nielsen, 2012)

**Radiological Weapon** – a radiological weapon means any device other than a manufactured nuclear explosive, specifically

**designed to employ radioactive material by disseminating it via crude explosion, aerosol, injection, dispersion, or aerial spraying to cause human destruction, damage, or injury, employing the emitted gamma or beta radiation over the years produced by the decay of such material.** (McCreight R., Convergent Technology and Future Strategic Threat, 2013) (McCreight M. S., 2020)

**False Flag Operation** – organized spreading of misinformation or disinformation.

## **Specific to Chapter 14, Satellite Killers**

### **Classification of Satellites**

Satellites are classified in terms of their purpose and are classified as follows:

Astronomical satellites – observation of distant planets and galaxies;

Biosatellites – carry living organisms to aid scientific experiments;

Communication satellites – communications satellites use geosynchronous or Low Earth orbits to communicate with each other and other systems;

Earth observation satellites are satellites intended for non-military uses such as environmental monitoring, meteorology, and producing maps;

Killer satellites are designed to destroy warheads, satellites, and space-based objects;

Navigational satellites use radio time signals transmitted to enable mobile receivers on the ground to determine their exact location. The relatively clear line of sight between the satellites and receivers on the ground allows satellite navigation systems to measure location to accuracies on the order of a few meters in real-time;

Reconnaissance satellites are communications satellites deployed for military or intelligence applications;

Recovery satellites provide a recovery of reconnaissance,

biological, space-production, and other payloads from orbit to Earth;

Space stations are orbital structures designed for human beings to live in space. A space station is distinguished from other crewed spacecraft by its lack of major propulsion or landing facilities. Space stations are designed for medium-term living in orbit;

Tether satellites are connected to another satellite by a thin cable called a tether; and

Weather satellites are used to monitor Earth's weather and climate.

### **Satellite Orbits**

The most common type of orbit is a geocentric orbit, with over 3,000 active artificial satellites orbiting the Earth. Geocentric orbits may be further classified by their altitude, inclination, and eccentricity.

The commonly used altitude classifications of the geocentric orbit are Low Earth Orbit (LEO), Medium Earth Orbit (MEO), Geosynchronous Orbit (GEO), and High Earth Orbit (HEO). Low Earth Orbit is any orbit below 2,000 km, Medium Earth Orbit is any orbit between 2,000 and 36,000 km, and High Earth Orbit is greater than 36,000 km (Figure 14.2).

### **Centric classifications**

A galactocentric orbit is an orbit around the center of a galaxy.

A heliocentric orbit is an orbit around the Sun. In our Solar System, all planets, comets, and asteroids are in such orbits, as are many artificial satellites and pieces of space debris.

Geocentric orbit is an orbit around Earth, such as the Moon or artificial satellites. Currently, there are over 2,500 active artificial satellites orbiting the Earth.

### **Altitude classifications**

Low Earth Orbit (LEO): Geocentric orbits ranging in altitude from 180 km – to 2,000 km;

Medium Earth Orbit (MEO): Geocentric orbits ranging in altitude from 2,000 km – to 20,000 km;

Geosynchronous Orbit (GEO): Geocentric circular orbit with an altitude of 36,000 km. The orbit period equals one sidereal day, which coincides with the Earth's rotation period. The speed is 3,075 m/s (10,090 ft/s).

High Earth orbit (HEO): Geocentric orbits above the altitude of a geosynchronous orbit (GEO) > 36,000 km (~ 40,000 km).

**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 R. et al., *Counter Unmanned Aircraft Systems Technologies, and Operations*, 2020) (Nichols & et al., 2020) (Nichols & et al., 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 are 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, 2009)

A majority of the technical abbreviations come from (Nichols R. K. et al., *Unmanned Aircraft Systems in the Cyber Domain*, 2019) and (Nichols R. al., *Counter Unmanned Aircraft Systems Technologies, and Operations*, 2020) (Nichols & 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., Chapter 14: *Maritime Cybersecurity*, 2021) (Nichols & Sincavage, *Disruptive Technologies with Applications in Airline, Marine, and Defense Industries*, 2021) (Nichols & Ryan, *Unmanned Vehicle Systems & Operations on Air, Sea & Land*, 2020)

Other definitions from the following references:

### Bibliography

(Seoul), B. T. (2018, November 27). *RF-EMF Exposure*. Retrieved from Published online 2018 Nov 27. DOI: 10.4062/biomolther.2018.152: doi: 10.4062/biomolther.2018.152

AARL. (2022, March 18). *RF Radiation and Electromagnetic Field Safety*. Retrieved from <https://www.arrl.org/>: <https://www.arrl.org/rf-radiation-and-electromagnetic-field-safety/>

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

Adamy, D. L. (2015). *EW 104: EW against a new generation of threats*. Norwood, MA: Artech House.

Adamy, D. L. (2021). *Space Electronic Warfare*. Norwood, MA: 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.

Arar, S. (2022, Feb 9). *All About Circuits Understanding*. Retrieved from [www.allaboutcircuits.com/technical:](http://www.allaboutcircuits.com/technical:) [HTTPs://www.allaboutcircuits.com/technical](http://www.allaboutcircuits.com/technical)

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

Army, U. (2014). *FM 3-38 Cyber Electromagnetic Activities*. Washington: DoD.

Army, U. (April 7, 2000). *Joint Doctrine for Electronic Warfare – Joint Pub 3-51*. Washington: DoD.

Askin, O. I. (2015). Cyberwarfare and electronic warfare integration in the operational environment of the future: cyber, electronic warfare. . *Cyber Sensing 2015* (14 May 2015) (pp. Proceedings Vol 9458, *Cyber Sensing 2015*; 94580H (2015) SPIE Defense + Security, 20). Washington: Askin, O., Irmak, R, and Avseyer, M. (14 May 2015) *Cyber warfare and electronic war 94580H* (2015) SPIE Defense + Security, 20.

Ball, M. (2020, January 13). *The Metaverse: What It Is, Where to Find It, and Who Will Govern it*. Retrieved from

<https://www.matthewball.vc/all/themetaverse/>:

<https://www.matthewball.vc/all/themetaverse/> Jan 13, 2020

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

Black Swan Definition. (2020, December 16). Retrieved from <https://www.investopedia.com/terms/>:

[https://www.investopedia.com/terms/b/](https://www.investopedia.com/terms/b/blackswan.asp#:~:text=A%20black%20swan%20is%20an,they%20were%20obvious%20in%20hindsight.)

[blackswan.asp#:~:text=A%20black%20swan%20is%20an,they%20were%20obvious%20in%20hindsight.](https://www.investopedia.com/terms/b/blackswan.asp#:~:text=A%20black%20swan%20is%20an,they%20were%20obvious%20in%20hindsight.)

Bunn, M. (2021). *The evolving global threat to nuclear and radiological*. Retrieved from [https://scholar.harvard.edu/files/matthew\\_bunn/files/transport-threat-brief-2021.pdf](https://scholar.harvard.edu/files/matthew_bunn/files/transport-threat-brief-2021.pdf)

Castrillo, V. (2022, Feb). A Review of Counter UAS Technologies for Cooperative Defense Teams of Drones. *Italian Aerospace Research Center. Drones*, p. 6.

CDC. (2022, March 18). CDC, *Radiological Threat Agents*, 2015. Retrieved from CDC: <https://www.cdc.gov/>

DHS. (2022, March 18). *countering-weapons-mass-destruction*. Retrieved from [www.dhs.gov/](https://www.dhs.gov/): <https://www.dhs.gov/countering-weapons-mass-destruction-office>

DHS. (2022, March 18). *Radiological Attack Fact Sheet*. Retrieved from <https://www.dhs.gov/publication/>: <https://www.dhs.gov/publication/radiological-attack-fact-sheet>

Diggelen, F. V. (2009). *A-GPS: Assisted GPS, GNSS, and SBAS*. NYC: Artech House.

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

DoD-02. (2018). *Information Operations (IO) in the United States*. Retrieved from JP 3-13: [http://www.dtic.mil/doctrine/new\\_pubs/jp3\\_13.pdf](http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf)

EarthSky – Earth, S. H. (2019). *EarthSky – Earth, Space, Human World, Tonight*. Retrieved from [earthsky.org/](https://earthsky.org/)2019: <https://earthsky.org/>2019

Eichelberger, M. (2019). *Robust Global Localization using GPS and*

*Aircraft Signals*. Zurich, Switzerland: Free Space Publishing, DISS. ETH No 26089.

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/>

EPA, [. (2012). *Radiation Facts, Risks, and Realities—US Government*. Washington: [US EPA – US Government].

FAS, M. /. (1998). *Nuclear Weapons Effects Technology Militarily Critical Technologies List (MCTL)*. Retrieved from *irp.fas.org/threat*: <https://irp.fas.org/threat/mctl98-2/>

FCC. (2022, March 18). *The effects of radiofrequency electromagnetic radiation on Human Health*. Retrieved from <https://ecfsapi.fcc.gov/>: <https://ecfsapi.fcc.gov/file/1093016723166/RF>

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

Gent, E. (2022, February 25). *Scientists Create Artificial Neurons that Power a Venus Fly Trap*. Retrieved from *techbely.com*: <http://techbely.com/scientists-created-synthetic-neurons-that-can-make-a-venus-flytrap-snap/>

globalsecurity.org. (2022, March 18). *Weapons of Mass Destruction (WMD)*. Retrieved from *www.globalsecurity.org*: <https://www.globalsecurity.org/wmd/intro/nuke.htm>

Grinter, P. (2021, Aug 25). *Avenger UAS Autonomously Tracks and Follows Target Aircraft*. *Unmanned Systems Technology*.

Haines, D. (2022). *Executive Summary, Feb 2, 2022, Analysis of Pending AHI Cases – Redacted*. Washington: DNI.

hawkeye-360. (2022, March 4). *hawkeye-360-signal-detection-reveals-GPS-interference-in-Ukraine*. Retrieved from *www.he360.com/*: <https://www.he360.com/hawkeye-360-signal-detection-reveals-gps-interference-in-ukraine/>

Henselmann, M. L. (2022, March 18). *Non-Kinetic Warfare: The New Game Changer in the Battle Space*. Retrieved from University of Jyväskylä, Finland : DOI: 10.34190/ICCWS.20.033].



IAEA. (2018). *IAEA Safety Standards: Regulations for the Safe Transport of Radioactive Material*. Retrieved from [www-pub.iaea.org/](http://www-pub.iaea.org/): [https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1798\\_web.pdf](https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1798_web.pdf)

IS-GPS-200G. (2013, September 24). IS-GPS-200H, GLOBAL POSITIONING SYSTEMS DIRECTORATE SYSTEMS ENGINEERING & INTEGRATION: INTERFACE SPECIFICATION IS-GPS-200 – NAVSTAR GPS SPACE SEGMENT/NAVIGATION USER INTERFACES (24-SEP-2013). Retrieved from <http://everyspec.com/>: [http://everyspec.com/MISC/IS-GPS-200H\\_53530/](http://everyspec.com/MISC/IS-GPS-200H_53530/)

Jaitner, M. (2014). *Russian Information Warfare. Conference Paper*, Swedish Defense Research Agency. Swedish Defense Research Agency.

Ju Hwan Kim, J.-K. L.-G. (2019, May 1). PMCID: PMC6513191PMID: 30481957 Possible Effects of Radiofrequency Electromagnetic Field Exposure on Central Nerve System Retrieved from <https://pubmed.ncbi.nlm.nih.gov/>: <https://pubmed.ncbi.nlm.nih.gov/30481957/>

Library, E. P. (2022, March 18). *Atoms for Peace*. Retrieved from [www.eisenhowerlibrary.gov/research/](http://www.eisenhowerlibrary.gov/research/): [www.eisenhowerlibrary.gov/research/online-documents/atoms-peace](http://www.eisenhowerlibrary.gov/research/online-documents/atoms-peace)]

Linda Douw, M. K. (2009). Cognitive and radiological effects of radiotherapy in patients with low-grade glioma. *Lancet Neurology*, Sept.

Losey, S. (2022, Feb 28). Killing drones with Thor's hammer: Air Force eyes counter-UAS Weapon. *Defense News*.

Malsi, B. F. (2022, February 27). Ukraine Says It Used Turkish-Made Drones to Hit Russian Targets. *WSJ*.

Martin, J. (2016). *Drone Nation-America's New Way of War*. Lexington Books.

McCreight, M. S. (2020, Sept. Quantum Conundrum: Multi-domain Threats, Convergent Technology & Hybrid Strategy, US Army Futures Command. *Mad Scientist #268*.

McCreight, R. (2013, October). Convergent Technology and Future Strategic Threat *Strategic Studies Quarterly*, pp. 10-18.

McCreight, R. (2013, March ). Convergent Technology Threats. *Strategic Studies Quarterly*, USAF Air University.

McCreight, R. (2021). NeuroStrike Weapons and the Strategic Domain after 2020: Caution *Academia Letters*, 2021.

McCreight, T.-F.-C. T. (2020, February 24). Twenty-First-Century Threats in a Complex World: Dealing with DUST in the Wind. *Wild Blue Yonder / Maxwell*.

Monte, L. (2021). *War at the Speed of Light*. Lincoln: Potomac Books.

NATO. (n.d.). NATO HAHANDBOOKN THE MEDICAL ASPECTS OF NBC DEFENSIVE. Retrieved from <http://large.stanford.edu/courses/2019/ph241/abbate2/docs/fm8-9.pdf>: <http://large.stanford.edu/courses/2019/ph241/abbate2/docs/fm8-9.pdf>

Nelson, K. (2022, February 20). What Could be Causing Havana Syndrome Cases on US Soil? *CBS News*.

NERC. (2019, November 5). *nerc\_emp\_task\_force\_report.pdf*. Retrieved from [nerc.com/pa/](https://nerc.com/pa/): [https://nerc.com/pa/stand/emp%20task%20force%20posting%20dl/nerc\\_emp\\_task\\_force\\_report.pdf](https://nerc.com/pa/stand/emp%20task%20force%20posting%20dl/nerc_emp_task_force_report.pdf)

News, B. (2022, February 5). Nuclear Plant Under Attack by Artillery. *BBC News*.

Nichols, R. K. (1999). *ICSA Guide to Cryptography*. New York City: McGraw Hill.

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). *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. (2020). *Counter Unmanned Aircraft Systems Technologies & Operations*. Manhattan, KS: [www.newprairiepress.org/ebooks/31](http://www.newprairiepress.org/ebooks/31).

Nichols, R. K. (2021). Chapter 14: Maritime Cybersecurity. In R. K. Nichols, & J. J. Ryan, *Unmanned Vehicle Systems & Operations on Air, Sea, Land* (pp. 330-356). Manhattan, KS: New Prairie Press #35.

Nichols, R. K. (2022). Chapter 18: Cybersecurity Counter Unmanned Aircraft Systems (C-UAS) and Artificial Intelligence. In D. M. R. K. Barnhart, *Introduction to Unmanned Aircraft Systems*, 3rd Edition (pp. 399-440). Boca Raton, FL: CRC.

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

Nichols, R. K., & Mumm, H. C. (2019). *Unmanned Aircraft Systems in the Cyber Domain*, 2nd Edition. Manhattan, KS: [www.newprairiepress.org/ebooks/27](http://www.newprairiepress.org/ebooks/27).

Nichols, R. K., & Sincavage, S. M. (2021). *Disruptive Technologies with Applications in Airline, Marine, and Defense Industries*. Manhattan, KS: New Prairie Press #38.

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](http://www.newprairiepress.org/ebooks/27)

Nichols, R., & al., e. (2020). *Unmanned Vehicle Systems and Operations on Air, Sea, and Land*. Manhattan, KS: New Prairie Press #35.

Nichols, R., & Ryan, D. &. (2000). *Defending Your Digital Assets Against Hackers, Crackers, Spies, and Thieves*. San Francisco: McGraw Hill, RSA Press.

Nichols, R., & Ryan, J. M. (2020). *Unmanned Vehicle Systems & Operations on Air, Sea & Land*. Manhattan, KS: New Prairie Press #35.

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.

NIEH. (2022, March 18). EMF Radiation? Retrieved from <https://www.niehs.nih.gov/>: <https://www.niehs.nih.gov/health/topics/agents/emf/index.cfm>

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

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

NRC. (2017). *NRC Backgrounder on Research and Test Reactors*. Retrieved from <https://www.nrc.gov/.../research-reactors-bg.html>: [www.nrc.gov/.../research-reactors-bg.html](https://www.nrc.gov/.../research-reactors-bg.html)

Okula, C. (n.d.). *Small anechoic chamber*. Edwards Air Force Base.

R.K. Nichols & Lekkas, P. (2002). *Wireless Security; Threats, Models & Solutions*. NYC: McGraw Hill.

R.K. Nichols, e. a. (2020). *Unmanned Vehicle Systems & Operations on Air, Sea & Land*. Manhattan, KS: New Prairie Press #35.

R. K. Nichols, & et al. (2022). *DRONE DELIVERY OF CBNRECy – DEW WEAPONS, Emerging Threats of Mini-Weapons of Mass Destruction and Disruption (WMDD)*. Manhattan, KS: New Prairie Press #TBA.

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.

Reports, E. C. (2018, February 27). EMP Report February 27, 201. Retrieved from [highfrontier.org: highfrontier.org/february-27-2018-publish-emp-commission-reports](https://highfrontier.org/highfrontier.org/february-27-2018-publish-emp-commission-reports/)].

Ryan, S. (2014, November 4). USASOC-CognitiveJointForceEntry.pdf. Retrieved from [info.publicintelligence.net/: https://info.publicintelligence.net/USASOC-CognitiveJointForceEntry.pdf](https://info.publicintelligence.net/USASOC-CognitiveJointForceEntry.pdf)

Scarpati, J. (2021, Feb 25). *What is a radio frequency (RF)?* . Retrieved from [https://techtargget.com: https://techtargget.com/searchnetworking/definition/radio-frequency](https://techtargget.com/https://techtargget.com/searchnetworking/definition/radio-frequency) Feb 25, 2021

Schwarz, R. a. (n.d.). *Two different anechoic chambers—one large and one small*. Image used courtesy of Rohde and Schwarz.

science media center.co.NZ. (2022, March 18). *Sources of Radiation: Where do mobile phones fit in?* Retrieved from <https://www.sciencemediacentre.co.nz/infographics/>: <https://www.sciencemediacentre.co.nz/infographics/>

Sciences, N. A. (2020). *An Assessment of Illness in U.S. Government*

*Employees and Their Families at Overseas Embassies*. Washington: National Academy of Sciences.

Scientists, B. o. (2009, May 19). *Iraq FFCD report – what-we-found-at-al-tuwaitha*. Retrieved from <https://thebulletin.org/https://thebulletin.org/2009/05/what-we-found-at-al-tuwaitha>

Scoles, S. (2022, March 11). Radioactive Material Is everywhere. *Scientific American*.

SOCOM. (2015). *SOCOM Leaders attribute risks to cognitive warfare*. Ft Bragg NC: SOCOM Unclassified brief.

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

Straussfogel, C. v. (2009 ). *International Encyclopedia of Human Geography*. Amsterdam: Elsevier.

SYSTEMS, G. A. (2022, March 3). How AI and supervised autonomy will change combat. GENERAL ATOMICS AERONAUTICAL SYSTEMS

T.E. Humphrees, e. (2008). Assessing the Spoofing Threat: Development of a portable GPS Spoofing Civilian Spoofer. ION (pp. Sept 16-19). Savana, GA: ION.

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

Tippenhauer, N., & et.al. (2011). On the requirements for successful spoofing attacks. *Proc. of the 18th ACM Conf. on Computing and communications security (CCS)*, 75-86.

Turnquist, C. (2020). Radiation-induced brain injury: current concepts and therapeutic strategies targeting neuroinflammation. *Neuro-Oncology Advances*, Volume 2, Issue 1, January-December.

Tzu, S. (475 – 221 B.C.E.). *The Art of War*. Retrieved from <http://classics.mit.edu>: <http://classics.mit.edu/Tzu/artwar.html>

USAF. (January 4, 2002). *Air Force Doctrine Document AFDD 2-5, Information Operations*. Washington: USAF.

USGPO. (2021, June 14). What is GPS? Retrieved from [Gps.gov: www.gps.gov/syste.ms/gps](https://www.gps.gov/syste.ms/gps)

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

[1] ECCM was considered T.S. classified with most secret protocols and design algorithms. TS = Top Secret

[2] EW, E.S., E.P., E.A. definitions were adjusted via (Adamy D., EW 101 A First Course in Electronic Warfare, 2001) to align with our UAS weapons deployment theme.

[3] GPS consists of at least 24 satellites orbiting around the Earth at approximately 20,000 km above the surface, circling the Earth twice a day, continuously transmitting its location and time code. Localization is done in space and time. GPS provides location and time information to receivers anywhere on Earth where at least four satellite signals can be received. Line of sight (LOS) between receiver and satellite is advantageous. GPS signals take between 64 and 89 ms to reach Earth. GPS works poorly indoors, with reflections, close to thick obstructions, and below trees in canyons. Orbits are precisely determined by GCS, optimized for a high number of concurrently visible satellites above the horizon at any place on Earth.

[4] LRAD = Long Range Acoustic Device (Chapter 13) / Long-Range Area Denial (Chapter 11)

[5] All Definitions are taken from (Eichelberger 2019) unless otherwise noted.

[6]  $\dot{\phantom{x}}$  = Order of magnitude; dot = dot product for vectors

[7] All these systems are discussed in Chapter 2 of (Eichelberger, 2019)

[8] Each satellite has a unique 1023-bit PRN sequence, plus some current navigation data, D. Each bit is repeated 20 times for better

robustness. The navigation data rate is limited to 50 bit / s. This also limits sending timestamps every 6 seconds and satellite orbit parameters (function of the satellite location over time) only every 30 seconds. As a result, the latency of the first location estimates after turning on a classic receiver, called the time to first fix (TTFF), can be high.



# Table of Contents -Detailed

## Title Page

Cover Art (Brenda Andrews, Suzanne Sincavage, Candice Carter)

Copyright / Publication Page

Books also by Professor Randall K. Nichols and the Wildcat Team

Dedications

Disclaimers (Lonstein)

Foreword (Harding)

Preface (Nichols)

Acknowledgments

List of Contributors

Abbreviations and Acronyms (Reduced to only Book 6)

Table of Contents

Table of Figures

Table of Tables

Table of Equations

## Chapters

### **Section 1: Chemical, Biological, Radiation, Nuclear, Explosive (CBRNE) Weapons / Payloads**

#### **1. Drone's Capabilities to Deliver Weapons of Mass Destruction / Disruption (WMDD) - a Global Perspective (Slofer)**

Learning goals

Weaponization Brief history Major types of Drones/Robots

Aquatic drones

Surface vessels

Submergible

Robots/drones

Unmanned Aerial Vehicle (UAV),

Conclusions  
Bibliography

## **2. Chemical Weapons (Hood)**

Student Objectives

Introduction

Case Study 1: The Potential for Chemical Weapons Release in Ukraine

Case Study 2: Chemical Weapons Release in Syria and the Organization for the Prohibition of Chemical Weapons

Ghoutha: The Leper of the 21st Century

False Declaration and Chemical Weapons Attacks

Deepening Chemical Weapons Crisis

OPCW Response to Widening Chemical Weapons Use

The Fight for a Future Free of Chemical Weapons

The intersection of Drones and Chemical Weapons

A Parting Nightmare

Bibliography

## **3. Biological Weapons (Sincavage & Carter)**

Student Objectives

Introduction

Early Unmanned Biological Weapon

Attack

Terrorist Groups

Democratic People's Republic Of Korea (DPRK) (North Korea)

Drone Swarms

Detection

Conclusions

## Bibliography

### **4. Radiological, Electromagnetic, Drone & Metaverse Risks and Issues (McCreight)**

Introduction

n

2

Radiological Threats—Everything Old is New Again

The Nature of Radiological, Electromagnetic, and Drone Risk  
Inside the Metaverse

Radiological and Electromagnetic Risks and the Era of Cognitive  
Warfare

Threat Dynamics—Radiological and Electromagnetic Issues Post  
2021

Grasping the Non-Kinetic Aspects of CONV-CBRN

Special Delivery of Death and Destruction: Adding Drone Risk  
Factors Post 2021

CONV-CBRN Drone Augmented Threat and Risk Possible  
Scenarios

CONV-CBRN—Onward Security and Risk Challenges Post 2021

Conclusions

### **5. Nuclear Weapons (Carter)**

Student Objectives

Introduction

State Actors

Russia

Soviet Union

Russian Federation

Посейдон And Белгород

Nuclear Alert Status

China

Other Countries  
Conclusions  
Bibliography  
Endnotes

## **6. Explosives Delivered by Drone (Hood)**

Student Objectives  
Introduction  
Case study 6.1:  
Case Study 2: Ukraine Adapting Drones to Drop Improvised  
Explosives  
Case Study 3: Anti-Personnel Munitions  
Point shooting with a drone  
Case Study 6.4: Loitering Munitions  
Conclusions  
Bibliography

## **7. Deception (Nichols)**

Student objectives  
Introduction  
Vulnerabilities of modern societies to UAS attack  
Basic terminology  
Perspectives of deception  
Deception maxims  
Surprise  
Four Fundamental Principles  
Three examples of UAS Attacks that could be *Destruction, Disruption, or Deception (D/D/D)*  
Taxonomy of Technical Methods of Deception

Technical Sensor Camouflage, Concealment, and Deception  
(CC&D)

CEA

Information Operations (IO)

Signal and Information Systems (IS) Denial and Deception

Electronic Warfare (EW)

EW Generalities

Legacy EW definitions

Spoofing – GPS Spoofing

Spoofing techniques

Eichelberger's CD – *Collective Detection Maximum Likelihood*

*Localization Approach* (ECD)

Signals Intelligence (SIGINT)

Conclusions

Bibliography

Endnotes

## **Section 2: Directed Energy Weapons (DEW) / Payloads**

### **8. DEW Primer (Nichols)**

Student Objectives

Introduction

Common Framework

Effects Of Directed Energy Weapons (Dew)

The Beloved Btu Gives Way To Joules

Energy Required For Damage

Ice Cube

10,000 Joules

Energy Alone Sufficient For Hard Damage?

Energy Delivery Rate

Thermal Conduction

Constant Surface Temperature Case

Convection  
Wind V Temperature Convection Heat  
Vacuum Black Body Radiation  
Implications  
Fluence And Intensity  
All-Purpose Damage Criteria  
Energy Spread And Loss In Propagation  
Energy Spread  
Conclusions  
Bibliography  
Endnotes

## **9. DE Weapons, Projectiles, Damage (Nichols)**

Student Objectives  
Introduction  
Common Framework (Chapter 8 Recap)  
Fundamentals Of Kew  
Hunting Wild Boars  
At The Boar Skin  
Damage  
Sacrificial Drones  
Propagation In An Atmosphere  
Sir Isaac Newton (1643-1727)  
Newton's First Law  
Newton's Second Law  
Newton's Third Law  
Shooting In The Air  
Drone Vs. Drone In Air – Complexity  
Flight Equations With Forces  
Thrust  
Vertical Location  
Vertical Descent

Velocity  
Acceleration  
Vertical Ascent  
Horizontal Location  
Summary: Propagation In The Atmosphere  
Interaction With Targets – Damage  
Pressure And Impulse  
Angle Of Attack (AoA)  
Target Material And Shape  
What Is Damage?  
Sabot Projectile Design  
Shaped Charges  
Modern Military  
Shape Charge Functions  
Summary: Target Interaction  
Bibliography

## **10: DE Weapons, MASERS/LASERS (Mai)**

Student Objectives  
Laser Pointer  
Can A Laser Pointer Be Used To Bring Down A Drone?  
Infrared Interference  
Bright Lights  
Heat Damage  
Is Taking A Drone Down With A Laser Illegal?  
Rafael Drone Dome  
Raytheon Drone-Killing Laser  
Athena  
Evasive Measures Used By Drones  
Which Laser Colors Are The Most Dangerous And Why?  
Hy Are Blue Laser Pointers More Dangerous?  
What Laser Pointer Color Is The Most Powerful?  
Classes Of Laser Pointers  
Class 1 Laser Pointers

- Class 2 Laser Pointers
- Class 3 Laser Pointers
- Class 4 Laser Pointers
- Laser Pointer Summary
- A Little History
- Military Interests
- Weaponizing The Laser
- Moore's Law Implications
- Nanotechnology
- Fair-Weather Lasers
- Power Issues
- For The Geeks
- New Threats
- A Solution Waiting For A Conflict
- Laser Weapons Of Potential Adversaries
- Other Considerations
- Conclusion
- Bibliography
- Endnotes

## **11. DE Weapons, Microwaves (Mai)**

- Student Objectives
- Back to Microwave Ovens
- Microwave Weapon
- U.S. Microwave Weapons Antipersonnel Microwave Weapons
- Neurological Microwave Weapons
- Hello, Goodbye, and Goodnight
- The PANDORA Project
- Biological Microwave Weapons
- Skin Irritation
- Frey Effect Weapons
- CHAMP



Russian Microwave Weapons  
Chinese Microwave Weapons  
Detecting And Disabling Drones  
Drone Detection Radar  
Detecting Drones Using RC  
Detection and Jamming Ranges  
Deploying CUAV Systems  
Conclusions  
Managing Editor's Opinion  
Bibliography

## **12. Hypersonic Drone Missiles (Slofer)**

Student Objectives  
The Speed spectrum  
Subsonic  
Supersonic  
Hypersonic  
Speed and Distance  
Types of Hypersonic missiles  
Types of Launch Platforms  
Stationary Land Based  
Sea/ocean based  
Power Plants/ Propulsion systems  
Supersonic-combination ramjet aka scramjet  
Technology considerations for hypersonic  
Navigation, guidance, and control systems  
Other considerations  
Military application and threats  
Time is everything  
Doctrines, Policies, and Strategies in an era of hypersonic weapons  
Summary

## Bibliography

### 13. **Acoustic Weapons (Nichols, Carter, McCreight)**

Student Learning Objectives

Disclaimer

Detection Signatures Review

Essentials of Audiology

Audiology Fundamentals

The intensity and Inverse Square Law

Decibels

The Nature of Sound

Other Parameters of Sound waves

Complex waves

Standing Waves and Resonance

In terms of UAS. Countermeasures, why are Acoustics so important?

What are the Acoustic Detection Issues?

Can UAS acoustic signatures be reduced?

Is Acoustic Quieting possible?

What is an Acoustical attack on the UAS's Gyroscope?

How has the Long-Range Acoustic Device (LRAD) been used as a sonic weapon?

LRAD

NATO Autonomous Mine Sweepers (ATM)

MEMS

Resonance Effects on MEMS – we have arrived at the NUB of this section

What is Resonance Tuning?

What is the “so what” for Acoustics?

Are there Countermeasures for Acoustic attacks on gyroscope?

South Korean Experiment

NOISE

UAS Collaboration – SWARM

Remember the Problem the Wildcat team has addressed in every book of our series.

A Problem Solution Not The ONLY Problem Solution:

Switching to A Dangerous Theater of Operations (TO) – Chinese Drones in the Spratly Islands, and Chinese Threats to USA forces in the Pacific

Location of the Spratly Islands and Their Strategic Importance

Target Drones

Shark Swarm and Wanshan Marine Test Field

Fast Drone Ship

Long-Range UUV

Crisis Watch

Red Drones over Disputed Seas

BZK -005

DRONESEC Report April 2022

Acoustic Dynamics: Havana Syndrome and Neurological Vulnerability

Acoustics and Havana Syndrome Illustrate our Collective Neurological Vulnerability

Acoustic Technologies

SCREAMERS

Bibliography

#### **14. Satellite Killers [Jackson]**

Student Learning Objectives

Satellites

Introduction

Classification of Satellites

Satellite Orbits

Centric classifications

Altitude classifications

Inclination classifications

- Eccentricity classifications
- Synchronous classifications
- Satellite Killers
- Introduction
- Denying space
- Satellite Killers: China
- Satellite Killers: Russia
- Space Awareness and Space-Based Weapons
- Questions
- Bibliography
- Informative Readings and Additional Bibliography
- Satellite Killing and Denying Space
- Space Awareness and Space-based Weapons
- Space Breakthroughs and Inventions

## **15. Cyber Weapons and CBRNE (Nichols)**

- Student Objectives
- Problem – The Risk of Terrorist Attack vs. U.S. Air Defense System or CBRN Facilities
- CBRN Infrastructure Attacks
- Contributing Technologies
- Attack / Defense Scenarios
- Description of the sUAS/UAS Landscape – What’s available for Deployment against CBRNE Assets?
- Autonomy v Automation Levels
- UAS Collaboration
- Cyber Related CBRNE Attacks
- Drones as Rogue Access Points
- CBRNE Attack Scenarios
- What Is the Counter-UAS Problem?
- Operational Protection from Hostile UAS Attacks – A Helicopter View

|  |  |
|--|--|
| Countering UAS Air Threats                                 |  |
| Vulnerabilities Perspective                                |  |
| Conventional Vulnerabilities of Air Defense Systems (ADS), |  |
| Attacks By sUAS, and Countermeasures                       |  |
| Conventional Countermeasures Against sUAS / UAS            |  |
| Passive Measures   |  |
| Conclusions  |  |
| Discussion Topics  |  |
| US Navy Official Response                                  |  |
| The Case for a Cyber Weapon                                |  |
| Discussion Question  |  |
| Bibliography   |  |
| Endnotes   |  |

### **Section 3: Policy Considerations**

#### **16. Assessing the Drone Delivery Future WMDD / DEW Threats and Risks (Mumm / Lonstein)**

|  |  |
|--|--|
| Student Learning Objectives                                      |  |
| A Look Back at the Traditional Delivery Systems                  |  |
| Stack Integration-Emerging Technologies Offers New Tactics,      |  |
| Techniques, and Procedures (TTPs)                                |  |
| Assessment of Emerging Threats of Mini-WMD                       |  |
| Does the World Have an Answer to These Emerging Threats?         |  |
| Airspace-Freedom of Movement of Autonomous Systems               |  |
| Risks to Access in Time and Space? How Over The Horizon          |  |
| Capability Limits the Usefulness of Freedom of Movement Policies |  |
| Legal Considerations for Autonomous Systems as WMD/DEW           |  |
| Delivery Platforms   |  |
| Assessment of the State of Readiness for the Legal Community to  |  |
| Prosecute Cases with Autonomous Systems Use in the WMD/DEW       |  |
| space  |  |

Legal and Cyber Considerations While Building the Legal Framework Towards Peaceful Containment/Use of Autonomous Systems in the Future

Conclusions

Questions

References

**17. Unique Challenges of Responding to Bioterrorism and Chemical Threats and Attacks delivered by Drones (Sincavage & Carter)**

Student Objectives

Introduction

Advanced Robotics

Robotics: Technology Overview

3D Printing

Bioprinters

The Risks

The Opportunities

Conclusions

Bibliography

**18. Practical Crime Scene Investigation (CSI) Using Autonomous Systems (Mumm / Lonstein)**

Student Learning Objectives

A Look Back at the Science of Crime Scene Investigation (CSI)

Challenges of CSI in Hot Zones-Why Not Use Robots?

Autonomous Systems Technology to Augment Human CSIs

Legal Considerations for Autonomous Systems Use at a Crime Scene

Autonomous Evidence: If You Can't Explain It, Courts Will Not Allow It

Prosecutorial Evidence Collection by Human CSI VS. Autonomous Systems

Evidence Preservation Via Chain of Custody-Technical and Cyber Considerations

Augmenting and Integrating Artificial Employees/Autonomous CSIs-The Changing -Horizon of Scene Collection and Justice for All?

Conclusions

Questions

## **19. Navigation Spoofing and ECD (Nichols)**

Student Objectives

Summary

Definition: Spoofing

Introduction

Spoofing

GPS Signal

Classic Receivers

A-GPS – Reducing The Start-Up Time

Course – Time Navigation

Snapshot Receivers

Collective Detection

ECD

Research To 2016: Survey Of Effective GPS Spoofing Countermeasures

Spoofing Techniques

A-F Analysis

GPS Spoofing Research: Out Of The Box Brilliance To ECD Defense

Maximum Likelihood Localization

Spoofing Mitigation

|   |  |
|---|--|
| Successive Signal Interference Cancellation             |  |
| GPS Signal Jamming                                      |  |
| Two Robust GPS Signal Spoofing Attacks and ECD          |  |
| Seamless Satellite-Lock Takeover                        |  |
| Navigation Data Modification                            |  |
| ECD Algorithm Design                                    |  |
| Branch And Bound  |  |
| ADS-B Security  |  |
| ADS-B Standards   |  |
| ADS-B Security Requirements                             |  |
| Vulnerabilities In ADS-B System                         |  |
| Broadcast Nature of RF Communications                   |  |
| No Cryptographic Mechanisms                             |  |
| ADS-B Cots  |  |
| Shared Data   |  |
| Asterix Data Format                                     |  |
| Dependency On The On-Board Transponder                  |  |
| Complex System Architecture And Passthrough Of GNSS     |  |
| Vulnerabilities   |  |
| Threats To ADS-B System                                 |  |
| Eavesdropping   |  |
| Data-Link Jamming                                       |  |
| Two Types Of Jamming Threats For ADS-B                  |  |
| Ground Station Flood Denial                             |  |
| Aircraft Flood Denial                                   |  |
| ADS-B Signal Spoofing                                   |  |
| Ground Station Target Ghost Injection / Flooding        |  |
| Aircraft Target Ghost Injection / Flooding              |  |
| ADS-B Message Deletion                                  |  |
| ADS-B Message Modification                              |  |
| Circling Back To ECD                                    |  |
| Indoor Localization With Aircraft Signals Using ECD Vs. |  |
| Competitive Technologies                                |  |
| ECD Vs. Minimum Us Government GPS Standards             |  |
| Related Work  |  |



WiFi [T]  
Ultrasound [I]  
Light [T,E]  
Bluetooth [T, I]  
RFID [I]  
Sensor Fusion  
HAPS  
Security Of GNSS  
Conclusions  
Definitions  
Bibliography  
Endnotes

#### **Section 4: Tools of the Trade**

### **20. Social Network implications for WMDD (Lonstein)**

Student Learning Objectives  
Social Media Networks as a Weapon of Mass Destruction,  
Distraction, and Division  
Consumer and Commercial Drone Technology as a Tool of  
Espionage, Command, and Kinetic attacks  
Questions for Students to Consider  
Bibliography

### **21. Tools of The Trade (Monnik & Neo)**

Student Objectives  
Introduction  
Accuracy

|  |  |
|--|--|
| Reliability  |  |
| Timeliness   |  |
| Tools for UAS Threat Intelligence                        |  |
| Open-Source Tools  |  |
| Closed-Source Tools                                      |  |
| Collection data types                                    |  |
| Tools for historical and current UAS threat intelligence |  |
| Configuring Google (Open-Source, free)                   |  |
| Configuring LiveUAMap (Open-Source, paid)                |  |
| Tools for current and future UAS threat intelligence     |  |
| Configuring Slack (Closed-Source, free)                  |  |
| DroneSec Notify (Open/Closed-Source, free/paid)          |  |
| Stolen Drone Info (Open/Closed-Source, free/paid)        |  |
| Conclusions  |  |
| Bibliography   |  |
| Endnotes   |  |

# Table of Figures

## 1. Drone Capabilities to Deliver Weapons of Mass Destruction / Disruption (WMDD) -Global Perspective

Figure 1.1-Armed Unmanned Surface Vehicle from BAE Systems

Figure 1.2 Dumpsites of reported chemical and explosive munitions from 1918-to-1980

Figure 1.3 Robot drone

Figure 1.4 Robot drone

Figure 1.5 Robot drone

Figure 1.6 DARPA funded Atlas robot developed by Boston Dynamics

Figure 1.7 Aerial drone used in movie scene filming

Figure 1.8 Image of Predator B drone

Figure 1.9 Use of synchronized swarming drones in a night display

Figure 1.10 Field assembly of a drone capable of thermal imaging and delivery of 1.5kg bombs

Figure 1.11 Drones are being used to drop Molotov cocktails against Russian troops in Ukraine.

Figure 1.12 DJI drone carrying grenade in an improvised carrier made from a plastic jug

## 2. Chemical Weapons

Figure 2.1 Soldiers in Mission Oriented Protective Posture (MOPP) Gear

Figure 2.2 Civil Defense member carries a damaged canister in Ibleen village.

Figure 2.3 Soldier in MOPP Gear Ready

Figure 2.4 Mustard gas artillery shells

Figure 2.5 Agriculture Drone is spraying pesticides on crops

Figure 2.6 DJI Agri's T30

### 3. Biological Weapons

Figure 3.1 Early Unmanned Bioweapons

Figure 3.2 Spraying Drone

Figure 3.3 African Swine Fever Across Asia

Figure 3.4 Democratic People's Republic Of Korea (DPRK) (North Korea) Drone

Figure 3.5 Swarm Of Mass Destruction

### 4. Radiological, Electromagnetic, Drone & Metaverse Risks and Issues

Figure 4.1 Common Sources of Radiation

Figure 4.2 Cognitive Key Terrain

Figure 4.3 Radiological Spectrum

Figure 4.4 Anechoic Chamber[large vs. small] example

Figure 4.5 CONV-CBRN Threat Dynamics

Figure 4.6 Setting the Stage for NV

### 5. Nuclear Weapons

Figure 5.1 Russian President Vladimir Putin Addresses The Russian Federal Assembly

Figure 5.2 Russian Poseidon 2m39 Torpedo

Figure 5.3 A&B Belgorod – Russian Unmanned Nuclear Submarine

Figure 5.4 Belgorod – Russian Unmanned Nuclear Submarine

Figure 5.5 China Nuclear Expansion

Figure 5.6 China Drone Lineup Sharp Sword Stealth Drone And The Wing Loong Reaper

### 6. Explosives Delivered by Drone

Figure 6.1: A Picture Taken By A Drone From Above Its Intended Target.

Figure 6.2: Ukrainians Develop Drone That Drops Molotov Cocktails

Figure 6.3: Close-Up – Ukrainians Develop Drone That Drops Molotov Cocktails

Figure 6.4: Molotov Cocktail Released

Figure 6.5: Heavy Modifications To Civil Drone Platforms Enabled To Carry Very Low Cost Yet Powerful Munitions Such As Mortars 60-81mm Rounds.

Figure 6.6: Point Shooting with a Drone

Figure 6.7: Russian KUB-BLA “Suicide Drone”

Figure 6.8: KUB-BLA Russian Loitering Munition

Figure 6.9: Russian Suicide Drone Used in Ukraine That Picks its Targets Though Advance AI

Figure 6.10: The Wreckage of Another Russian KUB-BLA Loitering Munition

Figure 6.11: US Marine firing Switchblade from a pneumatic launch tube

Figure 6.12: Switchblade 600

Figure 6.13: Artist rendition of a switchblade launch

## 7. Deception

Figure 7.1 Operating Nuclear Power Plants within the U.S.

Figure 7.2 Cyber Electromagnetic Activities

Figure 7.3 CEA / CEW in the view of Total War

## 8. DEW Primer

Figure 8.1 Energy Deposition from Bombs and DEW

Figure 8.2 Energy Flow and Resulting Change in Temperature

Figure 8.3 Special Case: Constant Surface Temperature

Figure 8.4 Effect of Wind v Temperature

Figure 8.5 Black Body Radiation

Figure 8.6 Fluence and Intensity

Figure 8.7 Depth Vaporized by 104 Joules v Area Engaged and Fluence

Figure 8.8 Divergence and Jitter

9: DE Weapons, Projectiles, Damage

Figure 9.1 Coyote unmanned aircraft system.

Figure 9.2 Coyote unmanned aircraft system on the tarmac of Avon Park Air Force Range in Florida.

Figure 9.3 IAI Israeli Harop

Figure 9.4 Newtons Second Law of Motion Relationships

Figure 9.5 Projectile Distance and Velocity Coordinates

Figure 9.6 Effect Of Elevation Angle On Velocity Components

Figure 9.7 Flight Equations with Drag

Figure 9.8 Thrust

Figure 9.9 Smashing two Bricks without spacers for 2nd Degree Black Belt Test

Figure 9.10 Possible Effects Of Kinetic Energy Projectiles

Figure 9.11 SABOT APFSDS Projectile

Figure 9.12 HEAT Projectile

Figure 9.13 Charge Projectile Detail

## 10. DE Weapons, MASERS/LASERS

Figures 10.01 & 10.02 Laser Pointers – Pilot View

Figure 10.00 Laser Pointer (small)

Figure 10.1: Charles Townes (Left) And Jim Gordon With A Beam Type Maser.

Figure 10.2: Theodore Maiman

Figure 10.3: Laser Coherence

Figure 10.4: Laser Dazzler For M-4 Rifle

Figure 10.5: Laser Dazzler In Operation

Figure 10.6: Atmospheric Influences

Figure 10.7: Laser Platform Mounted On Boeing 747

Figures 10.8 & 10.9: Laser Testing

Figure 10.10: Laser Weapon Destroying UAV

Figure 10.11: Hel (High Energy Laser) USS Ponce

Figure 10.12: Drone Being Destroyed

## 11: DE Weapons, Microwaves

Figure 11.1: Microwave Portion of the Electromagnetic Spectrum

Figure 11.2: Kitchen Microwave

Figure 11.3: Inside of ordinary kitchen microwave oven

Figure 11.4: Magnetron and Set-up Transformer

Figure 11.5 ADS (Active Denial System) / LRAD (Long Range Active Denial)

Figure 11.6: US embassy in Havana, Cuba

Figure 11.6A Two styles of US Marine Corps trucks are seen carrying the Active Denial System, March 9th, 2012, at the US Marine Corps Base Quantico, Virginia. The non-lethal weapon projects a strong electromagnetic beam up to 1000-meters

Figure 11.7: Frey Effect

Figure 11.8: CHAMP

Figure 11.9 DJI Phantom 4

Figure 11.10: Analyzing a Radar Pulse Using an R&S Spectrum Analyzer

Figure 11.11: Theoretical Detection Range Without Noise

Figure 11.12: Theoretical Detection Range With Noise, e.g., In An Urban Environment.

Figure 11.13: Theoretical jamming range

Figure 11.14: Jamming ration for CE-compliant remote control operating in the 2.4GHz ISM band

## 12. Hypersonic Drone Missiles

Figure 12.1 Comparison of speeds for various aircraft and vehicles

Figure 12.2 Commercial flight time from New York City to Orlando Florida

Figure 12.3 Categories of Hypersonic missiles

Figure 12.4 HGV trajectories compared to a Ballistic Reentry Vehicle

Figure 12.5 Detection avoidance

Figure 12.6 Russia's land-based silo launch

Figure 12.7 India Mobile Launcher

Figure 12.8 Zircon Hypersonic missile ship launch

Figure 12.9 Aircraft launched a hypersonic missile

Figure 12.10 Cutaway diagram of a basic jet engine

Figure 12.11 Cutaway diagram of scram engine

Figure 12.12 General thrust equation

Figure 12.13 Tile weights per cubic foot for the Thermal Protection System tiles used on the STS Orbiter

Figure 12.14 Cutaway diagram of the X-51A HCM with subsystems

Figure 12.15 Countries pursuing hypersonic weapon technology

Figure 12.16 Attack scenario against 3 NATO countries from a Baltic based launch

Figure 12.17 Distances between possible Chinese launch sites and targets in Korea, Japan, and Taiwan

Figure 12.18 Various Ranges for ballistic coverage from eastern Chinese missile launch facilities providing coverage in the south Pacific

Figure 12.19 Illustration of China's hypersonic tests

Figure 12.20 The Observe. Orient. Decide. Act-Loop

Figure 12.21 Cruise missiles' launch footprints and travel times to target

Figure 12.22 Possible target coverage ranges of a Hypersonic Glide Vehicle

### 13. Acoustic Weapons

Figure 13.1: Inverse Square Law, Sound Intensity

Figure 13.2 shows common decibel and Intensity levels within the hearing range.



Figure 13.3: Tuning for Oscillations  
Figure 13.4: Tuning fork oscillations over time  
Figure 13.5: Standing wave  
Figure 13.6 LRAD  
Figure 13.7 NATO OTAM ATM  
Figure 13.8 LRAD Ship Defense on USS ESSEX  
Figure 13.9: MEMS Gyroscope  
Figure 13.10 Location of Dongsha Island and Taiwan  
Figure 13.11 Spratly Islands  
Figure 13.12 Spratly Islands  
Figure 13.13 S-100 Chinese Drone  
Figure 13.14 S-100 Drone Trajectories in the Spratly Islands  
Figure 13.15 BZK -005 Chinese Drone  
Figure 13.16 Chinese UAS. Chinese Intelligence Assets Deployment in Spratlys  
Figure 13.17 Malicious Drone Activities in SCS near Taiwan  
Figure 13.18 ATS – SCREAMER

#### 14. Satellite Killers

Figure 14.1. A satellite in Low Earth Orbit (LEO) around Earth  
Figure 14.2. Classification of altitude orbits and uses  
Figure 14.3. Number of Russian (left) and Chinese (right) satellites in orbit between 2019 and 2021  
Figure 14.4. The counter-space continuum shows the range of threats to space-based satellite services  
Figure 14.5. Computer simulation of tracked objects in Earth's orbit. Red, yellow, and green objects are representations of active satellites and debris in the GEO and MEO.  
Figure 14.6. Space-based weapons

#### 15. Cyber Weapons and CBRNE

Figure 15.1 CIS Shared Threats

Figure 15.2 Infrastructure Interdependencies

## 16. Assessing the Drone Delivery Future WMD / DEW Threats and Risks

Figure 16.1 Picture of a Sea-Air Integrated Drone

Figure 16.2 Diagram showing communications between sea-air drone and remote operator

Figure 16.3 Illustration of UGVs, UGVs, and UAVs swarms working together

Figure 16.4: Image of a soldier and a Black Hornet UAV

Figure 16.5 Timeline of Industrial Revolutions,

Figure 16.6 Future capabilities of autonomous/ AI systems

Figure 16.7 Image of Industrial Revolution and the next revolution

Figure 16.8 WWII Red Cross Prisoner of War Gift Package

Figure 16.9 United States Department of Defense

Figure 16.10 MIT Technology Review

## 17. Unique Challenges of Responding to Bioterrorism and Chemical Threats and Attacks Delivered By Drones

Figure 17.1 *Chemputer* Drones

Figure 17.2 3D Printed Drone

Figure 17.3 ISIS 3D Printed Bomb

Figure 17.4 3D Bioprinter

## 18. Practical Crime Scene Investigation (CSI) Using Autonomous Systems

Figure 18.1 A Timeline of the History of Forensic Science

Figure 18.2 Law enforcement humanoid in Dubai shopping mall

Figure 18.3. Law enforcement humanoid in a public space

Figure 18.4 UGV assisting at an IED site

Figure 18.5 Investigator using a UAV at a crime scene Examining UAV use in CSI-Crash Scene Photo Royal Canadian Mounted Police

Figure 18.6. Side by Side Comparison of DS-1A and DS-1B UAVs

Figure 18.7 A Timeline of Fingerprint Firsts

Figure 18.8 Dr. Henry Lee, examining evidence

Figure 18.9 Glove demonstration from the Simpson trial. The gloves did not fit.

Figure 18.10 Automated Speed Enforcement Technology

Figure 18.11 Scenes from the Rittenhouse courtroom

## 20. Social Network implications for WMDD

Figure 20.1 A third of US Tik Tok Users may be 14 or under, Raising Safety Concerns.

Figure 20.2 Drone operator flying over rooftops

Figure 20.3 Grenade launched from DJI Phantom

Figure 20.4 DJI Operator

## 21. Tools of The Trade

Figure 21.1 A typical UAS Threat COP over one month.

Figure 21.2 Using search engines to list incident events in the past seven days.

Figure 21.3 Google.com au/ alerts

Figure 21.4 A global view of tweeted drone incidents

Figure 21.5 A collection of words for slack.

Figure 21.6 The free, weekly UAS Threat Intelligence brief Source

Figure 21.7 The UAS TIP provides global incident tracking and analysis capabilities.

Figure 21.8 The DroneSec Notify UAS TIP Dashboard

Figure 21.9 Performing a search for a specific prison Source

Figure 21.10 Viewing a running list of recent high-priority reports

Figure 21.11 Viewing a running list of UAS artifacts

Figure 21.12 A search for C-UAS related content in the Knowledge Base

Figure 21.13 The Stolen Drone Info tool dashboard

Figure 21.14 Example of a stolen drone reported on the SDI.

# Table of Tables

- 1. Drone Capabilities to Deliver Weapons of Mass Destruction / Disruption (WMDD) -Global Perspective

Table 1.1 Timeline of drones and their uses

- 3. Biological Weapons

Table 3.1 Biological Agents That Can Be Used In Biological Warfare

- 5. Nuclear Weapons

Table 5.1 Limits On Start, Moscow Treaty, And New Start

- 7. Deception

Table 7.1 characteristics of emergency behavior

Table 7.2 three perspectives on deception

Table 7.3 Deception maxims

Table 7.4 Deception

Table 7.5 Categories of Deception Channels and Methods

Table 7.6 Representative CNO Deceptive Operations

Table 7.7 Standard Taxonomy of Representative Electromagnetic (EM) Deception Techniques

- 8. DEW Primer

Table 8.1 Battlespace Dimensions

Table 8.2 Thermal Properties of Common Materials

Table 8.3 Energy losses in Propagation

- 9. DE Weapons, Projectiles, Damage

Table 9.1 Parameters affecting Target Response and Damage

Table 9.2 Kinetic Energy Required for a 7.62 mm Projectile to Penetrate Targets

11. DE Weapons, Microwaves

Table 11.1 shows several environments and the typical ranges in the ARDRONIS system.

Table 11.2 Typical Jamming Ranges

12. Hypersonic Drone Missiles

12.1 Comparison of the various aircraft and speed ranges in the sound spectrum

12.2 Speed, time, and distance comparisons at various Mach speeds from 1-30 and times to cover 1000 miles

12.3 Melting temperatures of 10 common metals.

12.4 Melting Points for Critical Electronic Components

12.5 Listing of countries with their hypersonic devices and associated speeds and distances

12.6 Steps and times from observation to launch decision for incoming ballistic missile

13. Acoustic Weapons

Table 13.1: Principal Physical Properties

15. Cyber Weapons and CBRNE

Table 15.1 Automation Levels

Table 15.2 UAS Collaboration

Table 15.3 Cyber-attacks by area of CBRNE

Table 15.4 Cyber Attack Scenarios by Area in CBRNE

18. Practical Crime Scene Investigation (CSI) Using Autonomous Systems

Table 18.1. Pros and Cons of UGVs supporting CSI environments

Table 18.2. Pros and Cons of UAS in a CSI environment

19. Navigation Spoofing and ECD

Table 19.1 & 19.2 Effectiveness Criteria

21. Tools of The Trade

Table 21.1 Important Data Points for Collection

# Table of Equations

## 8. DEW Primer

### 8.1 Thermal Conduction

#### 8.2 Thermal Diffusivity

#### 8.3 Constant Surface Temperature Case

#### 8.4 Convection

#### 8.5 Vacuum Black Body Radiation

## 9. DE Weapons, Projectiles, Damage

### 9.1 Kinetic energy of an object

#### 9.2 Newton's law

9.3 Ratio of drag force to the force produced by dynamic pressure times the area.

#### 9.4 Net Force

#### 9.5 Delta velocity in – out

#### 9.6 Universal Gravitation Law

#### 9.7 Force during flight as a function of velocity and time

#### 9.8 Constant mass $m$ , Newton's second law

#### 9.9 Newton's second law

#### 9.10 Newton's second law for bullet location (group)

#### 9.11 Drag

#### 9.12 Terminal velocity

#### 9.13 Acceleration changes with time

#### 9.14 Vertical ascent with time

#### 9.15 Vertical Ascent solved

#### 9.16 Maximum Vertical ascent

#### 9.17 $F$ net (drag)

#### 9.18 Horizontal decent fix



## 12. Hypersonic Drone Missiles

### 12.1 Speed of sound or Mach 1

#### 12.2 Speed and Distance

#### 12.3 General Thrust equation

## 13. Acoustic Weapons

### 13.1 Decibel formula in terms of Power Level (PL)

#### 13.2 Decibel formula in terms of Power Intensity Level (IL)

#### 13.2 Decibel formula in terms of Sound Power Level (SPL)

#### 13.4 Common format for Decibel formula in terms of Sound Power Level (SPL)

#### 13.5 String's resonant frequency ( $F_0$ )

#### 13.6 Decibel formula for the relationship between SPL and Sound Amplitude

#### 13.7 Decibel formula for the relationship between SPL and Sound Amplitude reference



PART I

SECTION I: CHEMICAL,  
BIOLOGICAL, RADIATION,  
NUCLEAR, EXPLOSIVE  
(CBRNE) WEAPONS AND  
PAYLOADS



# I. Drones Capabilities to Deliver Weapons of Mass Destruction / Disruption (WMDD)

by William Slofer, JR, Wilmington University

## Learning goals

- History of drones
- Weaponization of technology
- Various types of drones and their weaponization

## Weaponization

**Weaponize** “: to adapt for use as a weapon of war” (Merriam-Webster, n.d.). Throughout history, humans have become well-practiced in converting everyday devices into instruments of war and doing it with the technology available. We have seen horse-drawn carts, originally used in agriculture and transportation, turned into war chariots; black powder, developed in China for medicinal purposes, ironically lives in infamy as the building block for bullets, rockets, artillery, and an endless array of explosive devices with a list of virtually endless bi-products that have been weaponized. As humans continued to make major technological strides through the centuries, there have been colossal leaps that have improved the human condition. Unfortunately, a few individuals in power have always been who would use such advancements to satisfy their greed, lust, and desires to subjugate others. Likewise, through necessity, others have utilized

technological advancements to protect and ensure their survival by developing mechanisms or countermeasures to defend against acts of aggression. In the past, the number of people impacted by a particular apparatus was limited in scope by its destructive capabilities and more so by the ability of the assailant(s) to deliver the devices to the desired target. As technology has evolved, so has the want, need, and desire to create better and more efficient weapons and associated delivery systems that can breach or neutralize an opponent's defenses and perform large-scale attrition of enemy personnel. With numerous advancements in chemistry, medicine, aviation, aerodynamics, and nuclear science, to name a few, it has become possible for an adversary to penetrate almost any defense and eliminate almost every living thing on a continental or global scale.

Any weapon or weapon system's effectiveness depends on a viable delivery platform. In ancient times, fire weapons were often attached to animals, which became the delivery method to destroy crops or flush out enemies that may be hiding in the brush. Similarly, horses and chariots were a platform to forearm archers with speed and mobility to deliver their deadly arsenal of arrows and spears. Similarly, the small country of Britain became a world power, in large part because it developed a massive well-disciplined, and equipped navy. This navy provided Britain with a superior delivery platform based on ships. Ships allowed for the efficient transport of troops, munitions, and supplies to distant lands. As it continued to improve its technology surrounding cannons and ocean-faring vessels, it gained greater sea superiority via its floating fortresses.

It is important to understand there can and often are differences between weapons and a delivery platform that has been weaponized. This distinction will help explain how things can be repurposed for uses outside their original intent. A sad example that proves this out is commercial airliners. Such aircraft are not

built or designed to be a weapon of mass destruction. However, on September 11, 2001, two Boeing 767 jets were hijacked by terrorists and used to crash into New York City's World Trade Towers, killing an estimated 3,000 people (History.com Editors, 2018). This is an important point from a security perspective because the knowledge, accessibility, and imagination are the only limiting factors. The upcoming chapters will discuss how drones or Unmanned Aerial Vehicles (UAV) have been used in the past and how other technologies are being used as delivery systems or platforms for various types of weapons and weapon systems in the areas of surveillance, chemical, biological, and nuclear warfare, as well as other disruptive technologies. The roles they have played and continue playing in weapons delivery and countermeasure advancements.

To obtain a better perspective of drones, it is essential to know that a drone is essentially an unmanned vehicle or device, including robots, that can be remotely controlled, inertially guided, or managed via automatic systems that can be dynamically updated, pre-programmed, or both. It is also important to note that misconceptions should be debunked to appreciate this technology's possible impact on delivery systems. Although today's technology is vastly improved, drones are not new, and their use as a delivery platform is certainly not a new concept. If we look through history, it becomes apparent that drones have been used in military applications dating back to an Austrian attack on the besieged city of Venice in 1849 with balloons carrying explosives (Holman, 2009). Another of many examples is the use of the V-1 rocket, which was essentially a non-guided cruise missile but still an Unmanned Aerial Vehicle (UAV), deployed by Nazi Germany and starting in June of 1944, rained havoc on Great Britain (Wikipedia, n.d.).

### **Brief history**

Although media attention is given to Unmanned Aerial Vehicles (UAVs), other drone types and delivery platforms should not be overlooked. In addition to UAVs. Remote Operated Vehicles (ROV)

and autonomous vehicles are removed from aviation and must be considered when discussing possible delivery systems for Weapons of Mass Destruction/Disruption. Although the below timeline portrays a history of UAVs, its purpose is to show the history of drones as a general category.

**Table 1.1**  
**Timeline of drones and their uses**

| Year | Activity   | Year | Activity  |
|------|--|------|---|
| 1783 | The first-ever UAV                                   | 1973 | Israel has begun using UAVs for surveillance and scouting purposes. |
| 1849 | Shift to the military use of UAVs                    | 1985 | The production of drones in the US has increased drastically.       |
| 1858 | The first Aerial Photograph with a UAV               | 1986 | The introduction of the RQ2 Pioneer Drone                           |
| 1898 | The first Radio-Controlled craft                     | 1996 | The introduction of the Predator Drone                              |
| 1917 | The first UAV, known as the Kettering Bug            | 2006 | The US Civilian Airspace used UAVs for the first time.              |
| 1935 | The development of the first modern drone            | 2010 | Parrot Controls a drone with a Smartphone                           |
| 1936 | The drone arrived in the US                          | 2013 | Companies tested drone use as a delivery platform                   |
| 1937 | The US Navy developed the first radio-controlled UAV | 2014 | The beginning of commercial drone use                               |
| 1941 | The Radio Plane was invented                         | 2020 | Drone use for the Covid-19 pandemic                                 |
| 1943 | The Beginnings of First-Person View (FPV) Flight     |      |   |

Source: (WAcademy Editors, 2021)

**Major types of Drones/Robots**

As previously mentioned, there on more drone types than aerial, with each having its own set of operational capacities, operating



ranges, and capabilities that can be weaponized in a manner to address the theater of use or mission profile:

**Aquatic drones**

Have some unique characteristics and capabilities not found in air and land-based systems. For example, they must protect their components from water and water under extreme pressures. These devices typically come in two flavors, surface vessels or submersibles.

**Surface vessels**, also known as Unmanned Surface Vehicles (USV), have a complete range of communications options that could provide near real-time navigation and complete Communication, Command, and Control (C3) facilities for both autonomous semi-autonomous vessel management. Such a device could be used as an explosive delivery system against military or civilian ships. In the wrong hands, a properly outfitted USV, such as the one below, can be a major threat to any surface vessel.

**Figure 1.1**  
**Armed Unmanned Surface Vehicle from BAE Systems**



*Note: Navy completed trials with this system that can supersede human endurance barriers.*

Source: (BAE Systems, 2019)

Tactical USVs of this type could jam ship-to-shore communications and ship-to-ship, leading to increased angst in areas with heightened tensions. On the backdrop of an ocean, the vehicle's small dimensions provide a level of built-in stealth, giving it the capability to loiter in the ocean undetected for extended periods. It could also be fitted with an aerial system to extend its line of sight, enhancing its ability to detect approaching vessels beyond the horizon to gain an advantage for a sea-based raid or ambush. If performing a hostile act on a civilian vessel, A small USV such as this could cause large destruction and many casualties. The potential occupancy of a Quantum-ultra class cruise vessel with double occupancy would be 4,246 guests and 1,551 crew for 5,797 souls (Thakka, 2022). If there were a 50% mortality rate, approximately 2,900 souls would be lost. It should be noted that the World Trade Towers lost approximately 3,000 people. Alternately, such devices can cause ship-wide chaos and panic. For example, China has reported developing and is ready to deploy a set of high-speed USVs that can intercept, besiege, and expel targeted vessels at sea (Tang, 2021). Such devices circling or simulating an attack on a cruise ship could cause significant chaos and mayhem that the crew may not be able to contain the fear and ensuing panic.

**Submergible**, or Unmanned Underwater Vehicles (UUV), unlike the USVs, don't typically have as extensive a range of communication options to obtain and maintain navigational and real-time command and control directives. While submerged, they typically have very limited communications with the surface and therefore have limited or reduced access to satellite or land-based communication aids such as GPS. However, despite such limitations, these vehicles could potentially be the more insidious weapon delivery platform due to their ability to lurk or loiter

beneath the water's surface, awaiting a striking opportunity. The UUV technology can be used as a delivery and recovery platform for weapons created and abandoned by previous generations. A perfect example of this scenario could be retrieving weapons discarded at the bottom of the ocean. From 1918 to 1970, many countries, including the United States, participated in ocean-dumping lethal weapons as a disposal technique. One such example is the intentional sinking of the SS LeBaron Russell Briggs on August 14th, 1970, with a cargo of weapons to be disposed of. Although much of its contents are not published, few details are available. For example, it is reported to have been sunk in 16,000 feet of ocean and was scuttled with "418 steel and concrete coffins in which are embedded twelve and a half thousand rockets containing GB nerve gas, plus one land mine containing the more deadly VX gas whose contents are still top secret." (Downs, 2017). This is one of many ships lying at the bottom of the ocean with such cargo.

**Figure 1.2**  
**Dumpsites of reported chemical and explosive munitions from 1918-to-1980**



Source: (Wilkinson, 2017)

At the time, many nations considered ocean-dumping of munitions a speedy method of disposal and safe from adversaries because the pressure would crush anything in existence at that time. However, some are bottomed at lesser and others at greater depths. For example, the pressure at 16,000 feet is approximately 7,169 pounds per square inch, and no vehicle at the time would be capable of exploring such depths, let alone perform needed work for extended periods. However, today drones can map the ocean floors at such depths and provide 3d images of any vessel on the ocean bottom. Also, ROVs like the SuBastian can work at depths of 4,500 meters (14,764 feet) and for extended periods (Schmidt Ocean Institute, 2020). The advancements in underwater drone technology have put retrieval of once believed to be deposited weaponry within reach of anyone who may have the means and desire to retrieve them.

### **Robots/drones**

Contrary to popular belief, drones are robots, although many people no longer consider them as such. For discussion, the generic term robots will describe devices other than UAV, USV, and UUV types. Many people have seen robots in such roles as manufacturing, autonomous cars, warehouse transport, and retrieval:

### **Figure 1.3 Robots – Manufacturing**



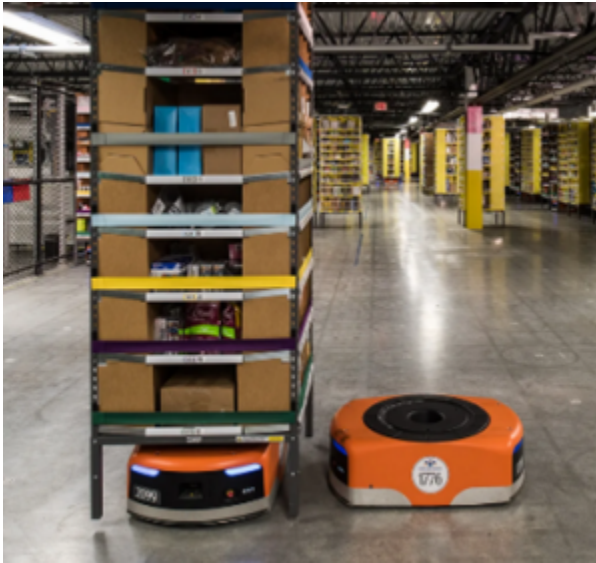
Source: (Rupnar, 2019)

**Figure 1.4 Robots – Autonomous Cars**



Source: (Safda, 2015)

**Figure 1.5 Robots – Warehouse Transport, and Retrieval**



Source: (Wohlsen, 2016)

In addition to these now commonplace robots/drones are those of the humanoid variety. The technological advancements in mechanics, computers, and Artificial Intelligence have transformed what was once science fiction into current-day reality. The military has invested billions of dollars in technology research associated with robotics. The Boston Consulting Group (BCG) has been projecting trend spending, and “In 2014, BCG projected that the market would reach \$67 billion by 2025. In 2017, we increased that estimate to \$87 billion.” (Wolfgang, Lukic, Sander, Martin, & Kupper, 2017). Some of this funding has been spent with such companies as Boston Dynamics. This engineering and robotics design company

has developed its Atlas robotic line to mimic combat soldiers' performance.

**Figure 1.6**

**DARPA funded Atlas robot developed by Boston Dynamics**



Source: (Ungureanu, 2015)

In the case of an autonomous automobile, it would be very feasible for a terrorist to transport a car bomb via such a delivery

method or cause disruption by altering its programming and driving it into a crowd of people in Times Square on New Year's Eve. In the case of this humanoid robot, an army of these 6'2", 345-pound (Ungureanu, 2015) devices will make for a formidable adversary. In the hands of a bad actor or an opposing force, they could cause mass panic on sight and, if equipped with proper weaponry, could extirpate many people's lives if unleashed in a populated area.

### **Unmanned Aerial Vehicle (UAV),**

UAV engineering in the 21st century has demonstrated unprecedented capabilities for this technology. UAVs have revolutionized aerial shots in cinematography and become essential in the pipeline and electrical tower inspections, perimeter surveillance, and the list.

**Figure 1.7**  
**Aerial drone used in movie scene filming**



Source: (Italdron, n.d.)

As discussed earlier in the chapter, most tools and technology



can be weaponized, which has occurred with drones. Although some have been designed from the bottom-up for war and war-related activities, recreational and commercial drones have been weaponized. A drone does not need to be of a Reaper or Predator classification with the ability to carry 2,000 plus pounds of bombs or Hellfire missiles to be a Weapon of Mass Destruction/Disruption.

**Figure 1.8**  
**Image of Predator B drone**



Source: (Gupta, 2020)

A smaller device with less complexity and a lower price tag can wreak havoc and massive destruction. For example, small drones have demonstrated the ability to fly in swarms. The capabilities of these swarms have been demonstrated in light shows around the world to celebrate festivals, opening ceremonies, and even July 4th celebrations.

**Figure 1.9**  
**Use of synchronized swarming drones in a night display**



Source: (Poliak, 2022)

Many drones of respectable quality can be purchased for under \$300.00 US. A bad actor could synchronize a small number of these swarming drones to target a passenger aircraft. Flying into the engine intake would cause engine damage and cause an untold large-scale devastation. A similar example of using swarms to create disruption may be a scenario where there is a large gathering, say, the Super Bowl, where a swarm of drones could airdrop pamphlets around the stadium and fly off. The pamphlets could contain a simple printed warning announcing the coming of another swarm carrying a poisonous or explosive payload that will arrive in 10 minutes. Ten minutes later, the appearance of another swarm would most likely cause stadium-wide panic, and some unimaginable number of people would be trampled or crushed to death by the stampede of people attempting to vacate the vicinity. In this case, the mere appearance of the second swarm would be sufficient to cause disruption and death.

*Note: R. K. Nichols to W. Slofer (February 18, 2022) Private*

*communication regarding Disinformation dropped from drones.*  
(Nichols, 2022)

As the bazooka and LAW rocket gave individual foot soldiers anti-tank and artillery capabilities, the drone has added aerial support. With drones, a foot soldier can survey an area to determine enemy positions and deliver ordinance to real-time identified targets. This technology has been demonstrated in Ukraine, where soldiers can transport and assemble aerial platforms in the field.

**Figure 1.10**  
**Field assembly of a drone capable of thermal imaging and delivery of 1.5kg bombs**



Source: (Borger, 2022)

Or launch a kamikaze drone against tanks or other armored vehicles. With technology such as Switchblade drones, a 2.5kg backpackable drone with a 10km range and the ability to loiter for approximately 15 minutes (Aero Vironment, n.d.), a group of soldiers

could hold off a convey. In addition to extending the versatility of the soldier, the UAV technology has also armed the civilian population. Reports have shown weaponized adaptations of recreational and commercial drones for explosive delivery.

**Figure 1.11**

**Drones are being used to drop Molotov cocktails against Russian troops in Ukraine.**



Source: (Kesslen, 2022)

**Figure 1.12**

**DJI drone carrying grenade in an improvised carrier made from a plastic jug**



Source: (McCarthy, 2021)

### **Conclusions**

The continued evolution of various disciplines such as chemistry, medicine, construction, engineering, aviation, microprocessors, Artificial Intelligence, and battery technology, amongst others, has allowed humans to heat/cool homes, travel into space, and plant/harvest food in quantities to feed the world. The human race has developed technologies that extend the range of human physical limitations, and the imagination only limits that continued advancement. One outgrowth of this image has been the development of weapon platforms such as drones, robots, and remote or unmanned vehicles that can travel via air, land, or seas and cause destruction without a person on the front line. Also, the creation of weapon systems that can destroy objects from vast distances with a beam of light or high/low-pitched acoustics. Unfortunately, the dark side of this imagination and ingenuity cannot be ignored because, in the wrong hands, it can kill millions with the push of a button. As technology has gotten faster, smaller, and cheaper, there is more of it available for recreational and commercial everyday use. This has made it possible to weaponize

things that were not previously conceived of being a weapon or part of a weapon delivery platform. It has also made it possible for bad actors to obtain or create Weapons of Mass Destruction with a simple toolset. Therefore, it is essential to utilize technology as a countermeasure for technology that some individuals or nation-states may abuse. One way to counter such individuals or entities is by understanding the available technologies and those on the horizon and anticipating possible ways they can be weaponized. Such knowledge will provide a basis for developing defenses and countermeasures that can aid in maintaining a balance of power.

## **BIBLIOGRAPHY**

(n.d.). Retrieved from <https://nypost.com/2022/03/10/ukrainians-develop-drone-that-drops-molotov-cocktails/>

AeroVironment. (n.d.). *Switchblade 300*. Retrieved from [avinc.com: https://www.avinc.com/tms/switchblade](https://www.avinc.com/tms/switchblade)

BAE Systems. (2019, July 26). *BAE Systems announces evolution in unmanned boat technology*. Retrieved from [defencetalk.com: https://www.defencetalk.com/bae-systems-announces-evolution-in-unmanned-boat-technology-72410/](https://www.defencetalk.com/bae-systems-announces-evolution-in-unmanned-boat-technology-72410/)

Borger, J. (2022, March 8). *The drone operators who halted the Russian convoy headed for Kyiv*. Retrieved from [theguardian.com: https://www.theguardian.com/world/2022/mar/28/the-drone-operators-who-halted-the-russian-armoured-vehicles-heading-for-kyiv](https://www.theguardian.com/world/2022/mar/28/the-drone-operators-who-halted-the-russian-armoured-vehicles-heading-for-kyiv)

Downs, B. (2017, December 5). *1970. U.S. Scuttles Cargo Ship Full of Nerve Gas Controversy Over the SS LeBaron Russell Briggs*. Retrieved from [billdownscbs.com: https://www.billdownscbs.com/2017/12/1970-us-scuttles-cargo-ship-full-of.html](https://www.billdownscbs.com/2017/12/1970-us-scuttles-cargo-ship-full-of.html)

Gupta, S. (2020, July 25). *The US eases export restrictions on unmanned drones and New Delhi benefits*. Retrieved from [hindustantimes.com: https://www.hindustantimes.com/world-](https://www.hindustantimes.com/world-hindustantimes.com)

news/us-eases-export-restrictions-on-unmanned-drones-new-delhi-to-benefit/story-flGfxnB4e7vKLDvOTRBKwN.html

History.com Editors. (2018, August 25). 9/11 attacks. Retrieved from history.com: <https://www.history.com/topics/21st-century/9-11-attacks>

Holman, B. (2009, August 22). *The first air bomb: Venice, 15 July 1849*. Retrieved from airminded.org: <https://airminded.org/2009/08/22/the-first-air-bomb-venice-15-july-1849/>

Italdron. (n.d.). *italdron.com*. Retrieved from Aerial Filming: Images that generate emotions: <https://www.italdron.com/professional-drones-application/aerial-filming>

Kesslen, B. (2022, March 10). *Ukrainians develop a drone that drops Molotov cocktails*. Retrieved from nypost.com: <https://nypost.com/2022/03/10/ukrainians-develop-drone-that-drops-molotov-cocktails/>

McCarthy, P. (2021, December 28). *Weaponized Drones: The Spread of Commercial-Grade Flying IEDs*. Retrieved from offgridweb.com: <https://www.offgridweb.com/preparation/weaponized-drones-the-spread-of-commercial-grade-flying-ieds/>

Merriam-Webster. (n.d.). Definition of WEAPONIZATION. Retrieved from [www.merriam-webster.com: https://www.merriam-webster.com/dictionary/weaponization](https://www.merriam-webster.com/dictionary/weaponization)

Nichols, R. (2022, February 18). R. K. Nichols to W. Slofer (February 18, 2022) Private communication regarding Disinformation dropped from drones. Carlisle, PA, USA: KSU EMAIL.

Poliak, M. (2022). *What is a drone light show? DroOne display*. Retrieved from [dronetechplanet.com: https://www.dronetechplanet.com/what-is-drone-light-show-drone-display/](https://www.dronetechplanet.com/what-is-drone-light-show-drone-display/)

Rupnar, D. (2019, March 26). *Small Industrial Robots: What Are The Different Types?* Retrieved from techicy.com: [https://www.techicy.com/wp-content/uploads/2019/03/Small-industrial-robots\\_1.jpg](https://www.techicy.com/wp-content/uploads/2019/03/Small-industrial-robots_1.jpg)

Safda, H. (2015, November 22). *Google Self Driving Car Overview and Photo Gallery*. Retrieved from Inspirationseek.com:

<https://inspirationseek.com/wp-content/uploads/2015/11/Google-Self-Driving-Car-Future-Car.jpg>

Schmidt Ocean Institute. (2020, April 14). *4500 Meter-Capable Underwater Robotic System Discovers New Species*. Retrieved from Roboticsresearch.ch: although some are bottomed at lesser and others deeper depths,

Tang, D. (2021, November 29). *China's drone ships home in on targets at sea*2021. Retrieved from thetimes.co.uk: <https://www.thetimes.co.uk/article/chinas-drone-ships-home-in-on-targets-at-sea-jsw00swb5>

Thakka, E. (2022, January 29). *Cruise News Update: January 29, 2022*. Retrieved from cruisehive.com: <https://www.cruisehive.com/cruise-news-update-january-29-2022/64893>

Ungureanu, I. (2015, January 21). *Pentagon's Humanoid Robot Designed for DARPA Challenge Got a Big Update*. Retrieved from autoevolution.com: [https://s1.cdn.autoevolution.com/images/news/pentagons-humanoid-robot-designed-for-darpa-challenge-got-a-big-update-video-91386\\_1.jpg](https://s1.cdn.autoevolution.com/images/news/pentagons-humanoid-robot-designed-for-darpa-challenge-got-a-big-update-video-91386_1.jpg)

WAcademy Editors. (2021, October 19). *Drone Timeline: An Overview of the History of Drones*. Retrieved from academy.wedio.com: <https://academy.wedio.com/history-of-drones/>

Wikipedia. (n.d.). *V-1 flying bomb*. Retrieved from wikipedia.org: [https://en.wikipedia.org/wiki/V-1\\_flying\\_bomb](https://en.wikipedia.org/wiki/V-1_flying_bomb)

Wilkinson, I. (2017, August 1). *Chemical weapons material dumped at sea: An interactive map*. Retrieved April 6, 2022, from nonproliferation.org: <https://nonproliferation.org/chemical-weapon-munitions-dumped-at-sea/>

Wohlsen, M. (2016, December 14). *Amazon Reveals the Robots at the Heart of Its Epic Cyber Monday Operation*. Retrieved from Wired.com: [https://media.wired.com/photos/593232485c4fbd732b55127a/master/w\\_1600,c\\_limit/dk\\_113014-301.jpg](https://media.wired.com/photos/593232485c4fbd732b55127a/master/w_1600,c_limit/dk_113014-301.jpg)

Wolfgang, M., Lukic, V., Sander, A., Martin, J., & Kupper, D. (2017, June 14). *Gaining Robotics Advantage*. Retrieved from bcg.com:



<https://www.bcg.com/publications/2017/strategy-technology-digital-gaining-robotics-advantage>

## 2. Chemical Weapons

**By Captain John-Paul Hood, US Army**

### **Student Objectives**

The student will be introduced to recent employments of chemical weapons within the last ten years and discover how they can be retrofitted for delivery by drone.

### **Introduction:**

#### **Case Study 1: The Potential for Chemical Weapons Release in Ukraine**

There is a “real threat” of Russia using chemical weapons in Ukraine, President Joe Biden said Wednesday before flying to Brussels to meet with leaders about stopping Moscow’s war. (Feldscher, 2022)

Russia has spent weeks falsely claiming that Ukraine is working on chemical and biological weapons programs funded by the United States. Even though the Soviet Union has been making unfounded allegations about the American use of biological weapons since 1949, Russian officials recently brought the claims to the UN Security Council and have attempted to justify the invasion of Ukraine as necessary to stop this alleged research. (Feldscher, 2022)

#### **Figure 2.1 Soldiers in Mission Oriented Protective Posture (MOPP) Gear**



Source: (Inform Napalm, 2022)

That rhetoric from Russia makes officials worry that a biological or chemical weapons attack could be on the way because it fits a pattern in which Moscow blames Ukraine or the West for something before taking that same action itself. (Feldscher, 2022)

“The main thing we’re looking at right now is the deliberate drumbeat of misinformation and propaganda and lies on this subject that has all the markers of a precursor to them using these weapons,” National Security Advisor Jake Sullivan said Wednesday at a briefing. He declined to comment on whether intelligence showed Russia moving chemical or biological weapons into position to use. (Feldscher, 2022)

Even if it does not use chemical weapons, Russia has already committed brutal attacks in Ukraine, including targeting a shelter marked as having children inside and bombing a maternity hospital. On Wednesday, Secretary of State Antony Blinken said an investigation found that Russia’s troops have committed war crimes in Ukraine. (Feldscher, 2022)

Russia is also suffering significant casualties in the conflict, making troops more desperate to use all possible tools to stop the losses. A NATO military officer said Wednesday that between 30,000 and 40,000 Russian troops had been harmed, including between 7,000 and 15,000 killed, the Associated Press reported. (Feldscher, 2022)

Before Moscow's invasion began on Feb. 24, the administration repeatedly highlighted how Russia's playbook often includes so-called "false flag" operations, spreading misinformation about Ukraine and the United States to argue that Russia had to defend itself and attack Ukraine.

"What worries us about those types of statements or accusations is they may be again laying...a pretext for them to do something more or much worse inside Ukraine," Julianne Smith, the U.S. permanent representative to NATO, said Wednesday at an Atlantic Council event. "We've been warning allies about this. We've been warning the Ukrainians. We've issued warnings to Russia." (Feldscher, 2022)

Ned Price, the State Department spokesman, said on March 9 that Russia is spreading "outright lies" and confirmed that the United States does not own or operate any chemical or biological weapons labs in Ukraine. (Feldscher, 2022)

At the NATO Summit on Thursday, leaders are expected to approve additional military assistance for Ukraine, including equipment to protect Ukrainians against chemical and biological weapons, NATO leader Jens Stoltenberg said Wednesday. Stoltenberg also strongly urged Russia not to use these types of weapons in the fight, saying he is "concerned" by Russia's statements on chemical weapons use. (Feldscher, 2022)

"Any use of chemical weapons would totally change the nature of

the conflict and be a blatant violation of international law and will have far-reaching consequences,” he said at a press conference. “We are also concerned because we know that Russia has used chemical agents before, and they have supported Assad and facilitated the use of chemical weapons in Syria.”

More than 300 chemical attacks were launched during the Syrian Civil War, NPR reported in 2019. American officials accused Russia of helping Syrian President Bashar al-Assad’s regime cover up these attacks, but Russian officials denied using chemical weapons. Instead, Russians claimed that the event was staged, and the West used the findings to justify taking military action, Reuters reported. (Feldscher, 2022)

On March 11, Biden also promised Russia would pay a “severe price” if it deployed chemical weapons in Ukraine. A biological, chemical, or nuclear weapons attack in Ukraine could trigger a response from NATO if the fallout from the attack drifted into a neighboring member of the alliance and impacted people there. At a Defense Writers Group event, Sen. Jack Reed, D-R.I., said Wednesday. (Feldscher, 2022)

“It would all be viewed through the lens of, is this an attack against a NATO country?” he said. “If a nuclear device is detonated and the radiation goes into an adjacent country, that could be perceived as an attack against NATO....It will be a very difficult call, but it’s a call that the president and the entire NATO council will have to make.” (Feldscher, 2022)

## **Case Study 2: Chemical Weapons Release in Syria and the Organization for the Prohibition of Chemical Weapons**

For much of its early history, the Organization for the Prohibition of Chemical Weapons (OPCW) was a little-known international organization quietly verifying the destruction of Cold War-era stockpiles required by the Chemical Weapons Convention (CWC).

Today, the OPCW is the epicenter of a global chemical weapons crisis and a front line in a broader confrontation between the West and Russia. (Ward, 2021)

When the CWC entered into force in 1997, it seemed that all that remained to achieve a world free of chemical weapons was to verifiably destroy declared stockpiles and universalize membership. Instead, the international norm against chemical weapons use is under siege, most prominently by Syria and Russia, two states-parties to that treaty. The world is now precariously perched on the knife's edge of a new era of chemical weapons use. (Ward, 2021)

Once the chemical weapons crisis erupted in Syria, the OPCW was forced to make a historic transformation, moving from being solely a standard arms control monitoring body to becoming an indispensable instrument of international peace and security, as recognized when the organization was awarded the 2013 Nobel Peace Prize. This new role must be strengthened to address the chemical weapons threat that has metastasized globally due to recent chemical weapons use in the United Kingdom, Russia, Iraq, and Malaysia. (Ward, 2021)

### **Ghouta: The Ieper of the 21st Century**

The hope that chemical weapons use had been consigned to the 20th century was shattered on August 21, 2013, when the Syrian military launched a barrage of rockets filled with the nerve agent sarin against the opposition-controlled town of Ghouta, a suburb of Damascus. Soon afterward, a UN investigation team confirmed the worst: 1,400 people were killed from exposure to sarin. The images of the Ghouta victims were seared into the collective conscience of humanity alongside Ieper, the site of the first major use of chemical weapons in World War I, and Halabja, where Iraqi President Saddam Hussein in 1988 perpetrated a devastating nerve agent attack against the Kurds. (Ward, 2021)

Western powers considered military intervention to deter further carnage as the world reeled in horror from the Ghouta attack. Still, when U.S. Secretary of State John Kerry and Russian Foreign Minister Sergey Lavrov met in Geneva to discuss the crisis on September 14, they achieved a diplomatic breakthrough known as the Joint Framework for the Elimination of Syrian Chemical Weapons. The United States and Russia found common ground on only one point: the Syrian chemical weapons stockpile needed to be removed and destroyed. To this end, Russia tacitly assumed responsibility as the guarantor, ensuring that its Syrian ally would not use chemical weapons and would fully declare its chemical weapons stockpile so it could be destroyed under international oversight. Syria initiated formally joining the CWC just 24 days after the Ghouta attack. During that brief period, the Assad regime had not undergone a moral conversion but bowed to pressure from the Western powers and Russia. (Ward, 2021)

By the end of September 2013, the international community had legally anchored the U.S.-Russian joint framework in a decision of the OPCW Executive Council and in a UN Security Council resolution, which included measures to address any Syrian failure to comply with the resolution's provisions or with the prohibitions of the CWC. (Ward, 2021)

### **False Declaration and Chemical Weapons Attacks**

In the spring of 2014, while Syria's declared chemical weapons stocks were being removed from its territory for destruction, the first signs appeared that Damascus did not intend to comply fully with its commitments under the CWC and the UN resolution. The unraveling of the historic joint framework had begun. (Ward, 2021)

Widespread reports emerged of chemical weapons attacks involving chlorine gas barrel bombs dropped by helicopters on opposition-controlled towns, resulting in injuries and fatalities. The claims prompted the OPCW director-general to establish a fact-

finding mission, which later determined that chlorine had been used as a weapon in Syria repeatedly and systematically from April to August 2014. (Ward, 2021)

**Figure 2.2 Civil Defense member carries a damaged canister in Ibleen village.**



Source: REUTERS/Abed Kontar/File Photo (Anthony Deutsch, 2018)

A Civil Defense member carries a damaged canister in Ibleen village from what activists said was a chlorine gas attack on Kansafra, Ibleen, and Josef villages, Idlib countryside, Syria, May 3, 2015.

During that same period, there were indications that Syria had



not fully disclosed its chemical weapons program in its October 2013 declaration to the OPCW. The OPCW Technical Secretariat, after a detailed examination of the declaration and site visits in Syria, identified troubling discrepancies, prompting the organization's director-general to establish a dedicated group, the Declaration Assessment Team, to continue engagement with Syrian authorities until the declaration could be fully verified as accurate and complete. That group has conducted more than 20 rounds of consultations with Syria, yet 19 issues remain unresolved. (Ward, 2021)

Renewed concern over chemical weapons uses in Syria prompted the adoption of another UN resolution in which the Security Council unanimously established the OPCW-UN Joint Investigative Mechanism (JIM). Since the fact-finding mission mandate was limited to determining only whether chemical weapons use occurred in Syria, the JIM was established as a panel of experts to identify those individuals, groups, or governments involved in their use. In the fall of 2016, the JIM reported its findings, concluding that the Syrian military had been involved in using toxic chemicals (chlorine gas) as weapons in three attacks in 2014 and 2015. (Ward, 2021)

Although Moscow refused to accept the JIM's findings that its Syrian ally was using chemical weapons in violation of the CWC and the Security Council resolution, it begrudgingly agreed in November 2016 to renew the JIM's mandate for another year and endorsed a new panel of experts to lead the effort. Within months, the JIM would become seized with the most devastating chemical weapons attack since Ghouta. On April 4, 2017, the Assad regime launched a sarin nerve agent attack against the opposition-controlled town of Khan Shaykhun. Damascus and Moscow quickly flooded the media with disinformation and outright fabrications, claiming the opposition itself had launched the attack to accuse the Assad regime falsely. The United States launched cruise missiles

against the Syrian airfield where the attacking aircraft originated to deter further chemical weapons use. (Ward, 2021)

Despite Russian and Syrian efforts to bury the truth of what happened in Khan Shaykhun, the JIM determined that the Syrian military had used sarin in the attack. However, it was evident at the United Nations and the OPCW that Russia would seek to block any international action against its Syrian ally, no matter how damning the evidence. Indeed, it was in direct reaction to the JIM's competence that Russia vetoed three renewal resolutions at the UN, and the JIM ended in November 2017. (Ward, 2021)

**Figure 2.3 Soldier in MOPP Gear Ready**



Source: (Stein, 2018)

### **Deepening Chemical Weapons Crisis**

Two chemical weapons attacks in the spring of 2018 escalated the threat to the international norm against the use of chemical

weapons. In March, former Russian spy Sergei Skripal, now a UK citizen living in Salisbury, and his daughter were poisoned by a Novichok nerve agent known to have been developed by the Soviet Union. The UK blamed Russia for the assassination attempt, underscoring the terrible risk the use of such a nerve agent had posed to the local community. Indeed, a resident of the adjacent town of Amesbury later died. The UK requested a technical assistance visit by OPCW experts, who confirmed that a nerve agent was used in the attack. (Ward, 2021)

On April 18, 2018, the OPCW Executive Council met to address the experts' findings. In the wake of the expulsion of Russian diplomats by the UK, the United States, and others, the meeting immediately escalated into high politics, with Russia unleashing absurd counteraccusations and protesting that it was the victim of a Western smear campaign.

(Ward, 2021)

Before the day was over, it was clear that a front line in a broader international confrontation had opened. In addition to the Syrian crisis, there was now an even more ominous Russian problem. Russia was no longer just an enabler of Syria's use of chemical weapons, protecting it at the OPCW and the UN Security Council; it was itself a perpetrator, signaling to the world that it still illicitly possessed its own dangerous chemical weapons agent. Moreover, Moscow now viewed the OPCW Technical Secretariat as an adversary. Just a week earlier, as reported by the Dutch government, agents from the Russian military intelligence branch, the GRU, were deported from the Netherlands for attempting to conduct cyber operations against OPCW headquarters in The Hague from an adjacent hotel. (Ward, 2021)

As the chemical weapons threat widened to the European continent, the crisis in Syria deepened. On April 7, multiple chlorine-filled barrel bombs were dropped on the Damascus suburb

of Douma, killing dozens of civilians. Again, a highly charged special meeting of the OPCW Executive Council was convened on April 16, just two days after joint military strikes against Syrian government facilities by France, the UK, and United States. Russia and Syria falsely claimed that the UK and the United States “staged” the Douma chlorine attacks with the help of the White Helmets, an organization of volunteer first responders in Syria that Russia has tried to label as terrorists. Within weeks, OPCW fact finders went to Douma to further its investigation, concluding that chlorine was used. (Ward, 2021)

The OPCW also faced a grim new reality extending beyond Syrian and Russian transgressions. The Islamic State group had used chemical weapons in Syria and Iraq. Moreover, North Korea, although not a party to the CWC, was advertising its chemical weapons capabilities by assassinating the stepbrother of leader Kim Jong Un with a VX nerve agent in a Malaysian airport.

### **OPCW Response to Widening Chemical Weapons Use**

With the increasing use of chemical weapons undermining the CWC, seriously eroding the international norm, and putting the world at risk of a new era of chemical weapons threats, the OPCW had to act or succumb to irrelevance. (Ward, 2021)

Deeply aggrieved by Russia's use of chemical weapons on its territory and concerned with a worsening chemical weapons crisis, the UK initiated a special session of CWC states parties to forge an international response. After Russia and Syria tried unsuccessfully to block the adoption of the agenda, the fourth special session of the conference of CWC states-parties on June 27, 2018, with broad international support, took unprecedented steps to address the crisis by adopting the historic decision titled “Addressing the Threat From Chemical Weapons Use.” (Ward, 2021)

Most importantly, the decision dealt with Syria's continued

possession and use of chemical weapons. To remedy the termination of the JIM, the conference directed the OPCW Technical Secretariat to “put in place arrangements to identify the perpetrators of the use of chemical weapons” in Syria. Director-General Fernando Arias implemented that directive by establishing the Investigation and Identification Team, which, in April 2020, found reasonable grounds to conclude that Syria conducted three chemical weapons attacks against opposition-controlled areas in March 2017. In response to these findings, the conference of states-parties in April 2021 suspended Syria’s voting rights at the OPCW. (Ward, 2021)

The decision further clarified the mandate of the OPCW Technical Secretariat in the context of the CWC. If requested by a state party investigating the possible use of chemical weapons on its territory, the director-general was expressly authorized to provide technical expertise to help identify the perpetrators of any chemical weapons attack. (Ward, 2021)

The decision also authorized the release of OPCW information to any entities established under the auspices of the UN investigating chemical weapons use in Syria. This provision would aid the ongoing investigation efforts of two such entities: (1) the International, Impartial, and Independent Mechanism (IIIM) established to assist in the investigation and prosecution of persons responsible for committing war crimes in Syria, and (2) the Independent International Commission of Inquiry on the Syrian Arab Republic. (Ward, 2021)

### **The Fight for a Future Free of Chemical Weapons**

Threats to the CWC and the international norm against chemical weapons remain ominous and unabated, as evidenced by Russia’s attempted assassination of opposition leader Alexei Navalny with a Novichok nerve agent in August 2020. (Ward, 2021)

Russia's contempt for and repeated violation of the convention are appallingly evident. Moscow has enabled and protected its Syrian ally by relentlessly wielding its veto at the UN Security Council, opposing action by the OPCW, and engaging in a calculated global campaign of disinformation and distortion. In two assassination attempts against opponents, Russia has advertised that it illicitly maintains a chemical weapons program, possesses Novichok nerve agents, and has no compunction about using such outlawed weapons against its adversaries. There should be no expectation that Russia's contempt for the convention will ebb in the foreseeable future. Indeed, Moscow's continued embrace of chemical weapons is not an isolated insult but rather part of a much larger challenge to the West. (Ward, 2021)

The Assad regime remains a long-term threat to the convention and the international norm against chemical weapons use. It views chemical weapons as a vital survival tool and a strategic counterweight to Israel. There should be no expectation that Syria will finally comply with its CWC obligations once the conflict is over. Rather, Syria should be expected to seek to produce and deploy chemical weapons as long as the Assad regime remains in power. (Ward, 2021)

### **Figure 2.4 Mustard gas artillery shells**



Source: (Details, 2012)

In the fourth special session of the conference of CWC states, parties in June 2018 began an effort to push back against these threats and avoid a return of the chemical weapons horrors of the 20th century. This must continue and intensify as it will be a long-term struggle. (Ward, 2021)

The United States must prioritize defending the CWC and lead an international effort to hold perpetrators accountable in all relevant forums. What would this entail? Chemical weapons used by North Korea and the Islamic State group are sure of concern, but they are not parties to the treaty and thus not a primary factor in the current crisis, which is largely a Russian problem. It is important to recognize that deterring Moscow from possessing or using chemical weapons or enabling their use by others is a challenging task. Increased pressure through sanctions and initiatives at the OPCW and UN General Assembly will continue to play a role. Importantly,

the United States and its allies must mount a diplomatic and public messaging campaign to counter Russian disinformation and deprive Moscow of credibility or support. This would include further isolating Russia from the international community by encouraging key states in Africa and Asia sitting on the sidelines to join efforts to condemn chemical weapons use by Syria and Russia. (Ward, 2021)

To be clear, the near-term prospects for deterring further Russian chemical weapons affronts are not favorable. The Russian chemical weapons problem is rooted in Moscow's broader confrontation with the West. It should be expected that any progress would ultimately depend on the broader political landscape. In 2013, Russia worked constructively with the United States to diplomatically address the Syrian chemical weapons crisis. However, in the years that followed, Russia chose to abet rather than dissuade its Syrian ally from chemical weapons use and then went beyond that by targeting the Kremlin's opponents for assassination with chemical agents prohibited by its treaty obligations. All these premeditated decisions helped to precipitate the wider strained situation and are symptomatic of Moscow's intractability. (Ward, 2021)

Justice and deterrence require that a diplomatic strategy defend the convention also ensure personal accountability for those individuals who ordered, enabled, or carried out chemical weapons attacks. Much of the groundwork for such an effort has been laid, but its promise may not be realized for years. (Ward, 2021)

Internationally, two UN-established entities—the IIIM and the Independent International Commission of Inquiry on the Syrian Arab Republic—are mandated to investigate violations of international law and have reported on incidents involving chemical weapons use. France has spearheaded a multilateral initiative, launching in January 2018, called the International Partnership Against Impunity for the Use of Chemical Weapons, to gather and share information to facilitate national and international



prosecution of chemical weapons perpetrators. Currently, 40 states and the European Union are members. (Ward, 2021)

The United States and its allies should intensify efforts to expand support for the partnership substantially. Although prosecutions could take years, these cooperative efforts signal the international community's determination to ensure that those who use chemical weapons will someday face a reckoning and their victims will see justice done. (Ward, 2021)

To successfully weather the assault on the convention and the norm, diplomacy must be paired with concerted international investment in the OPCW. The Technical Secretariat must remain the calm eye of the political storm. The convention does not endow the OPCW with enforcement authority. Still, it does provide the secretariat with the ability to assess the accuracy of state party declarations, investigate chemical weapons use, and provide technical assistance to states parties. Indeed, in the Syrian case, the secretariat's reports underscored that objective analysis from an independent organization is the best antidote to false claims from the perpetrator of a chemical weapons attack. (Ward, 2021)

The Technical Secretariat must remain fit for its mission in an increasingly challenging environment. That will require annually increasing the budget to adjust for inflation. The OPCW budget has remained virtually unchanged for almost a decade at about \$85 million. Meanwhile, the international community has asked the organization to do more when inflation has left it with 25 percent less purchasing power than in 2009. States-parties have responsibly provided the secretariat with many millions in voluntary contributions to fund Syria-related operations, the 2016 removal of chemical weapons precursors from Libya, and other important initiatives. Yet, such donations are not a reliable or sustainable way to maintain the organization's core activities and staffing. The OPCW is the best bargain in the international system. It should

be treated the same as the International Atomic Energy Agency, held to roughly zero real growth, with an annual increase reflecting inflation. (Ward, 2021)

Keeping the Technical Secretariat highly capable and operationally agile will also require establishing a long-term training program and a dedicated training directorate to ensure that the next generation of inspectors, investigators, laboratory technicians, chemical weapons experts, and analysts are fully trained prepared to face future challenges. (Ward, 2021)

Given that the OPCW is regularly detecting increasingly sophisticated hacking attempts, another priority must be securing the organization's computer network. The Technical Secretariat has initiated remedial measures to enhance security, but a broader revamp of the computer network, and additional cybersecurity resources are needed. These should be funded through the regular budget and voluntary contributions by states parties. (Ward, 2021)

The final requirement is to ensure the OPCW continues to be well-led. The director-general should always be a highly-skilled, experienced diplomat with expertise in chemistry being optional. Since the beginning of the Syrian chemical weapons crisis in 2013, the OPCW has been ably led by successive directors-general who have exemplified these attributes and faithfully implemented the convention while deftly navigating the diplomatic landscape. (Ward, 2021)

To paraphrase Edmund Burke, all that is needed for the evil of chemical weapons to triumph is for responsible nations to acquiesce. The CWC is a remarkable achievement in the progress of humanity, and the international community must continue to fight for it or risk losing it. The OPCW is an indispensable partner in this fight. With the broad support of its membership, the organization has taken unprecedented action to expose all

perpetrators—countries, groups, and individuals—who use chemical weapons. The world must redouble its efforts to ensure chemical weapons remain reviled and those who use them are held accountable. What started with the signing of the convention must be finished, finally turning the page on an ugly chapter in history. (Ward, 2021)

### **The intersection of Drones and Chemical Weapons**

**Figure 2.5** Agriculture Drone is spraying pesticides on crops.



Source: (Staff, 2020)

The prevailing trend for drones is constant innovation and development for a specific purpose(s), whether for a specific job, defense, or nefarious purposes. Successful criminals and terrorist organizations typically dare to do something new, never seen before, to thwart or penetrate current defenses/security

countermeasures. Nothing says an individual or group could not adapt current drone technologies to conduct acts of terror and coordinated offensive attacks on critical infrastructure or adversarial populations.

Examples of this could be combining an off-the-shelf drone aerosol delivery system such as an agricultural drone and filling its tanks with homemade chemical weapons like anthrax and ricin to spray low-yield toxins throughout a residential area. Another more recent military development would be through the use of 'suicide drone' technology to engage a point target or single building by flying into it with a chemical payload onboard.

Current models of off-the-shelf agriculture drones like the DJI Agri's T30 can carry an eight-gallon payload. They can cover 40 acres per hour with obstacle avoidance and terrain following capabilities and a range of 3.1 miles from the operator. (Drones, 2022)

### **Figure 2.6 DJI Agri's T30**



Source: (Drones, 2022)

### **A Parting Nightmare**

Did you realize that “Drones are nothing more than small crop dusters and work silently, effectively as a deployment vehicle for chemical weapons? Think of it over every agricultural field – *suicide drones avionics and programming* in a crop-dusting platform!

### **Bibliography**

Anthony Deutsch, R. (2018, April 16). *Insider*. Retrieved from the US Accuses Russia of possibly tampering with gas attacks evidence in Syria: <https://www.businessinsider.com/us-says-russia-possibly-tampering-with-gas-attack-evidence-in-syria-2018-4>.

Bowman, R. B. (2022, March 18). *Breaking Defense*. Retrieved from Ukraine is getting Switchblade. It should be just the first wave of

loitering munitions for Kyiv: <https://breakingdefense.com/2022/03/ukraine-is-getting-switchblade-it-should-be-just-the-first-wave-of-loitering-munitions-for-kyiv/>.

Crumley, B. (2022, March 11). *DroneDJ*. Retrieved from Ukraine reportedly adapts small drones to drop Molotov cocktails in war with Russians: <https://dronedj.com/2022/03/11/ukraine-reportedly-adapts-small-drones-to-drop-molotov-cocktails-in-war-with-russians/>.

Details, F. a. (2012, July). *Facts and Details*. Retrieved from Chemical Weapons: <https://factsanddetails.com/world/cat58/sub384/item2385.html>

Drones, T. (2022, April). *Talos Drones*. Retrieved from DJI Agricultural Drones: <https://talosdrones.com/product/buy-dji-agras-t30-sprayer-drone/>

Emir, C. (2022, January 13). *Interesting Engineering*. Retrieved from interestingengineering.com: <https://interestingengineering.com/the-most-brutal-mexican-cartel-used-drones-to-drop-bombs-on-their-rival>

Feldscher, J. (2022, March 23). *Defense One*. Retrieved from Threats: Chemical Weapons a 'Real Threat' in Ukraine, Biden Says <https://www.defenseone.com/threats/2022/03/chemical-weapons-real-threat-ukraine-biden-says/363523/>.

Front, S. (2020, August 12). *southfront.org*. Retrieved from Russia Confirms Usage of Kalashnikov Kamikaze Drone 'KUB-BLA' in Syria: <https://southfront.org/russia-confirms-usage-of-kalashnikov-kamikaze-drone-kub-bla-in-syria/>.

*HaberDergilik/Kara-birliklernin-silahi-havan-dronla-havlandi*. (2022, March 20). Retrieved from ssdergilik.com: [ssdergilik.com/tr/HbaerDergilik/Kara-birliklernin-silahi-havan-dronla-havlandi](https://ssdergilik.com/tr/HbaerDergilik/Kara-birliklernin-silahi-havan-dronla-havlandi)

*Inform Napalm*. (2022, March 03). Retrieved from Russia Prepares to use Chemical Weapons in Ukraine: <https://informnapalm.org/en/russia-prepares-to-use-chemical-weapons-against-ukraine/>

Kesslen, B. (2022, March 10). *Ukrainians develop a drone that drops Molotov cocktails*. Retrieved from New York Post: <https://nypost->

com.cdn.ampproject.org/c/s/nypost.com/2022/03/10/  
ukrainians-develop-drone-that-drops-molotov-cocktails/amp/

Knight, W. (2022, March 17). *Wired*. Retrieved from Russia's Killer Drone in Ukraine Raises Fears About AI in Warfare: <https://www.wired.com/story/ai-drones-russia-ukraine/>.

Lee, R. (2022, March 14 ). *Twitter*. Retrieved from Twitter @RALee85: [https://twitter.com/RALee85/status/1503494100233949190?ref\\_src=twsrc%5Etfw](https://twitter.com/RALee85/status/1503494100233949190?ref_src=twsrc%5Etfw)

Staff, A. (2020, February 04). *AgAirupdate*. Retrieved from Broad Acre Drone Spraying Unlikely: <https://agairupdate.com/2020/02/04/broad-acre-drone-spraying-unlikely/>

Stein, L. O. (2018, June 15). *War on The Rocks*. Retrieved from The Military Logic Behind Assad's Use of Chemical Weapons: <https://warontherocks.com/2018/06/the-military-logic-behind-assads-use-of-chemical-weapons/>

Valpolini, P. (2020, February 2). *European Defense Review Magazine*. Retrieved from Switchblade 600, the new Medium Range Loitering Munition: <https://www.edrmagazine.eu/switchblade-600-the-new-medium-range-loitering-munition>

Ward, K. D. (2021, September). *Arms Control Association*. Retrieved from Syria, Russia. and the Global Chemical weapons Crisis: <https://www.armscontrol.org/act/2021-09/features/syria-russia-global-chemical-weapons-crisis>

Wolfe, F. (2019, February 21). *Aviation Today*. Retrieved from Russia Unveils KUB-BLA Kamikaze Drone at IDEX 2019: <https://www.aviationtoday.com/2019/02/21/russia-unveils-kub-bla-kamikaze-drone-idx-2019/>.

# 3. Biological Weapons

**By Dr. Suzanne Sincavage & Professor Candice M. Carter**

## **STUDENT OBJECTIVES**

- To further understand the role of unmanned systems in the biological agent realm.
- To study advances in using biological agents with unmanned aerial systems.
- To develop an understanding of how the proliferation of biological attacks via drones is becoming an advanced threat.

## **INTRODUCTION**

Globally, there are well over 50 high containment (Biosafety Level (BSL)-4) laboratories, either in operation or under construction, spread throughout Asia, Africa, Europe, Russia, and the US. These labs carry out some of the most dangerous manipulations of pathogens with pandemic potential. (Lentos & Goodman, 2020) As the enhancements of pathogens rise in danger, delivery methods grow with advancements in technology.

Biological warfare agents are microorganisms like viruses, bacteria, fungi, protozoa, or toxins produced by them that give rise to diseases in man, animals, or plants when deliberately dispersed in an area. (Thavaselvam & Vijayaraghavan, 2010) The continued exploration of detection platforms and detection of bioweapons is vital. The threat of biological warfare agents, their use, and their method of attack delivery are a global concern. Biological attacks can cause a wide scale of casualties and contaminate public areas making the challenge of cleaning up unscalable. In ancient history, the well-known attempt to use biological warfare agents was during the 14th-century medieval siege of Kaffa, Feodosiya, Ukraine. (Thavaselvam & Vijayaraghavan, 2010) In this incident, the Tartars



(Mongols) who attacked Kaffa tossed dead and dying plague victims into the city in an attempt to spread the disease. In another well-documented incident at Fort Pitt, Ohio River Valley, the British troops deliberately spread smallpox among the native Indian population by presenting them with blankets and linens used by smallpox victims. (Thavaselvam & Vijayaraghavan, 2010) The importance of biological weapons was significantly advanced in the present century due to several wars and multiple threats. The accidental release of anthrax from a military testing facility in the former Soviet Union in 1979 and possession of anthrax, botulinum toxin, and aflatoxin in Iraq in 1995 point out to research and development of these agents despite the 1972 Biological Weapons Convention. (Thavaselvam & Vijayaraghavan, 2010) The combination of biological weapons and unmanned technology makes the scope of attack limitless. The delivery of a biological agent is, unfortunately, versatile. The agent can be delivered via unmanned missile or large aerial system at a Nation-state level or delivered by an off-the-shelf drone by a terrorist(s) (homegrown or foreign). Due to this type of varied attack, multiple defense options need to be developed to detect, prevent, or assist in cleaning up a biological weapon attack. When technology becomes widely available and less expensive, not to mention remotely operable, it becomes attractive to those with nefarious intent. Add the capability to deliver biological, chemical, and nuclear payloads, and the potential to be used as a Weapon of Mass Destruction by non-state actors becomes a frightening reality. (Nichols, 2020)

**TABLE 3.1 Biological Agents that can be used in Biological Warfare**

|          | Agents                       | Disease                                 | Route of infection    | Possible release |
|----------|------------------------------|---|-----------------------|------------------|
| Bacteria | <i>B. anthracis</i>          | Anthrax                                 | Aerosol               | Spores           |
|          | <i>V. parvuli</i>            | Plague                                  | Aerosol               | Vegetative cells |
|          | <i>B. melitensis</i>         | Brucellosis                             | Aerosol               | Vegetative cells |
|          | <i>B. abortus</i>            |   |                       |                  |
|          | <i>B. pasteurii</i>          | Stomach                                 | Aerosol               | Vegetative cells |
| Viruses  | <i>B. pseudomallei</i>       | Meloidosis                              | Aerosol               | Vegetative cells |
|          | Varicella virus              | Smallpox                                | Aerosol               | Virus particles  |
|          | Ebola virus                  | Ebola hemorrhagic fever                 | Aerosol               | Virus particles  |
|          | Marburg virus                | Marburg hemorrhagic fever               | Aerosol               | Virus particles  |
|          | C. botulinum                 | Botulism                                | Ingestion/Inoculation | Toxin            |
| Toxins   | <i>Staphylococcus aureus</i> | Staphylococcal enterotoxin type B (SEB) | Faecal/oral           | Toxin            |
|          | Ricin (plant)                | Ricin toxin                             | Faecal/oral           | Toxin            |
|          | Trichothecene (Fungus)       | Trichothecene T2 toxin                  | Faecal/oral           | Toxin            |

Source: (Thavaselvam & Vijayaraghavan, 2010)

### **EARLY UNMANNED BIOLOGICAL WEAPON**

American companies were expected to help with the U.S. defense department during World War II. Several companies answered the call and helped the military where they could. However, General Mills, the cereal company, really took the idea a step further, perhaps foreshadowing the abilities of the future. General Mills' first step was the creation of high-altitude reconnaissance balloons. These balloons could take photos of the Soviet Union and collect air samples to test for radioactive isotopes (indicating nuclear weapons testing). (Greenewald, 2020) General Mills suggested releasing biological agents from the balloon deep in enemy territory during the refining of balloon operations. The cereal company could grind fine particles from their cereal development. Unlike the use of an aircraft, the balloon would be able to go deep into a targeted area, avoiding blowback onto U.S. troops. The program went through a series of names as the program evolved, eventually retired as WS-124A, listed as a Weather Reconnaissance Project, a cover story used to shield the aerial biological weapons program. (Greenewald, 2020) This example demonstrates the early exploration of an unmanned aerial system that can go undetected not only for reconnaissance but as a mechanism for the delivery and detection of biological agents.

### **FIGURE 3.1 Early Unmanned BIOWEAPONS**



Source: (Airvector, 2021)

## **ATTACK**

### **Terrorist Groups**

Terrorist groups use drones to gather intelligence on high secure areas; drones are ideal for circumventing defenses. They use cameras with the visual, thermal, and infrared capability to examine their target. For example, terrorists often use consumer drones to see the layout of a secured area (i.e., nuclear plant, military base). Also, the drone allows them to observe the security practices of the facility. This gives an advantage for the attack on facility, personnel, or contents that are being protected. Weaponizing commercially available or building their own to hit targets, terrorists can easily obtain drones that can carry a small payload of a few kilograms to dozens of kilograms onboard. While the ability to carry a biological weapon needs a specialized dissemination device, it is available and can be attached by modifying the drone. Some biological products do not require crystallization for dissemination, such as animal and plant pathogens that an unmodified commercial drone could easily deliver. “If a terrorist group were able to carry out the complex tasks

of creating and using biological weapons, an intentional release of a biological weapon could be even more deadly than COVID-19”, said Dr. Goldring, who is also Visiting Professor of the Practice in Duke University’s Washington DC program. (Deen, 2020) “It is not the terrorist groups that are the problem here. It is the terrorist governments like the USA, China, Russia, UK, Israel, etc. that have the most advanced biological warfare facilities and biological weapons in the world that threaten the very existence of all humanity as Covid-19 is now doing, said Professor Boyle professor of international law at the University of Illinois College of Law. (Deen, 2020)

**FIGURE 3.2 Spraying Drone**

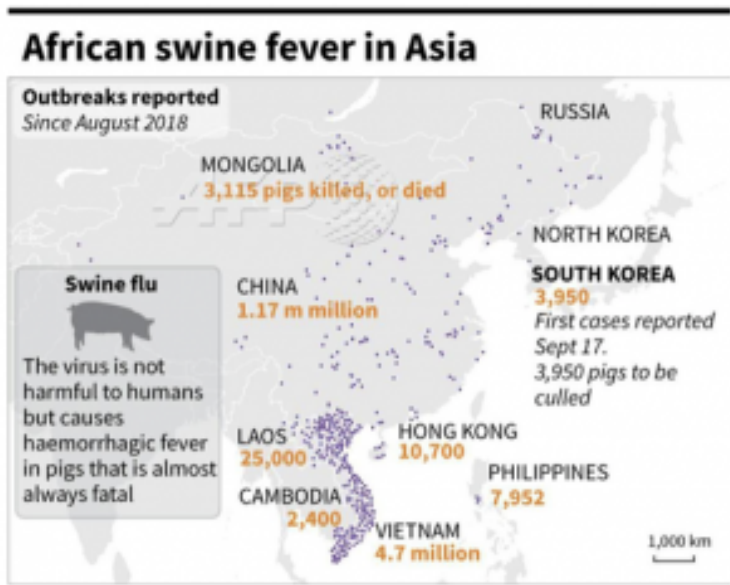


Source: (Lambert C. A., 2020)

In China, gangs use drones to spread African Swine fever to the pig population. The biological weapon has infected, killed, and spread the disease across Asia. The gang by the infected pigs at cost from the farmers then sells the meat as healthy meat and makes

a large profit. The gangs are also using misinformation on social media to drive further fear of their biological weapon, forcing the farmers to sell their pigs at a cost even if they are not infected. This attack has caught the eye of al-Qaeda and other terror networks. In January 2017, the Islamic State of Iraq and Syria (ISIS) started using commercial UAS to provide reconnaissance and targeting information against coalition forces<sup>5</sup>. It began showing interest in conducting UAS-based CBW attacks. (Lambert C. A., 2020)

**FIGURE 3.3 African Swine Fever Across Asia**



Source: (DeFranco & Giordano, 2020)

For Nation-states, could the advancements in biological weapons phase out nuclear weapons? As COVID-19 has vividly demonstrated, the risk of a catastrophic biological event is magnified by an

increasingly interconnected world, challenged by political instability, urbanization, climate change, and new technologies that make it easier, cheaper, and faster to create engineer pathogens. (Nuclear Threat Initiative, 2022) The development of gene editing gains functions capabilities by deliberately creating potential pandemic pathogens in the lab. Items like this and the significant advancement of agricultural drones should cause alarm. China is the leader in commercial UAS. (Lambert L. A., 2020). China's latest development, Agras MG 1S, is an agriculture octocopter UAS. The Agras MG 1S can carry up to 10kg of fluid spread across 10 acres with one flight. It can spray 60x faster than a manual sprayer. Imagine if this UAS was used for use with a biological weapon? Since the Spanish Emergency Unit used the octocopter to disinfect large outdoor areas during the Covid-19 pandemic, we can almost imagine that. (Silview" Costinescu, 2021)

#### **Democratic People's Republic of Korea (DPRK) (North Korea)**

The DPRK is suspected of not complying with the Biological and Toxin Weapons Convention (BTWC) and the Geneva Protocol. It is believed that the DPRK has continued to develop biological weapons despite committing to the world that they would not. In 2016, South Korea's Ministry of National Defense (MND) reported to the United States that DPRK is cultivating anthrax and smallpox as biological weapons. By DPRK defector accounts, it is believed DPRK has 13 biological weapons in play. The MND has reported a DPRK uptick in small drones infiltrating the shared border. From initial observations, the drones appear to be surveillance drones. However, through the voices of defectors, the drones have been armed with biological and chemical weapons. The defectors have also witnessed the testing of these weapons on animal populations. (Nuclear Threat Initiative, 2022)

#### **FIGURE 3.4 Democratic People's Republic of Korea (DPRK) (North Korea) Drone**



Source: (Choi, 2017)

### **DRONE SWARMS**

As mentioned in Chapter 5, drone swarms can be defined as “multiple unmanned platforms and/or weapons deployed to accomplish a shared objective, with the platforms and/or weapons autonomously altering their behavior based on communication with one another.” (Kallenborn & Bleek, 2019) Swarms have the potential to significantly improve chemical and biological weapons delivery. Sensor drones could collect environmental data to improve targeting, and attack drones could use this information in the timing and positioning for release, target selection, and approach. (Kallenborn & Bleek, 2019) Swarms make it easier to disperse biological weapons that can hang in the air to be breathed in by humans or animals. Also, pathogens and toxins payload is lighter, and the member of a drone swarm is ideal for this type of attack (i.e., crop dusting drones). The swarms are easier to adjust to

weather conditions such as rain and wind speed. Drone swarms also can combine a biological and a conventional weapon attack.

**FIGURE 3.5 Swarm of Mass Destruction**



Source: (Kallenborn & Bleek, 2019)

### **DETECTION**

The U.S. Department of Defense program Thunderstorm reviews new and emerging technologies and brainstorms how they can be used in warfare (defense and offense). In FY15, Thunderstorm focused on two areas of interest: 1) Chemical and biological detection capabilities deployed on Unmanned Aerial Systems (UAS); 2) Countering the threat of UAS with chemical and/or biological WMD payloads. (Global Biodefense Staff, 2014) The following was a list of requirements from the U.S. Department of Defense:

- A system that is carried in one backpack up to systems carried/deployed from a HUMVEE-sized vehicle
- UAS payloads that can remotely detect and/or collect and transmit chemical and/or biological data to a receiving unit at



least 1 kilometer from the sensing location.

- UAS operable by organic Chemical Biological Radiological and Nuclear (CBRN) unit personnel with minimal training and should be able to hover and land at or near the desired survey locations.
- Ground station capability to provide visual displays of the sensing data received from the mobile detection systems.
- Modular payload(s) capable of detecting: Standard G, H, and V series chemical agents in the vapor phase and/or liquid phase on surfaces or aerosolized particles; Chemical agent precursors or degradation products, priority toxic industrial compounds and materials; Biological Warfare Agents (vegetative cells, spores, and toxins); Persistent and natural flora (providing biological surveillance on current and emerging flora).
- Ground stations may utilize autonomous operation (takeoff, navigation, sample detection/collection, and landing) of the UAS utilizing standard geo-referenced satellite imagery that is either pre-loaded or downloaded on-demand from cellular or Wi-Fi networks. The autonomy interface should be simple enough to be learned in one day or less.
- UAS can operate between 0 and 1000 feet above ground level (AGL) and should have a flight time of at least 30 minutes.
- Positional accuracy of UAS should be +/- 10 meters and altitude accuracy within 1 meter.
- Command, Control, Communications, Computers, Collaboration, and Intelligence (C5I) and sensor systems that facilitate rapid detection, identification, and classification of UAS targets;
- Electronic systems that can interdict, defeat, or deny hostile use of UAS.
- Systems are providing the capability to intercept and neutralize the UAS. Both kinetic and non-kinetic solutions are encouraged and should cover both CONUS and OCONUS applications.

(Global Biodefense Staff, 2014) In January 2020, the U.S. Army was selected as the Department of Defense counter small unmanned aerial systems (C-sUAS) executive agent. The U.S. Army will now find joint solutions to counter the threats of small drones however does not include, among other items countering the biological use of UAS. The U.S. Army Chemical Corps and the Functional Area 52 Nuclear and Counterproliferation Officer Branch, in conjunction with the joint CWMD community, should update their training concepts and scenarios to better prepare the joint force for countering and defending against a UAS CBW threat. (Lambert C. A., 2020)

## **CONCLUSIONS**

The evolution of potential biological agents is exponentially growing by the month. Advancements with genes and modifications of past life-threatening diseases are already happening. Drone technology is growing rapidly and becoming a timely issue for everyone. These easy-to-obtain unmanned aerial systems are inexpensive, therefore opening the use of drones to any threat actor, any group, and any military. The combination of biology and UAS is easier than one might think. The threat is real and cannot be ignored by any Nation-state. Understanding how this biological weapon can be developed, produced, and executed is key to understanding how to defend against such an attack. The U.S. does not have a comprehensive national counter unmanned aircraft system (UAS) strategy to deal with the proliferation of intrusive, undetectable, and potentially lethal commercial UAS. (Lambert C. A., 2020)

## **BIBLIOGRAPHY**

Airvector. (2021, August 1). [3.0] *Cold War Balloon Flights 1945:1965*. Retrieved April 11, 2022, from AirVectors: [http://www.airvectors.net/avbloon\\_3.html](http://www.airvectors.net/avbloon_3.html).

Choi, D. (2017, March 30). *North Korea Reportedly Has a Fleet of*

1,000 Drones for Attacks. Retrieved April 11, 2022, from Business Insider: <https://www.businessinsider.com/north-korea-drone-attack-2017-3>.

Deen, T. (2020, November 20). *A Potential Weapon Kills Over 1.5 Million Worldwide –Without a Single Shot Being Fired*. Retrieved April 11, 2022, from Global Issues: <https://www.globalissues.org/news/2020/11/20/27042>.

DeFranco, J., & Giordano, J. (2020, January 24). *Dark Side of Delivery: The Growing Threat of Bioweapon Dissemination by Drones*. Retrieved April 11, 2022, from Defense IQ: <https://www.defenceiq.com/cyber-defence-and-security/articles/the-dark-side-of-delivery-the-growing-threat-of-bioweapon-dissemination-by-drones>.

Global Biodefense Staff. (2014, November 3). *Thunderstorm: Drones in CBRN Detection and Terrorism*. Retrieved April 11, 2022, from Global Biodefense: <https://globalbiodefense.com/2014/11/03/thunderstorm-drones-cbrn-detection-terrorism/>.

Greenewald, J. (2020, March 31). *General Mills and Biological Weapons*. Retrieved April 11, 2022, from The Black Vault: <https://www.theblackvault.com/documentarchive/general-mills-and-biological-weapons/>.

Kallenborn, Z., & Bleek, P. C. (2019, February 14). *Drones of Mass Destruction: Drone Swarms and the Future of Nuclear, Chemical, and Biological Weapons*. Retrieved April 11, 2022, from War on the Rocks: <https://warontherocks.com/2019/02/drones-of-mass-destruction-drone-swarms-and-the-future-of-nuclear-chemical-and-biological-weapons/>.

Lambert, C. A. (2020, September 29). *The Chemical and Biological Attack Threat of Commercial Unmanned Aircraft Systems*. Retrieved April 11, 2022, from Association of the United States Army: <https://www.ausa.org/publications/chemical-and-biological-attack-threat-commercial-unmanned-aircraft-systems>.

Lambert, L. A. (2020, October). *The Chemical and Biological Attack Threat of Commercial Unmanned Aircraft Systems*. Retrieved April 11, 2022, from Association of the United States Army:

<https://www.ausa.org/sites/default/files/publications/SL-20-5-The-Chemical-and-Biological-Attack-Threat-of-Commercial-Unmanned-Aircraft-Systems.pdf>.

Lentos, D., & Goodman, M. S. (2020, October 16). BNS0025 Written evidence submitted by Dr. Filippa Lentzos and Professor Michael S. Goodman, King's College London King's Coll. Retrieved April 11, 2022, from UK Parliament Committees: <https://committees.parliament.uk/writtenevidence/12902/pdf/>.

Nichols, R. K. (2020). *Counter Unmanned Aircraft Systems Technologies & Operations*. Manhattan, KS: [www.newprairiepress.org/ebooks/31](http://www.newprairiepress.org/ebooks/31).

Nuclear Threat Initiative. (2022). *Biological – The Nuclear Threat Initiative*. Retrieved April 11, 2022, from Nuclear Threat Initiative: <https://www.nti.org/area/biological/>

Silview” Costinescu, S. ` (2021, June 3). *The US ran gruesome bioweapon research in over 25 countries. Wuhan is the tip of an iceberg*. Retrieved April 11, 2022, from SILVIEW.media: <https://silview.media/2021/06/03/us-ran-grewsome-bioweapon-research-in-over-25-countries-wuhan-tip-of-an-iceberg-ecohealth-alliance-implicated-again/>

Thavaselvam, D., & Vijayaraghavan, R. (2010, July 3). *Biological warfare agents – PMC*. Retrieved April 11, 2022, from NCBI: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3148622/>.

# 4. Radiological, Electromagnetic, Drone & Metaverse Risks and Issues

**By Dr. Robert McCreight**

## **STUDENT OBJECTIVES**

Students will discuss, analyze and study:

- n the nature of intermingled radiological and electromagnetic risk today
- n the impact of drone technology and metaverse factors in shaping future risk
- n the significance of technology convergence and the emergence of CONV-CBRN
- n Indicators of threat CONV-CBRN dynamics and cognitive warfare threats after 2021
- n Radiological, electromagnetic security, CONV-CBRN, and drone risk scenarios
- n Unique future security risks and challenges

## **BACKGROUND**

When examined side by side, the nature of radiological risk and electromagnetic security may appear discontinuous. At first glance, the impact and reciprocal effects of one upon the other may seem less than spectacular. However, they signal a trajectory of security challenges and risks not readily grasped separately and in combination. Radiological emanations deemed harmful to humans must be evaluated independently from the same considerations applied to electromagnetics. When operating together and in

combination, we can find a unique set of risks and security issues that may elude conventional analysis but pose a difficult geostrategic array of threat dynamics deserving greater attention. In many ways, it depicts a massively complex and brand-new geostrategic threat puzzle that defies facile solutions. It is truly lethal to misunderstand it, incorrectly diagnose it, or underestimate it.

Radiological factors are one thing, but our imagination and the application of steadily improving technology dovetailed with neuroscience, electromagnetic, drones, and the metaverse change the entire dynamic of how we must reckon with and understand the future. Each area is arguably distinct, but they must be forced through the lens of convergence to appreciate their strategic implications. There are technologies today and emerging over the next few years; few can comprehend; however, they represent a challenge to society, security, and strategic stability. In every case, the application of dual-use technology that has every bit of potential to bring death, destruction, disruption, and decay to our world has always shown a benign face where cures, fixes, energy savings, and fantastic problem-solving technologies become the bright shiny object that distracts us from the evil side of science and tech.

Convergent strategic reality admits that in almost Newtonian logic, there is an equal and very opposite nefarious and dangerous side to the technology that wows us for every good thing that technology provides. Worst of all, when each liner technology such as robotics, nanotech, neurotech, proteomics, lasers, and hundreds of other futuristic technologies are extrapolated, you get one outcome. However, when you deliberately or accidentally blend several, you get something entirely different. (McCreight R., 2013)

When the issue of drones is added, whether air, sea, space, or via swarms directed by hostile personnel, the equation changes. Loitering drones with advanced convergence technologies usher in new immersive capabilities that define new operational realities. They open Pandora's box of emergent behavioral influences, which

require an innovative tactical response, quick adaptation, and evidence-based adjustments to a nascent threat. Suppose autonomous killer drones are assigned to devastate a target by lethal ubiquity, the overall threat equation changes. Drones enable the autonomous or indirectly managed controlled and focused assembly of independently equipped aerial vehicles about the size of a microwave oven, which can deliver medical supplies, pizzas, wonderful nature photos, or rain down death and mayhem from the sky. Dozens of drones can swarm collectively and create a legion that defies easy defense or nullifies haphazard protection by delivering harmful or lethal packages against its intended target. Again, everything we suspect is friendly and helpful is a subtly hidden monster when re-engineered for destructive purposes.

When **convergent technology dynamics [CONV]** are included with drones and combined with the radiology and electromagnetic factors, we have touched upon the entire analytical lens through which the threat is seen. That nefarious blend of various technologies represents a conglomeration of risks that dramatically alters the spectrum of potential threats we must address. Geopolitical rivals will exploit its alleged potential, unveiling a new array of threats capable of shifting the global balance of power to allow some insidious and evil entity to harness its latent capabilities in ways we don't expect, plan for, or foresee. Myriad convergence bundling by itself unleashes deployed mayhem laden with unintended consequences requiring adaptive human-machine threat analytics we can only imagine.

We must reconsider our understanding of CBRN now that 2022 is upon us. Older traditional views of CBRN are insufficient for tomorrow's risks. The deliberate blending of heralded breakthroughs that quantum computing offers, alongside robotics, nanotech, 5th generation chemical/biological weaponry, neuroscience, and other cutting-edge scientific fields, suggests insidious risks. Their inherent convergent risks magnify the presumptive threat equation and overall strategic terrain after 2022.

The scope and scale of CBRN after the 9-11 attacks were

understood to mean one thing largely accurate for its time. Today it looks much different and is likely to morph further in character and complexity by 2030. Worse of all, complex intervening variables have made CBRN, as we once understood it, tougher to grasp, identify and defeat. We find ourselves amid the Convergent CBRN revolution or what the author calls—**CONV-CBRN**. The era of convergent CBRN [CONV-CBRN] vastly complicates our grasp of future threat and risk equations, theories, and geostrategic applications. Worst of all, we lack the metrics and technologies to subdue it. What is the scope and trajectory of CONV-CBRN? Can we posit it in revolutionary terms as a force multiplier and strategic game-changer after 2022, especially in a dangerous dual-use universe of illegal arms transfers, rampant technology theft, and perpetually contending political actors and interests? Can it be predicted? Controlled? Redirected? Curtailed? Managed?

One salient insight from infusing AI and cyber elements into the future threat scenarios involving CONV-CBRN is to factor in yet another geostrategic variable—the evolving issue of the metaverse. We focus on deliberate, engineered, and directed blends of CONV-CBRN, radiological and electromagnetic factors, and advanced drone technology into something entirely new and never before seen. Adding in the metaverse and its variables makes it mind-boggling and blending what is real with what is virtual taxes our discerning skills and senses to a degree of uncertainty and caution that creates a strategic gap using A/R plus V/R plus reality.

The metaverse is largely undefined with any precision. Yet, it presumptively suggests a computer-generated world in parallel with reality which features technologies enabling *augmented reality* [AR] and *virtual reality* [VR]. Future sponsors and architects of the metaverse can expand its capabilities without limits and boundaries between what is real and what is virtual, becoming harder to discern. Some refer to it as a place or a space where replicas of real life can be created, sustained, and interact. IT expert Matthew Ball claimed in 2020 that the metaverse is “an expansive network of persistent, real-time rendered 3D worlds and simulations that [...]



*can be experienced synchronously by an effectively unlimited number of users, each with an individual sense of presence.”* According to his definition, the metaverse is a product or service with seven core attributes: persistence, synchronicity, and interoperability with the arguable layer of 3D aspects. (Ball, 2020)

In effect, the metaverse comprises whatever can be inserted or attached to it from genuine reality or the sphere of AR/VR ever-shifting and chameleon-like character. Here we must add to the points already made to emphasize that the existence of CONV-CBRN, mixed with radiological and electromagnetic tech issues—while inserting the possibilities derived from drones—suggests a new and staggering threat and risk set of issues in 2022. As such, the net implications of which radiological and electromagnetic technologies inform, support, or guide the operational definition of the metaverse are largely unknown. However, it is arguably a strategic arena for battle as its IoT, AI, cyber, nanotech, neurotech, biotech, and robotic aspects are configured to compete for dominance in an undefined space. Are we even equipped to conduct an objective risk analysis of this aggregation? Can we deal comprehensively with its consequences and downstream effects? Likely not. (McCreight R., *Convergent Technology and Future Strategic Threat*, 2013)

This aggregate array of threats and risks will transform the global geostrategic landscape for at least another decade or longer. This creates a geostrategic puzzle of gigantic proportions where neither the diagnostic strategies nor technologies designed to fit the CONV-CBRN threat adequately address its evolving nature and immediate emergence. Puzzle ingredients mix CONV-CBRN with cutting-edge dual-use science and technology mixing in radiological, electromagnetic, and drone aspects, a keystroke from our less insulated reality.

### **RADIOLOGICAL THREATS—EVERYTHING OLD IS NEW AGAIN**

When the spectrum of radiological threats is examined at the end of 2021, we find a mix of old traditional and some new issues

deserving of attention. This would necessarily include measures and technologies designed to mitigate anything resembling a nascent radiological threat. But the spectrum of radiological threats—both real and imagined—is larger and more complex. CDC says radiologic threat agents can issue from intentional or unintentional releases of dangerous radioactive materials. Unintentional emergencies include Nuclear Reactor Accidents and Transportation Accidents like a spill of radioactive material from a truck or train. However, intentional acts can include:[1]Contaminating food and water with radioactive material; [2] Spreading radioactive material into the environment; [3] Using conventional explosives mixed with highly radioactive substances – this is called a dirty bomb; [4] dispersing radioactive elements via wind currents or natural weather traffic patterns; [5]bombing or destroying a nuclear reactor; [6] causing nuclear material to spill while in transit as waste products from nuclear plants; [7] theft of radioactive materials and course [8]exploding a nuclear weapon. (CDC, 2022)

After the infamous 9-11 attacks, there were profound fears that terrorists could either create an *improvised nuclear device* [IND] or somehow match-high explosives with radioactive material or fissile material. The central fear was rooted in the risks of Radiological Dispersion Devices [RDD] and the parallel concern about direct attacks on nuclear power plants where surprise assaults by terror groups could trigger. Chornobyl or Fukushima tragedies release tons of radioactive steam via penetration of the processing core, disabling its safety controls or otherwise enflaming outdoor pools of spent nuclear fuel points to other risks. It was also assumed that terror groups after 9-11 were inclined to acquire, purchase, or steal enough radiological or nuclear material to fabricate a real or ‘dirty’ bomb. (Bunn, 2021) (DHS, Radiological Attack Fact Sheet, 2022)

A politically-charged chameleon type aphorism like the metaverse invites scrutiny. On the one hand, people would like to confine the metaverse to an extrapolation of the internet and praise it as simply the IoT and nothing more. However, other legitimate aspects of the metaverse, such as its 3-D properties exploiting neuromechanics

and biomechanics, are not well understood. It blends spatial computing capabilities, game engine capabilities, brain-computer interface options, digital twin potential, and parallel replica utility using engineered virtual reality. Its tendency to employ advanced algorithms to exclude humans from controlling or monitoring their covert activities—or making them virtually undetectable—is not beyond comprehension. So, sorting out aspects of hidden connectivity between RF, radiological, and the electromagnetic spectrum remains puzzling exactly because their relationships are opaque and diffuse. Not easy to identify, decode or discern. Their obvious and unintended outcomes linger to haunt us.

Radiological must be understood in this way— ***a radiological weapon means any device, other than a manufactured nuclear explosive, specifically designed to employ radioactive material by disseminating it via crude explosion, aerosol, injection, dispersion, or aerial spraying to cause human destruction, damage, or injury, employing the emitted gamma or beta radiation over the years produced by the decay of such material.***

This term encompasses most objects created expressly to distribute harmful radioactive materials as broadly and extensively as possible by various means. This is quite different from the risks and security implications of EMP attacks. Electromagnetic Pulse triggered by a high-altitude nuclear blast inflicts widespread electronic failure and chaos on organized society with minimal radiation effects. (Reports, 2018)

Likewise, it is also important to vehemently disprove those who mistakenly claim Iraq had no WMD—the fact is Iraq's technical infrastructure. Its resident nuclear science experts had the sophisticated capability to do so eventually without ever devising a tested weapon. In effect, the capability to produce WMD is sacrosanct and cannot be severed conveniently from the possession of actual WMD weaponry. (Scientists, 2009)

Good radiation can play a part in cancer therapy, blood irradiation, medical and food sterilization, structure and equipment testing, geologic exploration, and instrument calibration. Gamma

rays emitted by cesium and cobalt can kill germs multiplying in your meat and make your apples last longer. Affirming the positive value of radiological is important. (Scoles, 2022)

Finally, the related issue involving the possible effects of radiofrequency-electromagnetic field (RF-EMF) on the human body requires an appreciation for several factors which indicate harmful EMF impact on animal models. RF-EMF can induce changes in central nervous system nerve cells, including neuronal cell apoptosis, changes in the function of the nerve myelin and ion channels. Therefore, it is necessary to study the biological response to RF-EMF in consideration of the comprehensive exposure concerning the use of various devices by individuals. In this review, we summarize the possible biological effects of RF-EMF exposure. ((Seoul), 2018) (Ju Hwan Kim, 2019)

Security and safety are paramount with just over the 25 research reactors on college campuses. These reactors have a limited amount of radioactive material on site and pose a low risk from radiation and the theft of nuclear material. The NRC inspects the reactor's security and emergency plans and its operations and design to ensure public health and safety protection with increasing requirements for material that is less attractive for theft or diversion. The NRC continues to inspect research and test reactors to ensure compliance with all NRC regulations to protect t public health and safety. (NRC, 2017)

In sum, the risks of radiological weapons today after 2022, just as they were at the end of WWII, remain embedded in the variety of mechanisms and inventions which enable the widest possible distribution of harmful radioactivity and which are inextricably linked to evolving technology that more precisely and reliably magnifies that distribution. While the overall threat of radiological emergency or deliberate attack seems relatively low, the risk of accident, sabotage, terrorism, or system malfunction cannot be easily dismissed. Since events like Three Mile Island, Chornobyl, and Fukushima, we have learned that natural disasters, operator error, and systems malfunction can cause a serious radiological

emergency with contaminant radiation dwelling in the affected area for many decades rendering the compromised area uninhabitable. Future radiological weapons will grow in complexity and residual lethality as future enabling and supporting advanced technologies further magnify and directly target human groups in cities and heavily populated areas of industrial activity where radioactive contamination can harm many.

### **THE NATURE OF RADIOLOGICAL, ELECTROMAGNETIC, AND DRONE RISK INSIDE THE METAVERSE**

It is now a broad and ill-defined strategic question connected to several technical challenges, asking how the risk terrain after 2022 should be understood for CONV-CBRN events and its connection to other emerging technology? No easy answer comes to mind as the blended and re-engineered mix of convergent technologies, supported and enabled by AI. Cyber enhancements create a milieu of threat dynamics never before seen. Risk estimation becomes a blend of alchemy, science, technology, countermeasures, and conjecture supplanted by the imperfections of warning intelligence. Victims of targeted epigenetic neuromodulation rooted in electromagnetic, nano pulsed RF [radio frequency], and acoustic pulse combinations cannot fathom how they have been neurologically compromised or wounded. The medical profession has no diagnostic framework or treatment architecture and therapeutic strategy to treat these victims of so-called Havana Syndrome and tends to write them off as psychotic or hallucinogenic. The key is that a precise neuro-cognitive strike has been inflicted. Nobody can verify it has happened—neither the victim nor the so-called medical professional who examines the victim. So, we dwell in an era of neurocognitive warfare, ignorant of its effects.

If we absorb targeted neurological attacks which go undetected and evidence of covert neurological harm cannot be verified, we are in a season of strategic jeopardy. This is gradual and insidious as propaganda, disinformation, deceit, information warfare, and social

media manipulation slowly and deliberately chisel away our rational thought and analysis filters. We fall victim to Psychological Operations [PsyOp] without realizing we have been duped until too late. Deep Fake technology using President Obama's voice artificially imposed on another's body and face exemplifies the calculated deception aimed at mass influence. The fact that many millions can fall victim to this 'deep fake' scheme and be falsely manipulated is technologically possible. However, we would like to believe otherwise.

One chief issue involves strategic warning and the specific indicators and sensors which reflect a robust technology designed to signal and alert friendly nations of impending CONV-CBRN incursions and attacks of a non-kinetic nature. How should that be done? How would future societies discern when they are under real-time vs. virtual threats of immediate attack? How would the virtual and the real components of such a threat be sorted out? What merged versions of radiology, electromagnetics, drones, and the metaverse can be ably diagnosed as a threat and deterred given the near-term availability of their CONV-CBRN options 2022–2025??

How has the existence of CONV-CBRN itself changed the very definition of a strategic threat? What is the near-term vs. long-term impact on society and security? What is infrastructure governance necessary to curtail and control its worst effects? What optional and viable countermeasures and deterrent technologies can be assembled to thwart the incipient CONV-CBRN threat after 2022? When the AI, cyber, and metaverse aspects are included in such an analysis, does this signify an unbounded mix of virtual and real weapons platforms that can have both a biophysical and a neurophysiological effect? If combined radiological, electromagnetic, and drone technologies inflict widespread neuro-cognitive harm in undetectable ways, what does that imply for reserve use of kinetic firepower? If a target population is rendered incapable of performing basic human behavioral tasks or rational analysis by such technology can, we say the attacker has *'won the*

*battle without firing a shot*, as ancient Chinese philosopher Sun Tzu argued in the 6th century BC essay ‘The Art of War.’ (Tzu, 475 – 221 B.C.E.)

Given the pervasive global existence of CONV-CBRN technologies among the world’s leading military and economic superpowers, this begs how geostrategic risk should be constructed and defined. If this threshold threat dynamic is another decade distant, we may have enough time to contend with it. However, the CONV-CBRN warfare era augmented by drones is already upon us then our efforts to deflect or mitigate its worst effects will be a perpetual catch-up game. Therefore, risk analysis itself is hampered, blinded, and constrained by a myopic vision of what convergent technology suggests is possible.

Failure to imagine the most sweeping scope of high-tech threats immediately as derived from the CONV-CBRN risk terrain coupled with AI, cyber, metaverse and drone technology is to miss the most colossally disruptive tidal wave of the 21st century. Who can reliably estimate the strategic risks and nuanced implications of a carefully engineered and convergent blend of quantum, robotics, nanotech, biotech, drones, AI, cyber, and its operational significance in a mixed metaverse? Are we even equipped to conduct and calibrate an objective risk analysis of this aggregation? (McCreight R., Convergent Technology and Future Strategic Threat, 2013)

## **RADIOLOGICAL AND ELECTROMAGNETIC RISKS AND THE ERA OF COGNITIVE WARFARE**

Technologies derived from the electromagnetic spectrum can damage the human brain, especially if targeted nano pulsed RF and acoustic waves are used to adversely affect cognition and normal brain function. *Neurological vulnerability* [NV], the dawn of what the author terms ‘NeuroStrike’, and the era of cognitive warfare are here now. Not decades away as some would view it. The central thesis is that we have been amid hostile brain hacking and elementary forms of cognitive warfare for at least 12 years. NV attacks via the mastoid bone, vestibular, and otolith systems and our

proprioceptive systems by harmful externally based technologies have been targeting persons for quite some time. This is integral and crucial to grasping future CONV-CBRN conflict rather than seeing it as excessive. (McCreight R., NeuroStrike Weapons and the Strategic Domain after 2020: Caution, 2021)

While IO and influence operations in 2014 were not seen strictly as 'cognitive warfare,' the overall intent was to steer popular confusion towards an empathetic view of Russia's invading forces in Crimea, offering important clues for the interplay between IOs kinetic activity. The course of events – from the takeover of parliament in Simferopol and dismantling of the Ukrainian military presence on the peninsula to the disputed referendum and the de facto annexation of the area to the Russian Federation – was accompanied by intense activity aimed at controlling the flow of information and influence public opinion in ways designed to divert civil attention away from Russia's operational battle aims. This activity extended across the entire spectrum of communication and included kinetic, cyber, and IOs targeting the physical, logical, and social layers of communication. This must be understood as part of Russia's Information Warfare [IW] campaign. The interplay between different levels of information – from the political leadership of President Putin at the tip, via the traditional media to the grassroots level in social media – and propaganda appears to be an important core element of Russian IW.

One of the core narratives surrounds Russia's position in the world: a misunderstood counterweight to Western liberal values and a misjudged historic superpower. This narrative is slim and can be easily absorbed by the general population and even groups abroad. For example, nationalist groups focus on Russia's historical position of power, while communist groups discuss Russian antagonism to capitalism regarding the Soviet era. (Jaitner, 2014) Today we witness it daily in the bloody Ukraine conflict as a necessary companion to outright murder.

The more sophisticated and the non-kinetic aspects of stealthily influencing perception, thinking, and normal brain functions



created an invisible and undetectable technology that Russia used systematically on our diplomats in Havana, Cuba-known as AHI. The use of covert technology designed to disable and degrade human thought, induce psychomotor disruption and a variety of discernible symptoms like loss of balance, speech erosion, tinnitus, frequent headaches, and other documented issues must be viewed as the current generation of cognitive warfare technology which continues to puzzle neuroscience experts and seasoned medical professionals. (Sciences, 2020)(Haines, 2022) Even today, we wrestle with the bona fides of those complaining of AHI and how best to diagnose and treat them. The absence of a consensus case definition and divergent theories on therapeutic strategies loom. In the interim, the threat continues to our diplomats, IC staff, and military leadership posted overseas and a few disturbing cases here at home. As long as the enemy targets our personnel and attacks them in small groups of 12 or less, we can safely relegate these bizarre events to the bottom of the priority pack. (Nelson, 2022)

Radiation-induced brain injury can result in cognitive dysfunction, including hippocampal-related learning and memory dysfunction that can escalate to dementia. Our current understanding of the mechanisms behind radiation-induced brain injury, focusing on the role of neuroinflammation and reduced hippocampal neurogenesis, remains useful. (Turnquist, 2020) (Linda Douw, 2009) Risk assessments of the radiological and electromagnetic impact on normal brain function and neurological well-being are not as further in research as we might expect or desire. Now 2022 finds us in an unrestricted cognitive warfare battlefield where multi-domain operations must somehow account for these factors blended with various non-kinetic technologies. Where are we then? The array of radiological risks arising from fissures in nuclear plant containment towers, mixing high explosives with radiological elements, and ambient radiation from various medical and food processing sites are reflective of well-known risks. Do we grasp the full array of radiological risks which may arise? What about the radiological risks in our immediate

environment, such as **radioactive isotopes in potable water systems or derived cadmium from disturbing** sandy grounds, which may be more prevalent than imagined. (EPA, 2012)

**FIGURE 4.1 Where Do Mobile Phones Fit?**

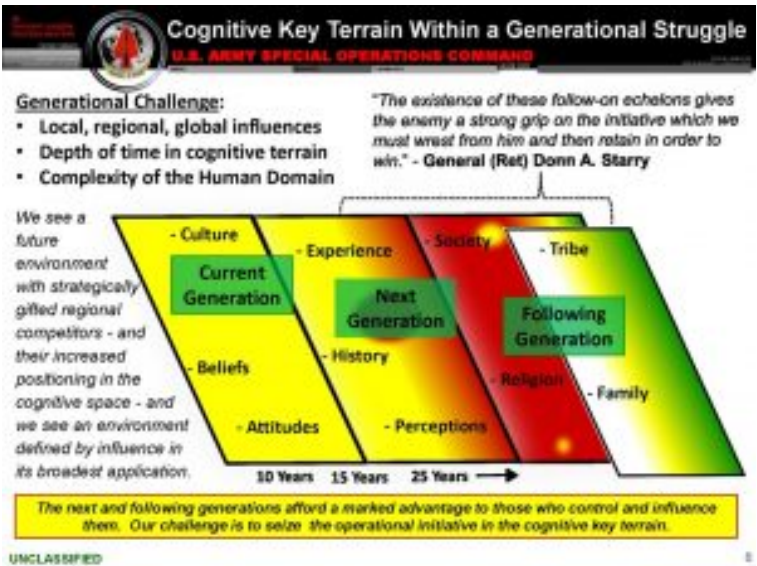


Source: <https://www.sciencemediacentre.co.nz/infographics/> (sciencemediacentre.co.nz, 2022)

The fact that US military briefings and reports referred to this phenomenon in 2015 and 2016 as an ambiguous yet burgeoning hostile and clandestine threat that US forces and allies must contend with doesn't alter the fact that simple awareness of cognitive warfare in its earliest stages took a back seat to sexier and more sophisticated weapons systems. Hypersonics, cyber-attacks,

and other systems crowded out sustained attention to cognitive warfare so consistently that the interim response was limited, cautious, and late by the time we had verifiable victims of it. This briefing slide from 2015 illustrates the limited strategic view our SOCOM leaders attributed to the risks of cognitive warfare. (SOCOM, 2015) If the threat is recognized as valid, but no countermeasures are formed to neutralize it, the net result will grant a battlefield advantage to those possessing this disruptive technology.

**Figure 4.2 Cognitive Key Terrain Within a Generational Struggle**



Source: (Ryan, 2014)

**THREAT                      DYNAMICS—RADIOLOGICAL                      AND  
ELECTROMAGNETIC ISSUES POST 2021**

The spectrum of radiological risk to society and security has become obscure, opaque, and otherworldly. Obscure that many believe radiological risk, including the prospect of such weapons as a 'dirty bomb,' is a distant worry dwarfed and stoked by seven decades of apocalyptic nuclear war fears. The radiological risk was also seen as opaque by many. Some experts saw a radiological weapon's technical requirements and instrumental risks as low probability, unlikely and speculative. However, events like Chernobyl, Fukushima, and the environmental calamity involving Cesium-137 at Goiania made us reckon with the radiological risks we tolerate in exchange for a measure of reliable nuclear power and the application of nuclear medicine technologies. To define our terms for this purpose, a widely cited descriptive definition of a radiological weapon reads— ***a radiological weapon means any device, other than a manufactured nuclear explosive, specifically designed to employ radioactive material by disseminating it via crude explosion, aerosol, injection, dispersion or aerial spraying to cause human destruction, damage, or injury, through the emitted gamma or beta radiation over the years produced by the decay of such material.*** This term encompasses most objects created expressly to distribute harmful radioactive materials as broadly and extensively as possible by various means. (DHS, countering-weapons-mass-destruction, 2022)

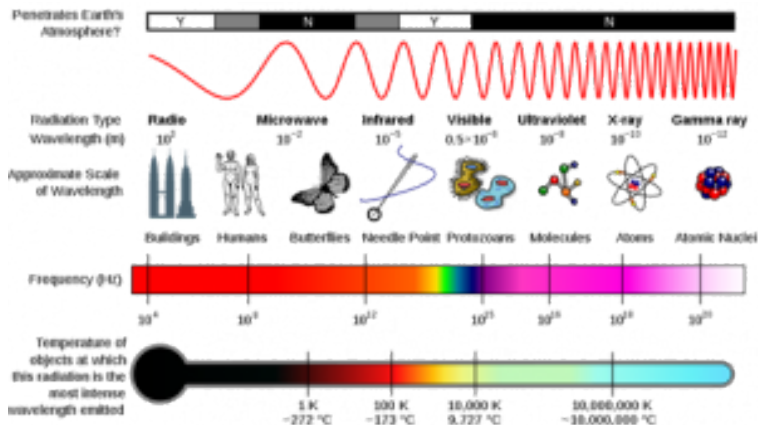
Congressional, press, and academic discussions were gradually discounted in favor of the increasingly complex, insidious, and divergent future technologies expected to damage our security more readily or effectively. This was underscored in great detail by the NERC EMP task force report to Congress in 2019. (NERC, 2019) This report drew attention, however temporary, to the implied crisis of radiological risks emanating from a poorly understood radiological threat. (NERC, 2019). In addition, we are aware of the so-called 'dirty bomb' issue where high explosives can be attached to detonate with highly radioactive substances like Cobalt 60 or Strontium 90 and render an entire area of many square miles contaminated for decades. Imagine where other radiological risks

and dangers can eventually be linked to CONV-CBRN, electromagnetic, drone, and metaverse exploitation. That intent on evil is well aware of it.

We saw the significance and impact of using passive nuclear power plants in the Russo-Ukraine war in 2022 as pivotal in changing the threat dynamics of the battlefield. There are claims and counterclaims about whose weaponry and artillery targeted the main reactors at Ukraine's largest nuclear plant. On February 5, 2022, Russia took control of Europe's largest nuclear power station in Ukraine after a shelling hit it. Both sides argued the other put the plants' safety in jeopardy. Ukrainian officials said a fire started at the Zaporizhian plant after being shelled by Russian troops. The Russians claim their part. They did not shell the facility at all. To everyone's relief, the UN's nuclear watchdog IAEA said radiation levels and the safety of reactors were not affected. Here the sterling issue is the contending and contradictory claims which cannot be readily verified and if containment was breached. Sadly, the issuance of radioactive gas and fumes or setting spent fuel ponds afire would have triggered a radiological disaster of international proportions. That crisis would have thwarted serious attempts to discern who attacked the site. So, post-disaster attribution, where responsibility is assigned to those held liable for the attack, becomes an ambiguous and ill-defined mess. (News, 2022)

Zeal for upgrading interest in radiological issues waned as experts concentrated on the power of nuclear weapons alone. When one inspects the electromagnetic spectrum in detail, we find the following distribution of phenomena which identify where certain electromagnetic technologies exert a radiological series of effects—some lethal and harmful—others much less so.

### **Figure 4.3 Radiological Spectrum//Earth, Sky, Net**



Source: (EarthSky – Earth, 2019)

From a quick scan of this chart Figure 4.3, one can readily point to areas on the electromagnetic spectrum where divergent waves and beams can affect human life in a harmful or benign way. When the electromagnetic set of issues is seen through radiological threats, we must also accept the proven negative influence of pulsed radiofrequency [RF] signals to inflict both biophysical and neurophysiological harm. A 1950s-era program known as “Atoms for Peace ” that US President Eisenhower launched to encourage a larger role for private industry in developing nuclear-power plants worldwide allowed nations bereft of nuclear weapons to pursue nuclear power still covertly and slowly use their nuclear power stations. They could enrich uranium and engage in covert processing of fissile material outside conventional inspection and review systems. In addition, the history of intelligence theft of nuclear technology contributed to the increase of nuclear weapons states to well over 12 nations. [US, Russia, China, UK, France, North Korea, Iran, South Africa, Brazil, India, Pakistan, and Israel possessed

robust nuclear infrastructures with other undesigned nations. (Library, 2022)

In physics, *electromagnetic radiation* (EMR) consists of electromagnetic (EM) waves propagating through space, carrying electromagnetic radiant energy. It includes radio waves, microwaves, infrared, (visible) light, ultraviolet, X-rays, and gamma rays. These waves form part of the electromagnetic spectrum and span the risk intensity from serious to harmless, including frequencies used for communications signals (as for radio and television broadcasting and cellphone and satellite transmissions) or radar systems. (Scarpati, 2021) (AARL, 2022) (FCC, 2022) See Figure 4.1. (sciencemediacentre.co.NZ, 2022)

Non-nuclear weapons states which have nuclear power plants on their soil number 314 according to the IAEA, which oversees global nuclear power reactors. (IAEA, 2018) Here the raw significance of these power reactors is the inherent risk of operational accident, terrorism, system safety breach triggered by natural disasters, and disintegration of safety systems in aged reactors approaching 50 years of useful life. They also reflect a potential nuclear weapons option.

In sum, the risks of radiological weapons today after 2021, just as they were emerging at the end of WWII, remains embedded in the variety of mechanisms and inventions which enable the widest possible distribution of harmful radioactivity due to terrorism accidents, operator error, or natural disaster. The overall risks from residual radiation after a nuclear blast are significant and overwhelming—so too are the many other radiation risks arising from the focused application of emerging technologies. (FAS, 1998) (globalsecurity.org, 2022) (NATO)

### **GRASPING THE NON-KINETIC ASPECTS OF CONV-CBRN**

Added to the scope and depth of CONV-CBRN when drones, AI, Cyber, and electromagnetic are infused into the threat picture is to assess the significance of non-kinetics in the milieu. Here we suggest a wide variety of non-kinetic but truly disabling, disruptive,

and debilitating technologies orchestrated by a determined foe who seeks to undermine and weaken his political civilian and corporate executive ranks via these measures. A wide variety of *effects-based operations* [EBO], which often go unnoticed or ignored in protracted 'ghost guerilla warfare' efforts, can occur outside notice. This is the emerging domain of non-kinetic warfare [NKW]. *Nonkinetic warfare* [NKW] options available to an enemy who can influence, persuade, enflame, discourage, overwhelm, weaken, or confuse targeted populations as part of a broader geopolitical offensive running over several years exerts its insidious and impressive effects where the focus is more psychological, more sociocultural, and more subtle as it stealthily undermines the fabric of social cohesion and identity. NKW disturbs and exploits the popular civil-social-urban environment behind an unsuspecting military to the extent that it erodes the foundation of community support for its forces and their strategic disposition.

NKW is not 'asymmetric warfare' as we often define it, where a battle between unequal belligerents is balanced via a determined insurgency or resistance movement capable of equivalent destructive outcomes inflicting harm on a superior force with unsophisticated tools and technologies that can be exercised frequently and covertly to acquire an unseen and undetectable strategic edge among a target population. Some experts have viewed NKW as a smoothly integrated mix of information, electromagnetic, and cyber warfare inside a digital environment to generate unique battlefield capabilities. (Henselmann, 2022)

The challenge to advocates of deterrence theory is that NKW is not easily thwarted until it has done its intended damage. Nonkinetic systems operate within frontiers of conflict beyond normal imagination. This reflects the so-called *phigital* world where digital and human characteristics patterns and essential ingredients overlap in indiscernible ways. The deceptive curtain of A/R or V/R intrudes on our layered perception impeding our ability to discern fact from illusion.

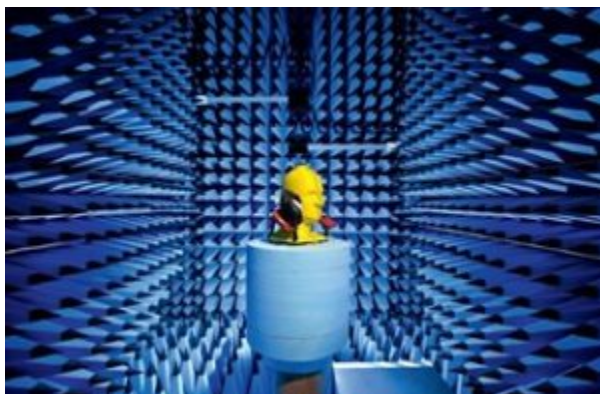
Science has recently demonstrated almost no barriers linking



common human functional biology to artificially created neurons. Brain implants, advanced prosthetics, and a wide range of medical implants and wearable devices rely on links between the body's autonomic nervous system and electronic circuits. Swedish researchers have found a better alternative to creating artificial neurons and [synapses](#)—the basic linking structures that connect two neurons—out of organic semiconductors that are biocompatible, biodegradable, soft, and can carry both electronic and ionic signals. The main pieces of natural biology can be merged and coupled with engineered materials to create operational and functional links. Scientists showed that the synapses were capable of [Hebbian learning](#), which is how the strength of the connection between any two neurons increases or decreases based on activity. This means neurons are activated and connected with other neurons, forming a neural network that at first starts weak but grows stronger and stronger with each stimulus. The new hybrid cell becomes more intuitive with the strengths of connections between neurons controlling the function of different brain circuits. We have far beyond the idea of a brain-computer interface which brings us closer to a genuine cyborg option in defense matters. (Gent, 2022)

A world where RF radiation and electromagnetics are merged via engineering creates a unique defensive challenge. Here the value of 'anechoic' chambers, which means 'without echo,' creates chambers are spaces designed to have minimal wave reflection from the walls, ceiling, and floor. Understanding Anechoic Chambers for Electromagnetic and RF Testing (Arar, 2022). Electronics engineers use anechoic chambers for [electromagnetic compatibility \(EMC\)](#) or [electromagnetic interference \(EMI\)](#) and RF testing. The interior walls of these chambers are treated with special material to absorb electromagnetic waves and thwart emanations that absorb sound waves rather than electromagnetic energy. See Figure 4.4.

**Figure 4.4 a&b Two different anechoic chambers—one large and one small.**



**Source: (Schwarz) (Okula)**

EMF radiation refers to low-frequency magnetic fields emitted by powerlines, household appliances, and power outlets. RF radiation refers to high-frequency electromagnetic radiation emitted by wireless equipment like cell towers, cellphones, GPS, televisions, and radios. Wireless networks inside our homes and workspaces have also become a major source of RF radiation. Although both EMF radiation and RF radiation have many similarities, they also have

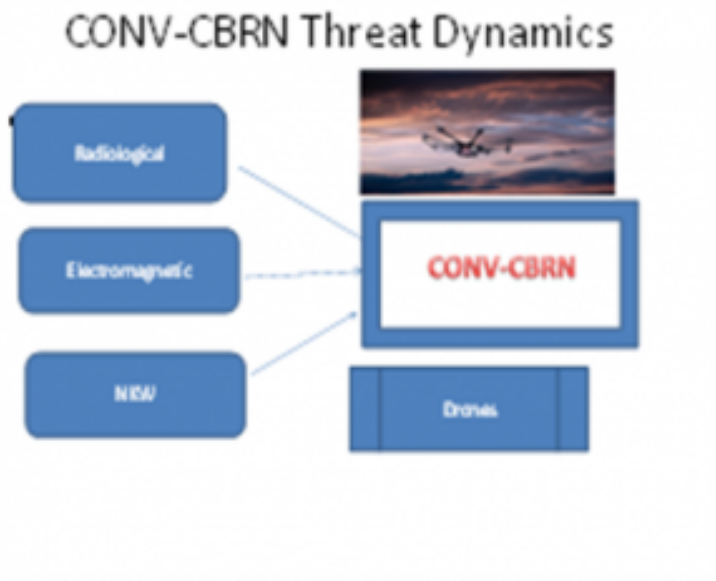
several key differences that affect how these electromagnetic energy forces interact with our bodies. (NIEH, 2022) Other things that emit EMF radiation may include Cellphones, Laptops, TV, Computers, Microwave Ovens Wi-Fi Devices; you can see there may be several common household and workplace items exposing you to EMF radiation. Consistent exposure to EMF radiation can have significant health consequences. Tests have shown that the closer you are to an object emitting EMF radiation, the higher the amount of EMF radiation you will be exposed to.

Chaos theory may be helpful as it tackles apparent randomness involving complex systems with underlying patterns, interconnectedness, constant feedback loops, repetition, and self-organization. According to Chaos Theory, changes arising inside tiny things or events can change the world. Examples include the stock market, weather, human psychology, and natural disaster cycles. Chaos Theory does not provide a comprehensive answer to dealing with a complex threat environment where CONV-CBRN, electromagnetic, NKW, drones, and radiological factors intermingle. (Straussfogel, 2009 )]

The scope and scale of ever-widening avenues for mixed applications of diverse technologies after 2022 creating hybrid systems and semi-human pathways to magnify what ordinary persons can perform or demonstrate and utilize it in both helpful and harmful ways, are eye-opening. Having said all of these views are legitimate and persuasive to a degree, we remain stuck with the realities of CONV-CBRN today, where drones, electromagnetic, radiological, and non-kinetics appear to dominate the threats we face after 2022. We find ourselves inside a complex, multi-dimensional, inherently multifaceted dilemma, requiring a broad and sweeping appreciation for unlimited technology convergence's immediate and long-term implications. The evolution of CONV-CBRN as it morphs after 2022 is unlikely to be static or unchanging. A crazy combination of CONV-CBRN, electromagnetic, NKW, and radiological phenomena is possible. The unknown effects of routine and unrestricted technology convergence are not well

understood, and thematic steps invoked to govern and regulate what happens in that space will defy easy solutions. Arguably, it begins with a realistic vision of the full spectrum, themes, and issues when we try to define that threat. If seen in combination with cascading influence and affect, the picture acquires greater complexity; to assume we have enough data and information is incorrect.

**Figure 4.5 CONV-CBRN Threat Dynamics**



Source: (McCreight R., 2013)

Is it the special mix of lethal and non-kinetic technologies which draw their collective and convergent power from each other based on cutting-edge dual-use science? Or instead, can we posit the argument that they constitute a threat only when combined and

engineered in unison, unlike any we have seen before? Grasping threat issues post-2022 requires a sharper, more focused, and comprehensive lens to know what this set of geostrategic challenges signifies.

### **SPECIAL DELIVERY OF DEATH AND DESTRUCTION: —ADDING DRONE RISK FACTORS POST 2021**

On the one hand, drones appear to have some benign characteristics delivering pizzas, packages for Amazon, snapping powerful aerial nature photos, emergency rescue, standoff environmental monitoring, precision agriculture, and much-needed medications to isolated areas. However, their insidious dual-use nature allows them to be used as special delivery vehicles for death and destruction as their inherent value in wartime appears both appealing and overwhelming. The prospect of using drones in strictly beneficial and socially pleasing ways runs counter to their diligent, appealing, and expansive use as expedient instruments of warfare.

Experts warn of drone swarms numbering in hundreds, all designed to deliver a damaging payload powered by remote signals and near autonomy in their designated target options. As such, recognizing them, defending against them, and neutralizing their combined effect becomes the artful and scientific blend of anti-drone warfare and related technology. This is being emphasized simply because all we have summarized and described thus far—CONV-CBRN, NKW, electromagnetic, and conventional weaponry can be mounted on drones to maximize their harmful and lethal capabilities. The list of conceivable drone-based threats is virtually unlimited in scope. Several persuasive examples come to mind here as just a few battlefield scenarios are cited

- Turkish drones supplied to Ukraine to fend off Russian attacks during the 2022 war indicate their utility and lethality (Malsi, 2022)

- Some experts claim that drone use leads to unlimited and unexpected scenarios where repetitive international drone warfare

continues relentlessly simply based on their ubiquity and ease of operation. (Martin, 2016)

-Avenger # UAS was recently integrated with a virtual swarm of other UAS, which in unison searched and tracked an artificially generated adversary through the use of AI/ML algorithms, deciding which aircraft would autonomously 'break' from the pack and perform closed-loop, air-to-air tactics displaying autonomy by using a blend of simulated threats, real-world sensors, and live aircraft where robust autonomy was combined with machine learning to validate unmanned aircraft illustrating complex kill chains. (Grinter, 2021)

-Unintentional or deliberate GPS interference and jamming, along with the capability to detect and geolocate origins and sources of GPS interference, enables technologically equipped forces to detect and nullify frequent disruptions to friendly UAVs and thereby thwart the 'global commons' that all modern economies depend upon. Launching GPS signal interference can disrupt air travel, logistics, finance, transportation, communication, and many other aspects of ordinary life, preventing people, vehicles, ships, and planes from determining their accurate position or confirming their targeted locations. Such jamming can cripple the government and commercial operations over thousands of square miles. (hawkeye-360, 2022)

- Use of multiplatform counter-UAS system (CUS), relying on a team of mini-drones acting as a cooperative defensive system for sensing, mitigation, and C2 control systems that generally comprise a counter-drone network. (Castrillo, 2022)

-AFRL is building a system to zap small unmanned aerial systems with high-powered microwaves and disable them called THOR for Tactical High Power Operational Responder. (Losey, 2022)

-Unmanned drones monitoring the skies watching from multiple perspectives, using multiple sensors can loiter using its infrared search-and-track sensor to spot any hostile aircraft as they climb out from the clouds. AI-enabled autonomous systems onboard the drones can verify the location of the hostile jet's launch, its speed,

and other features to confirm its 'friend or foe' status. Data relayed in real-time to human commanders seeking combat response decisions allow the human-occupied aircraft can stay in touch. Hence, every human pilot in the area gets an alert immediately after the friendly UAVs identify the suspect plane and conclude whether attack conditions are right. (SYSTEMS, 2022)

As platforms for delivering lethality and related strike packages, drones are an option with real tactical leverage in combat. They are not invincible, but the variety of their military application is beyond the limit. The issue of armed drones and combat-equipped UAVs has become the principal instrument of tactical battlefield leverage since 2015, with extensive use of drones in the theaters of war in the Mid-East and Afghanistan. The real question is, how do drones maximize combat lethality in specific ways after 2022?

#### **CONV-CBRN DRONE AUGMENTED THREAT AND RISK POSSIBLE SCENARIOS**

Certain drone-enabled scenarios can be considered mechanisms for executing a combined CONV-CBRN attack where mixes of electromagnetic, radiological, and NKW elements can be added. These notional scenarios seem plausible and surface the overall implications for defensive strategies to offset their initial advantages. See Figure 4.6.

- drone bore laser attack on spent fuel ponds involving targeted explosives at a nuclear plant

- drone - borne laser or precision explosive attack on spent fuel truck convoys

- drone- borne laser or augmented kinetic attacks on nuclear waste storage sites

- drone -borne precision explosive attacks at University research nuclear labs

- drone- bore NKW Electromagnetic attack on nuclear plant safety operators

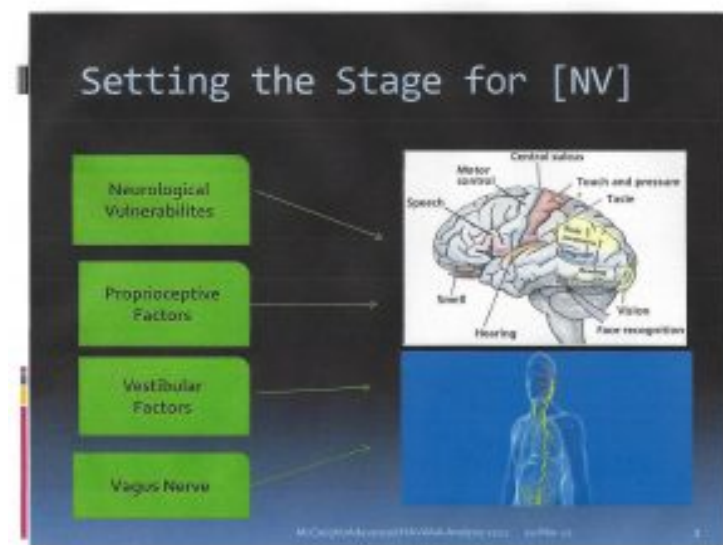
-drone-borne NKW attacks on spent fuel convoy drivers and security personnel

— drone-borne targeted CW attack on nuclear-reprocessing facilities and security staff. (McCreight M. S., 2020)

In addition, one more terrifying thought: Swarming drones equipped with EW enhanced platforms to beam sustained hostile RF pulsed waves can prepare the battlefield in a comprehensive nonkinetic operation, adversely affecting civilians and military personnel for which limited defense options exist.

The task of doctrinal writers and strategic military planners is to estimate what this scenario entails and requires as we confront a future battlefield where the mind is a preferred target over anything else. (McCreight R., Another future scenario, 2022)

**Figure 4.6 Setting the Stage for NV**



Source: (McCreight R., 2013) (McCreight M. S., 2020)



## **CONV-CBRN-ONWARD SECURITY AND RISK CHALLENGES POST-2021**

Mixing CONV-CBRN, electromagnetics, drones, NKW, and the metaverse would create an imaginary fabrication of threats confronting us after 2022 to the extent that many experts would view this risk as highly regarded improbable or evidence of science fiction. This would be a strategic blunder of the first order. Failing to recognize or characterize these threats—even in speculative wargames where risk scenarios are deeply explored—is a must. A world where these mixed technologies proliferate is central to future conflict and bedrock for strategic imagination. The issues and technologies covered in this chapter are meant to foster greater awareness of the Dual-Use Science and Technology threat [**DUST**], which is relentless as advances in science and technology hold no rational filter against nefarious and destructive purposes. As national and sovereign designs on greater military power where no apparent defenses or strategic warning systems exist, one can expect this space to become increasingly crowded. It is important to probe and define the entire threat spectrum where these issues and challenges remain a strategic challenge for the next decade. Experts dedicated to discerning the scope and scale of tomorrow's expected and unexpected areas of disruption, chaos, crisis, and calamity owe it to themselves to rigorously examine the warnings included here. (McCreight T.-F.-C. T., 2020)

### **DISCUSSION QUESTIONS**

1-What is the strategic significance that can be assigned to CONV-CBRN?

2-How do electromagnetic and radiological issues affect our understanding of strategic threats?

3-Why should we be concerned about NKW and the technologies it represents?

4-What aspects of radiological threats combined with electromagnetic warrant further research?

5- Does it make sense to include considerations of the metaverse

when assessing how a mix of advanced technologies such as CONV-CBRN, radiological, electromagnetics, and NKW can be seen independently as threats by themselves?

6-What threat and risk scenarios involving drones and the technologies discussed in this chapter pose unique strategic threats?

### **Bibliography**

(Seoul), B. T. (2018, November 27). RF-EMF Exposure. Retrieved from Published online 2018 Nov 27. doi: 10.4062/biomolther.2018.152: doi: 10.4062/biomolther.2018.152

AARL. (2022, March 18). RF Radiation and Electromagnetic Field Safety. Retrieved from <https://www.arrl.org/>: <https://www.arrl.org/rf-radiation-and-electromagnetic-field-safety/>

Arar, S. (2022, Feb 9). All About Circuits Understanding. Retrieved from [www.allaboutcircuits.com/technical](http://www.allaboutcircuits.com/technical): [HTTps://www.allaboutcircuits.com/technical](https://www.allaboutcircuits.com/technical)

Ball, M. (2020, January 13). The Metaverse: What It Is, Where to Find It, and Who Will Govern it. Retrieved from <https://www.matthewball.vc/all/themetaverse/>: <https://www.matthewball.vc/all/themetaverse/> Jan 13, 2020

Bunn, M. (2021). The evolving global threat to nuclear and radiological. Retrieved from <https://scholar.harvard.edu>: [https://scholar.harvard.edu/files/matthew\\_bunn/files/transport-threat-brief-2021.pdf](https://scholar.harvard.edu/files/matthew_bunn/files/transport-threat-brief-2021.pdf)

Castrillo, V. (2022, Feb). A Review of Counter UAS Technologies for Cooperative Defense Teams of Drones. *Italian Aerospace Research Center. Drones*, p. 6.

CDC. (2022, March 18). CDC, Radiological Threat Agents, 2015. Retrieved from CDC: <https://www.cdc.gov/>

DHS. (2022, March 18). countering-weapons-mass-destruction. Retrieved from [www.dhs.gov/](http://www.dhs.gov/): <https://www.dhs.gov/countering-weapons-mass-destruction-office>

DHS. (2022, March 18). *Radiological Attack Fact Sheet*. Retrieved from <https://www.dhs.gov/publication/>: <https://www.dhs.gov/publication/radiological-attack-fact-sheet>]

EarthSky – Earth, S. H. (2019). *EarthSky – Earth, Space, Human World, Tonight*. Retrieved from [earthsky.org//2019](https://earthsky.org//2019): <https://earthsky.org//2019>

EPA, [. (2012). *Radiation Facts, Risks, and Realities—US Government*. Washington: [US EPA – US Government].

FAS, M. /. (1998). *Nuclear Weapons Effects Technology Militarily Critical Technologies List (MCTL)*. Retrieved from [irp.fas.org/threat](http://irp.fas.org/threat): <https://irp.fas.org/threat/mctl98-2/>

FCC. (2022, March 18). *The effects of radiofrequency electromagnetic radiation on Human Health*. Retrieved from <https://ecfsapi.fcc.gov/>: <https://ecfsapi.fcc.gov/file/1093016723166/RF>

Gent, E. (2022, February 25). *Scientists Create Artificial Neurons that Power a Venus Fly Trap*. Retrieved from [techbely.com](http://techbely.com): <http://techbely.com/scientists-created-synthetic-neurons-that-can-make-a-venus-flytrap-snap/>

globalsecurity.org. (2022, March 18). *Weapons of Mass Destruction (WMD)*. Retrieved from [www.globalsecurity.org](http://www.globalsecurity.org): <https://www.globalsecurity.org/wmd/intro/nuke.htm>

Grinter, P. (2021, Aug 25). *Avenger UAS Autonomously Tracks and Follows Target Aircraft*. *Unmanned Systems Technology*.

Haines, D. (2022). *Executive Summary, Feb 2, 2022, Analysis of Pending AHI Cases – Redacted*. Washington: DNI.

hawkeye-360. (2022, March 4). *hawkeye-360-signal-detection-reveals-GPS-interference-in-Ukraine*. Retrieved from [www.he360.com/](http://www.he360.com/): <https://www.he360.com/hawkeye-360-signal-detection-reveals-gps-interference-in-ukraine/>

Henselmann, M. L. (2022, March 18). *Non-Kinetic Warfare: The New Game Changer in the Battle Space*. Retrieved from University of Jyväskylä, Finland : DOI: 10.34190/ICCWS.20.033].

IAEA. (2018). *IAEA Safety Standards: Regulations for the Safe Transport of Radioactive Material*. Retrieved from [www-](http://www-)

pub.iaea.org/: [https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1798\\_web.pdf](https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1798_web.pdf)

Jaitner, M. (2014). Russian Information Warfare. *Conference Paper, Swedish Defense Research Agency*. Swedish Defense Research Agency.

Ju Hwan Kim, J.-K. L.-G. (2019, May 1). PMID: PMC6513191PMID: 30481957 Possible Effects of Radiofrequency Electromagnetic Field Exposure on Central Nerve System. Retrieved from <https://pubmed.ncbi.nlm.nih.gov/>: <https://pubmed.ncbi.nlm.nih.gov/30481957/>

Library, E. P. (2022, March 18). *Atoms for Peace*. Retrieved from [www.eisenhowerlibrary.gov/research/](http://www.eisenhowerlibrary.gov/research/): [www.eisenhowerlibrary.gov/research/online-documents/atoms-peace](http://www.eisenhowerlibrary.gov/research/online-documents/atoms-peace)]

Linda Douw, M. K. (2009). Cognitive and radiological effects of radiotherapy in patients with low-grade glioma. *Lancet Neurology*, Sept.

Losey, S. (2022, Feb 28). Killing drones with Thor's hammer: Air Force eyes counter-UAS Weapon. *Defense News*.

Malsi, B. F. (2022, February 27). Ukraine Says It Used Turkish-Made Drones to Hit Russian Targets. *WSJ*.

Martin, J. (2016). *Drone Nation-America's New Way of War*. Lexington Books.

McCreight, M. S. (2020, Sept). Quantum Conundrum: Multi-domain Threats, Convergent Technology & Hybrid Strategy, US Army Futures Command. *Mad Scientist #268*.

McCreight, R. (2013, October). Convergent Technology and Future Strategic Threat. *Strategic Studies Quarterly*, pp. 10-18.

McCreight, R. (2013, March ). Convergent Technology Threats. *Strategic Studies Quarterly*, USAF Air University.

McCreight, R. (2022, April 6). Another future scenario. *Private email to Managing Editor, R. K. Nichols*.

McCreight, R. (2021). NeuroStrike Weapons and the Strategic Domain after 2020: Caution. *Academia Letters*, 2021.

McCreight, T.-F.-C. T. (2020, February 24). Twenty-First-Century

Threats in a Complex World: Dealing with DUST in the Wind. *Wild Blue Yonder* / Maxwell.

NATO. (n.d.). NATO HANDBOOK ON THE MEDICAL ASPECTS OF NBC DEFENSIVE. Retrieved from <http://large.stanford.edu/courses/2019/ph241/abbate2/docs/fm8-9.pdf>: <http://large.stanford.edu/courses/2019/ph241/abbate2/docs/fm8-9.pdf>

Nelson, K. (2022, February 20). What Could be Causing Havana Syndrome Cases on US Soil? CBS News.

NERC. (2019, November 5). *nerc\_emp\_task\_force\_report.pdf*. Retrieved from [nerc.com/pa/](http://nerc.com/pa/): [https://nerc.com/pa/stand/emp%20task%20force%20posting%20dl/nerc\\_emp\\_task\\_force\\_report.pdf](https://nerc.com/pa/stand/emp%20task%20force%20posting%20dl/nerc_emp_task_force_report.pdf)

News, B. (2022, February 5). Nuclear Plant Under Attack by Artillery. BBC News.

NIEH. (2022, March 18). EMF Radiation? Retrieved from <https://www.niehs.nih.gov/>: <https://www.niehs.nih.gov/health/topics/agents/emf/index.cfm>

NRC. (2017). *NRC Backgrounder on Research and Test Reactors*. Retrieved from <https://www.nrc.gov/.../research-reactors-bg.html>: [www.nrc.gov/.../research-reactors-bg.html](http://www.nrc.gov/.../research-reactors-bg.html)

Okula, C. (n.d.). *Small anechoic chamber*. Edwards Air Force Base.

Reports, E. C. (2018, February 27). *EMP Report February 27, 2018*. Retrieved from [highfrontier.org](http://highfrontier.org): [highfrontier.org/february-27-2018-publish-emp-commission-reports](http://highfrontier.org/february-27-2018-publish-emp-commission-reports)].

Ryan, S. (2014, November 4). *USASOC-CognitiveJointForceEntry.pdf*. Retrieved from [info.publicintelligence.net/](http://info.publicintelligence.net/): <https://info.publicintelligence.net/USASOC-CognitiveJointForceEntry.pdf>

Scarpatti, J. (2021, Feb 25). What is a radio frequency (RF)? Retrieved from <https://techtarget.com>: <https://techtarget.com/searchnetworking/definition/radio-frequency> Feb 25, 2021

Schwarz, R. a. (n.d.). *Two different anechoic chambers—one large and one small*. Image used courtesy of Rohde and Schwarz.

sciencemediacentre.co.NZ. (2022, March 18). *Sources of Radiation*:

Where do mobile phones fit in? Retrieved from <https://www.sciencemediacentre.co.nz/infographics/>:  
<https://www.sciencemediacentre.co.nz/infographics/>

Sciences, N. A. (2020). *An Assessment of Illness in U.S. Government Employees and Their Families at Overseas Embassies*. Washington: National Academy of Sciences.

Scientists, B. o. (2009, May 19). *Iraq FFCD report – what-we-found-at-al-tuwaitha*. Retrieved from <https://thebulletin.org>:  
<https://thebulletin.org/2009/05/what-we-found-at-al-tuwaitha>

Scoles, S. (2022, March 11). *Radioactive Material Is Everywhere*. *Scientific American*.

SOCOM. (2015). *SOCOM Leaders attribute risks to cognitive warfare*. Ft Bragg NC: SOCOM Unclassified brief.

Straussfogel, C. v. (2009 ). *International Encyclopedia of Human Geography*. Amsterdam: Elsevier.

SYSTEMS, G. A. (2022, March 3). *How AI and supervised autonomy will change combat*. GENERAL ATOMICS AERONAUTICAL SYSTEMS.

Turnquist, C. (2020). *Radiation-induced brain injury: current concepts and therapeutic strategies targeting neuroinflammation*. *Neuro-Oncology Advances*, Volume 2, Issue 1, January-December.

Tzu, S. (475 – 221 B.C.E.). *The Art of War*. Retrieved from <http://classics.mit.edu>: <http://classics.mit.edu/Tzu/artwar.html>

# 5. Nuclear Weapons

**By Professor Candice M. Carter**

## **STUDENT OBJECTIVES**

- To further understand the role of unmanned systems in the nuclear realm
- To study Nation-State advances with unmanned nuclear systems
- To develop an understanding of the next generation of warfare

## **INTRODUCTION**

The future battlefield looks different from traditional warfare with the continued advances in unmanned technology. Nuclear unmanned systems are alternatives for intercontinental ballistic missiles (ICBMs) and manned bombers and submarines for nuclear weapon delivery. The advantages of unmanned nuclear weapons are the ability to be deployed to reach further targets at set periods and enable unique attacks that normally would be challenging. Additionally, unmanned weapons increase the precision of targeting an attack. However, the advanced artificial intelligence required within the design of unmanned weapons can make them potentially unpredictable. The technology is not at the stage where it would allow nuclear-armed states to credibly threaten the survivability of each other's nuclear second-strike capability. (Caves, 2021)

## **STATE ACTORS**

### **RUSSIA**

In 2019, the United States and Russia withdrew from the Intermediate-Range Nuclear Forces (INF) Treaty. After years of discussion, the United States' withdrawal was precipitated by Russia's refusal to acknowledge, much less rectify, its testing of

the 9M729 (SCC-8) ground-launched cruise missile over the ranges permitted by the treaty. (Caves Jr. & Cares, 2021) In May 2020, the United States announced it would withdraw from the Open Skies Treaty in response to a history of Russian violations unless Russia returned to compliance. (Caves Jr. & Cares, 2021) “Responsibility for the deterioration of the Open Skies regime lies fully with the United States as the country that started the destruction of the treaty,” the Russian Foreign Ministry stated in December 2020. (Zherdin, 2022) After the U.S. withdrawal, Moscow sought written guarantees from the remaining states-parties that they would neither continue to share data collected under the treaty with Washington nor prohibit overflights of U.S. bases in Europe, but states-parties dismissed the request. (Zherdin, 2022) The Open Skies Treaty was an agreement among 34 countries regarding what type of technology could fly over their countries. The treaty required specific certifications of equipment.

The United States and Russia have agreed to The New START Treaty (Strategic Arms Reduction Treaty), activated in January 2022. Replacing The SMART Treaty, originally signed in 2010 and expired on February 5, 2021. The 2010 Start Treaty was an agreement between the two countries for nuclear arms reduction and established a limit of deployed strategic warheads. As part of the New START Treaty (which is enforced until 2026), intercontinental and submarine ballistic missile launchers and heavy

#### **Table 5.1 Limits on START, Moscow Treaty, and New Start**



| Treaty                      | START (1991)  | Moscow Treaty (1982)                                    | New START (2010)  |
|-----------------------------|---|---|---|
| Limits on Delivery Vehicles | 1,600 strategic nuclear delivery vehicles   | No limits   | 800 deployed and nondeployed ICBM launchers, SLBM launchers and heavy bombers equipped to carry nuclear weapons<br><br>Within the 800 limit, 700 deployed ICBMs, SLBMs, and heavy bombers equipped to carry nuclear weapons |
| Limits on Warheads          | 6,000 warheads attributed to ICBMs, SLBMs, and heavy bombers<br>4,900 warheads attributed to ICBMs and SLBMs<br>1,100 warheads attributed to mobile ICBMs<br>1,540 warheads attributed to heavy ICBMs | 1,700-3,200 deployed strategic warheads<br>No sublimits | 1,550 deployed warheads<br>No sublimits   |
| Limits on Throwweight       | 3,600 metric tons   | No limit  | No limit  |

Source: (Congressional Research Service, 2022)

bombers are counted under the limits until they are converted or eliminated according to the provisions described in the treaty's Protocol. (Congressional Research Service, 2022) This differs from the original Treaty by giving both countries greater flexibility to comply by allowing the countries to decide how to reduce forces.

Does The New START Treaty give China an advantage over the United States and Russia? Hong Kong-based military affairs commentator and former PLA instructor Song Zhongping said Beijing might use the five years to narrow the nuclear modernization gap with the US and Russia. (Chan, 2021)

### Soviet Union

The 1960s had the growth of nuclear weapons in the United States and Russia, leading to several discussions between the countries regarding taking nuclear action against one another. With the signing of the 1972 Anti-Ballistic Missile (ABM) Treaty, both sides accepted limits to protect themselves from a retaliatory nuclear

attack, thus reducing the attractiveness of being the first to strike. (Woolf, 2022) By the end of 1980, the Soviet Union declared they would not be the first to strike in a nuclear conflict. After the accident at the Chornobyl Nuclear Power Plant, Mikhail Gorbachev believed that the use of nuclear weapons would be catastrophic. (Woolf, 2022) The Soviet Union and the United States made great strides to turn away from nuclear weapons and focus on peace and diplomacy.

### **Russian Federation**

After the fall of the Soviet Union, the Russian Federation was formed in its place. The Russian Federation took Russia from a political state to a country. The liberal thinking and embracing of western ideology changed in 1999 when President Vladimir Putin was sworn to what would eventually become Russia's longest-serving leader and is in his fourth term as president. Over his leadership, Russia has slowly fallen back into a reflection of the past Soviet Union. Putin felt the Russian Federation was weak in the eyes of the world. One of the items that contributed to changing the of being just another country was in 1997. The Russian Federation eliminated the no-first-use pledge of nuclear weapons. It replaced it with the ability of the Russian Federation to use nuclear weapons for protection against attacks from other attacks countries. Eventually, the policy evolved into the Russian Military Doctrine of 2010, allowing for a preemptive nuclear strike. (Woolf, 2022) The 2010 doctrine stated that the main external military dangers to Russia were "the desire to endow the force potential of the North Atlantic Treaty Organization (NATO) with global functions carried out in violation of the norms of international law and to move the military infrastructure of NATO member countries closer to the borders of the Russian Federation, including by expanding the bloc." (Woolf, 2022) Since that time, Russian President Vladimir Putin's public stance on nuclear weapons has wavered until 2018. Over the past few years, the development of the Russian nuclear program has accelerated.

## Посейдон and Белгород

In March 2018, Russian President Vladimir Putin unveiled to the Russian Federal Assembly the modernized nuclear-armed system, highlighting the development of two new nuclear delivery systems, which, he said, could evade US anti-ballistic missile defenses. (Rosenberg, 2018) This included cruise missiles, intercontinental ballistic missiles, underwater drones, and supersonic jets. Putin strives for Russia to be a world superpower and reclaim former countries part of the Soviet Union.

**Figure 5.1 Russian President Vladimir Putin Addresses the Russian Federal Assembly**

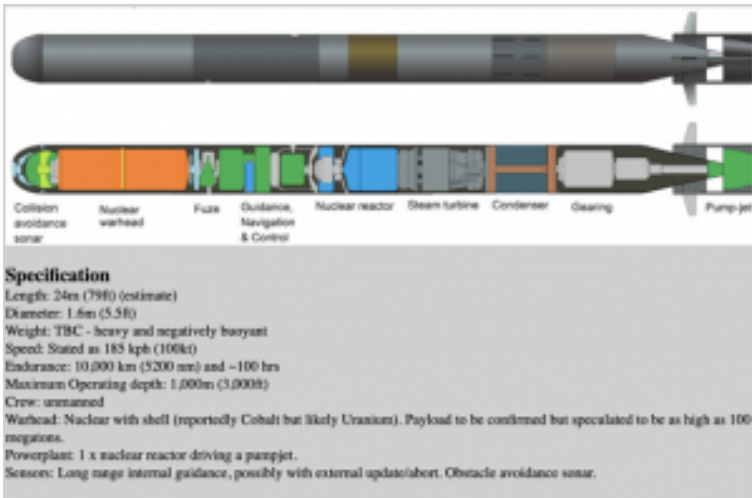


Source: (Rosenberg, 2018)

**Status – 6 (Статус-6)** is an autonomous, nuclear-armed, and powered unmanned underwater vehicle. Known now as **Poseidon (Посейдон)** is one of the six strategic weapons announced in The Project 09851 Khabarovsk special-purpose nuclear submarine, capable of carrying up to six Poseidon strategic drones, which will be launched in the first half of 2021. (Pike, 2021) Poseidon is an 'Intercontinental Nuclear-Powered Nuclear-Armed Autonomous

Torpedo.’ (Sutton H. I., 2022) The Poseidon 2M39 torpedo is still under development; however, it will be an unstoppable nuclear weapon when complete. The modern nuclear weapon is believed to be between 65 to 79 feet long, approximately 6.5 feet in diameter, with a dirty bomb warhead. The mega weapon will have a two-megaton nuclear or conventional payload that could be detonated “thousands of feet ” below the surface. (Woolf, 2022) With the ability to travel underwater past anti-defense systems with ease, Poseidon will cause a radioactive Tsunami that will last for years into the future. Professor Frank von Hippel, a senior research physicist at Princeton University, believes this next generation of Nuclear weapons will show the United States there is no way to escape our mutual nuclear hostage relationship. (Bergan, Papadopoulos, Erdemir, & Ozdemir, 2021) Poseidon is the largest torpedo ever developed in any country. (Sutton H., Covert Shores, 2016) It is twice the size of submarine-launched ballistic missiles (SLBMs) and thirty times the size of a regular ‘heavyweight’ torpedo. (Sutton H., Covert Shores, 2016) The original release date of the deadly torpedo was 2022. However, indicators point to the activation date targeting 2027. There is no other country that can match the creation of this nuclear weapon at this time.

**Figure 5.2 Russian Poseidon 2M39 Torpedo**



Source: (Sutton H. I., 2022)

When Russian President Vladimir Putin spoke to the Russian Federal Assembly in 2018, it was clear the next generation of Russian nuclear systems would be designed with the ability to bypass any United States missile defense system. Russia has construction underway to build a new military base to hold 30 Poseidon torpedoes and four unmanned nuclear submarines. Per President Putin, the unmanned submarines, **Belgorod (Белгород)**, are intercontinental, the fastest, largest, and noiseless in the world. According to President Putin, unmanned vessels can reach ultra-deep levels and cannot be detected by any current defense system.

**Figure 5.3A Belgorod – Russian Unmanned Nuclear Submarine**



**Figure 5.3B Belgorod – Russian Unmanned Nuclear Submarine**

|   |
|---|
| <b>Pr09852 Belgorod Specifications</b> (Provisional)  |
| Displacement: greater than 14,700 tonnes surfaced (est. 17,000 tonnes), 24,000 tonnes submerged (estimated 30,000 tonnes)   |
| Length: ~178 meters   |
| Beam: ~15 meters  |
| Speed: < 32 knots   |
| Range: Unlimited  |
| Endurance: Approximately 4 months   |
| Operating depth: Estimated as 500-520 meters per OSCAR-II SSGN  |
| Propulsion: nuclear (2 x pressurized water reactor OK-650M.02 with a capacity of 190 MW driving two steam turbines and twin screws. Plus at least two outboard thrusters, |
| Crew: TBC, estimated 110  |
| Armament: 6 x Poseidon (KANYON) nuclear torpedoes , 6 x 533 mm (21") torpedo tubes (tbc)  |

Source: (Sutton H. I., 2022)

**Figure 5.4 Belgorod – Russian Unmanned Nuclear Submarine**



Source: (Sutton H., Covert Shores, 2021)

**Nuclear Alert Status**

February 27, 2022, Russia’s President Vladimir Putin told his Defense Minister and Chief of General Staff to activate nuclear forces into combat readiness. There is speculation about how this action impacted forces; was it an internal change or an external

one? The Pentagon did not see any changes to Russia's nuclear landscape. Most signals indicate the announcement of the change of status was retaliation for sanctions against Russia for the invasion of Ukraine.

January 2021, Russia accepted delivery of the first of 10 brand-new Tu-160M strategic bombers with updated NV-70M radar and NK-32-02 engines, U.S. Admiral Charles Richard testimony to the U.S. House Defense Appropriations subcommittee April 2022. (Tiron & Musk, 2022)

## **CHINA**

Think of the Chinese use of swarming drones on the seas, in the air, floating nuclear power plants, underwater mining, robot freighters, and anti-submarine UUVs. In the author's view, they are leapfrogging US technology and antiquating defenses. (Nichols R. K., 2020) It is believed over the next six years, China will increase its nuclear warheads by at least 700. (Moore, 2021), (2021) The current inventory is closer to the numbers of warheads of the United Kingdom and France. Beijing's nuclear stockpile, which could top 1,000 deliverable warheads by 2030, is designed to match and even surpass the US' global military. (Moore, 2021) This contributes to China's goal of being a global superpower by breaking other countries' alliances with the U.S. and gaining partnerships in the Indo-Pacific Region by 2049. (Moore, 2021), Russia and China declared a new era of partnership against the United States and other members of NATO. Also, both countries have decided to collaborate on the Internet, space, and climate change. They each support the other in the desire to grab land, China for Taiwan, and Russia for Ukraine. Will this new partnership expand to the development of nuclear weapons?

China is closely following the developments of the U.S. Navy's plans to develop unmanned systems, especially in the underseas. These UUVs are used in various data collection roles in coordination

with satellites and other surveillance systems. Evidence points to China exploring nuclear-powered underwater drones and cruise missiles. (Standeford, 2021) China is substantially upsetting the offense-defense balance in underwater warfare. (Carnegie Endowment for International Peace, 2018) China's growth in the unmanned area includes the ability to detect stealth submarines without exploding their mother surface ships into the danger of sailing within range of Chinese anti-ship missiles. (Carnegie Endowment for International Peace, 2018) The Chinese strongly believe the U.S. uses unmanned systems to collect intelligence on their Strategic Nuclear-Powered Ballistic Missile submarines (SSBN). The Chinese have warned of mistaking these UUVs in the manner of engagement that could escalate to conflict. In 2014, the Pacific countries adopted the Code for Unplanned Encounters at Sea (CUES). With an additional agreement with the U.S., CUES outlines safety rules for air and maritime encounters to prevent potential conflict. However, in 2016 there was an incident in the South China Sea, and China finds this to be a gray area; if the U.S. dares to send underwater drones, China believes they have the right to seize them. (Carnegie Endowment for International Peace, 2018) China's focus on maritime weapons reinforces its desire to rule Taiwan. Taiwan does not have guaranteed protection from the United States if China should evade it. However, the U.S. has trained soldiers and sold advanced weapons to Taiwan. The policy between the U.S. and Taiwan is vague. One cannot help to think China is watching the U.S. reaction to Russia invading Ukraine very closely to see what they could be up against.

### **Figure 5.5 China Nuclear Expansion**





Source: (Tiron & Musk, 2022)

UUVs are ideal for Nuclear powered weapons and bring unlimited possibilities of a range of targets. At the Conference on Disarmament, the United States conference ambassador, Robert Wood, stated that China has been building 110 new missile silos in the country's northern desert region. (Standeford, 2021) China is one of the leaders in drone swarm capabilities; this is an area of concern for China entering the unmanned nuclear space. In the action of a drone swarm, dozens of small, unmanned aircraft systems fly together, filling the sky. Some are collecting information. Some are identifying ground targets. Others might attack the same targets. (EurAsian Times Global Desk, 2020) A drone swarm can contain upwards of 10,000 drones, making defeating a swarm attack not feasible for humans. China has demonstrated its dominance in this space on numerous occasions, forcing other militaries to create anti-swarm defense systems while perfecting the use of a swarm attack.

**Figure 5.6 China Drone Lineup Sharp Sword stealth drone and the Wing Loong Reaper**



Source: (EurAsian Times Global Desk, 2020)

During the summer of 2021, China tested two nuclear-capable hypersonic missiles in August that circled the globe before speeding toward their target. (Sevastopulo, 2021). [1]The nuclear weapon test demonstrated to the U.S. and the world that China had accelerated its development of nuclear weapons that could go undetected by U.S. anti-ballistic missile defense systems.

China's nuclear weapon development proceeds to be a driving force for the country to become a competitive global superpower.

## **OTHER COUNTRIES**

The cooperation among NATO and non-EU allies is important in the next generation of warfare. Given the indications by global leading Nation-states that the nuclear arms race has been reignited, there is no doubt that other countries are anxious not to be left behind. Other countries, such as Israel, North Korea, Turkey, etc., plan to develop drones with radioactive impacts. However, North Korea, Israel, Pakistan, and India have nuclear weapons arsenals. France has nuclear weapons, launching submarines and aircraft.

The United Kingdom only can launch nuclear weapons via submarine. Overall, the countries of NATO will combine their military powers to defeat the threat from others outside of their alliance. Given the rapid developments from Russia and China with nuclear warheads, the partnerships in developing the nuclear weapons and defenses systems are critical to NATO.

An item to watch: In the current conflict in Ukraine, drone hobbyists are instructed how to modify off-the-shelf drones for military action in a similar fashion to non-state actors. This development should be closely studied for future conflict as next-generation warfare.

## **CONCLUSIONS**

Weapons may be understood as devices that deposit energy on targets. The energy that must be deposited to achieve a given level of damage is relatively insensitive to the type of weapon employed. Nuclear weapons may be characterized by megatons, bullets in terms of muzzle velocity, and particle beams in terms of amperes of current. (Nichols, Mumm, Carter, & Hood, 2020) The next generation of the nuclear arms race reinforces the need to develop international agreements and treaties for unmanned systems (including drone swarm advances) to prevent the threat of nuclear conflict. While aerial drones have limitations with the number of payload constraints, especially commercial, unmanned technology will continue to expand in the sea and space. Unmanned systems can hit targets with precision, especially in areas where normal weapons would have to overcome several technological and environmental challenges.

## **BIBLIOGRAPHY**

Bergan, B., Papadopoulos, L., Erdemir, M., & Ozdemir, D. (2021, July 7). *The Weapon That Eradicates Cities by Creating 'Radioactive Tsunamis'*. Retrieved April 4, 2022, from Interesting Engineering:

<https://interestingengineering.com/poseidon-nuclear-weapon-radioactive-tsunamis-russia>

Carnegie Endowment for International Peace. (2018, October 24). *The Impact of Future Unmanned Systems – Tides of Change: China's Nuclear Ballistic Missile Submarines and Strategic Stability*. Retrieved April 8, 2022, from Carnegie Endowment for International Peace: <https://carnegieendowment.org/2018/10/24/impact-of-future-unmanned-systems-pub-77497>.

Caves Jr., J. P., & Cares, W. S. (2021, February). *The Future of Weapons of Mass Destruction*. National Intelligence Press. Retrieved April 2022 from National Intelligence University: [https://ni-u.edu/wp/wp-content/uploads/2021/02/Future\\_of\\_WMD\\_Final.pdf](https://ni-u.edu/wp/wp-content/uploads/2021/02/Future_of_WMD_Final.pdf).

Caves, J. P. (2021, February). *THE FUTURE OF WEAPONS OF MASS DESTRUCTION*. Retrieved April 8, 2022, from National Intelligence University: [https://ni-u.edu/wp/wp-content/uploads/2021/02/Future\\_of\\_WMD\\_Final.pdf](https://ni-u.edu/wp/wp-content/uploads/2021/02/Future_of_WMD_Final.pdf).

Chan, M. (2021, January 31). *China may seek to close the nuclear gap as US and Russia extend the treaty*. Retrieved April 3, 2022, from South China Morning Post: <https://www.scmp.com/news/china/military/article/3119913/china-may-seek-close-nuclear-gap-after-us-and-russia-agree>.

Congressional Research Service. (2022, February 2). *The New START Treaty: Central Limits and Key Provisions*. Retrieved April 3, 2022, from FAS Project on Government Secrecy: <https://sgp.fas.org/crs/nuke/R41219.pdf>.

EurAsian Times Global Desk. (2020, August 28). *US, China Developing “Super Swarm” Drones With Destruction Power Equivalent To Nuclear Weapons*. Retrieved April 5, 2022, from EurAsian Times: <https://eurasianimes.com/us-china-developing-super-swarm-drones-with-destruction-power-equivalent-to-nuclear-weapons/>.

James Martin Center for Nonproliferation Studies at Monterey's Middlebury Institute of International Studies. (2022, January 1). *New START Treaty*. Retrieved April 3, 2022, from The Nuclear Threat

Initiative: <https://www.nti.org/education-center/treaties-and-regimes/treaty-between-the-united-states-of-america-and-the-russian-federation-on-measures-for-the-further-reduction-and-limitation-of-strategic-offensive-arms/>.

Janes. (2021). JAMES ALL THE WORLD'S AIRCRAFT: *In-Service*. JANE'S INFORMATION GROUP.

Moore, M. (2021, November 3). *China is expanding its nuclear weapons force faster than predicted*. Retrieved April 8, 2022, from New York Post: <https://nypost.com/2021/11/03/china-expanding-nuclear-weapons-force-faster-than-predicted/>.

Nichols, R. K. (2020). *Chapter 14 Maritime Cybersecurity* [Nichols] – UNMANNED VEHICLE SYSTEMS & OPERATIONS ON AIR, SEA, LAND. Retrieved April 8, 2022, from New Prairie Press Open Book Publishing: <https://kstatelibraries.pressbooks.pub/nicholsproject/chapter/chapter-14-maritime-cybersecurity-nichols/>.

Nichols, R., Mumm, H., Carter, C., & Hood, J. (2020, February 1). *Counter Unmanned Aircraft Systems Technologies and Operations – Simple Book Publishing*. Retrieved April 8, 2022, from New Prairie Press Open Book Publishing: <https://kstatelibraries.pressbooks.pub/counterunmannedaircraft/>.

Pike, J. (2021, August 25). *Status-6 / Kanyon – Ocean Multipurpose System – Russian and Soviet Nuclear Forces*. Retrieved April 3, 2022, from GlobalSecurity.org: <https://www.globalsecurity.org/wmd/world/russia/status-6.htm>.

Rosenberg, S. (2018, March 1). *Russia's Putin unveils 'invincible' nuclear weapons*. Retrieved April 3, 2022, from BBC: <https://www.bbc.com/news/world-europe-43239331>.

Sevastopulo, D. (2021, October 16). *China tests new space capability with a hypersonic missile*. Retrieved April 8, 2022, from Financial Times: <https://www.ft.com/content/ba0a3cde-719b-4040-93cb-a486e1f843fb>.

Standeford, D. (2021, July 12). *China To Obtain Nuclear Powered Underwater Drones And Cruise Missiles*. Retrieved April 5, 2022, from Defcon Level: <https://www.defconlevel.com/news/>

2021-07-12/china-to-obtain-nuclear-powered-underwater-drones-and-cruise-missiles.php.

Sutton, H. (2016, June 25). *Covert Shores*. Retrieved April 4, 2022, from H I Sutton: <http://www.hisutton.com/Spy%20Subs%20-Project%2009852%20Belgorod.html>.

Sutton, H. (2021, June 29). *Covert Shores*. Retrieved April 4, 2022, from H I Sutton: <http://www.hisutton.com/Belgorod-Class-Submarine.html>.

Sutton, H. I. (2022, March 3). *Russia's New 'Poseidon' Super-Weapon: What You Need To Know*. Retrieved April 4, 2022, from Naval News: <https://www.navalnews.com/naval-news/2022/03/russias-new-poseidon-super-weapon-what-you-need-to-know/>

Tiron, R., & Musk, E. (2022, April 4). *The US Sees Rising Risk in 'Breathtaking' China Nuclear Expansion*. Retrieved April 8, 2022, from Bloomberg Quint: <https://www.bloombergquint.com/politics/u-s-sees-rising-risk-in-breathtaking-china-nuclear-expansion>.

Woolf, A. F. (2022, March 21). *Russia's Nuclear Weapons: Doctrine, Forces, and Modernization*. Retrieved April 4, 2022, from FAS Project on Government Secrecy: <https://sgp.fas.org/crs/nuke/R45861.pdf>.

Zherdin, D. (2022, January). *Russia Officially Leaves Open Skies Treaty*. Retrieved April 8, 2022, from Arms Control Association: <https://www.armscontrol.org/act/2022-01/news-briefs/russia-officially-leaves-open-skies-treaty>.

[1] Further information regarding hypersonic missiles can be found in Chapter 12.

# 6. Explosives Delivered by Drone

**By Captain John-Paul Hood US Army**

## **Student Objectives**

The student will be introduced to the explosive payloads delivered by drones – especially in Ukraine – Russian conflict.

## **Introduction**

With the recent conflicts in Syria, Nagorno-Karabach, and Ukraine, unmanned aerial systems (drones) have become the topic of concern and debate for a good reason. These small and relatively inexpensive systems continue to grow in complexity, speed, and payload carrying capacity. Citizen hobbyists of war-torn regions continue to find ways to successfully militarize group 1 UAS seeking to carry out covert aerial surveillance and, more recently, precision strikes using manufactured small yield ordinance that is common use by militaries around the world. In many cases, hobbyist drone flyers turned militant combatants have resorted to improvised explosives delivered with devastating effects on point targets.

These new tactics and techniques have become alarming and pose a real threat to the U.S. homeland. As these conflicts continue, tactics and techniques are shared through social media, giving would-be internal dissidents options for conducting terrorism and sabotage within our borders. The following chapter contains a selection of recent use cases in which drones have been successfully employed against their intended targets, using everything from simple homemade explosives to dropping mortar round and Molotov cocktails to the drone being used to loiter, hunt targets on its own, and strike swiftly at will.

**Case study 6.1:** Mexican Cartel members use drones to target rivals and government officials.

At the outset of 2022, Mexican cartels have begun emplacing improvised explosive devices along roadsides to slow/deter law enforcement. The cartels eventually escalated their efforts by using drones to deliver explosives more precisely in targeted attempts against their rivals.

**Figure 6.1: A Picture Taken By A Drone From Above Its Intended Target.**



Source: (Emir, 2022)

The video, filmed with the drone's camera, shows the drone hovering over its target and then dropping its payload of small bombs with a parachute. The footage ends when the drone loses altitude rapidly, presumably after causing at least three separate explosions. The status of possible casualties and the extent of the damage is unknown. (Emir, 2022).

Local news channels have shared the video and claimed that



the [Cártel de Jalisco Nueva Generación](#) (CJNG), or Jalisco New Generation Cartel, is based in Jalisco, western Mexico, has attacked at least two towns, El Bejuco and La Romera, with drones.

CJNG, the most dangerous cartel in the country, is known for its brutality. The cartel members have been reportedly ripping out their victims' hearts, dissolving their bodies in barrels of acid, and even targeting pregnant women. They seek to dominate the illegal but extremely lucrative narcotics traffic in the area. The CJNG has become responsible for smuggling approximately 30 percent of all illegal drugs from Mexico into the United States since its inception in 2009. (Emir, 2022)

The CJNG can call upon a wide variety of weapons, vehicles, and equipment, including camo trucks, pickups, and SUVs, some of them armed with mounted weapons and equipped with add-on armor. The cartel members are also heavily armed and provided with military-style tactical gear. Though the cartel was once loyal to the Sinaloa cartel, CJNG sought to dominate other cartels in trafficking narcotics after the capture and U.S. jailing of Sinaloa's chief, Joaquín "El Chapo" Guzmán. (Emir, 2022)

### **Case Study 2: Ukraine Adapting Drones to Drop Improvised Explosives**

Soon after the outset of the Russian invasion of Ukraine on February 24, 2022, the drone-owning citizens of Ukraine set out to begin arming their personal drones for military use.

#### **Figure 6.2: Ukrainians Develop Drone That Drops Molotov Cocktails**



Source: (Kesslen, 2022)

Less than two weeks after Ukraine officials called on drone-owning citizens to volunteer their craft for use in defending the country from invading Russian forces, some of those non-military crafts have now been reportedly weaponized to drop Molotov cocktails on targets below. (Crumley, 2022)

The fruit of innovation, teamwork, a Soviet-era repair tradition known as “snotting things together,” in any way that works, the incendiary aerial delivery device was featured in photos in the New York Post, which failed to catch the clear markings on the UAV it says was developed by the Ukrainian Territorial Defense Forces. The Ukraine craft in the images is a DJI Inspire cinematic drone tricked out with a fastening to hold gas-filled beer bottles for dropping, one would suspect, on Russian army targets. (Crumley, 2022)

The repurposing of the drone involves the collaboration of Ukrainian Territorial Defense Forces – which has been training

volunteers to the resistance against how to make and use Molotov cocktails effectively in the battle against Russian invaders in Lviv's Pravda Brewery. However, anyone seeking to slake their thirst from the small, artsy, and decidedly patriotic maker of craft beers will have to wait while it serves the national cause. (Crumley, 2022)

"On February 24, our brewery stopped brewing beer and started making Molotov cocktails to win the war!" Pravda's "For Molotov!" product web page informs browsing customers, "You can make a donation by purchasing a cocktail." (Crumley, 2022)

Each bottle of flaming Molotov is 100 Ukraine Hryvnia (\$3.35), and for orders of \$25.12 or more, Pravda Brewery will deliver for free – now, quite possibly, by a drone above Russian forces. All by way of the adapted UAVs like the one shown in the Post's photos. (Crumley, 2022)

The front-loaded DJI Inspire's camera appears to be angled straight downward, possibly to offer a clear view of intended targets directly below. An L-shaped brace is affixed to the rear underside of the craft and features a downward, rimmed aperture into which the beer bottle's mouth is slid. (Crumley, 2022)

A thin plastic band is affixed around the container's center – possibly how it is held into place because a subsequent picture of a dropped bottle shows it falling nearly upright, indicating a rear release. Also feasible is the camera mounting has been adapted to secure the bottle's back end. (Crumley, 2022)

**Figure 6.3: Close-Up – Ukrainians Develop Drone That Drops Molotov Cocktails**



Source: (Kesslen, 2022)

Military instructors have been teaching civilians to use Molotov cocktails against the heavily armed Russian troops, and the instructions to build them reportedly have been aired on Ukrainian radio. (Kesslen, 2022)

**Figure 6.4: Molotov Cocktail Released**



Source: (Kesslen, 2022)

Whatever the case, the use of consumer or enterprise drones by Ukrainian forces for the attack, rather than just surveillance against Russian forces, would be another indication of escalation in the fighting – and may not be the last. (Crumley, 2022)

After all, modification of UAVs to drop gas bombs on enemies might logically lead to the release system being reworked to hold the grenades or small bombs that Mexican cartels, Middle East radical groups, and foes in the battles over pro-Moscow separatist regions in east Ukraine have deployed in the past year. (Crumley, 2022)

### **Case Study 3: Anti-Personnel Munitions**

#### **Figure 6.5: Heavy Modifications To Civil Drone Platforms**

**Enabled To Carry Very Low Cost Yet Powerful Munitions Such As Mortars 60-81mm Rounds.**



Source: (HaberDergilik/Kara-birliklernin-silahi-havan-dronla-havlandi, 2022)

The recent fighting in Ukraine has also seen the heavy modifications to civil drone platforms enabled to carry very low cost yet powerful munitions such as mortars 60-81mm rounds.

Ostim Technical University Faculty Member Prof. Dr. Sinan Kivrak and his students developed the Mortar Release System with their laboratory work. After the tests were carried out in the laboratory environment, field tests started with the system integrated into the drone. Three mortars of 60 and 81 millimeters were loaded into the release system in the test. With the command given by the remote control, the drone fired at the point determined with the non-explosive test ammunition. (HaberDergilik/Kara-birliklernin-silahi-havan-dronla-havlandi, 2022)

After the test, Kivrak told Anadolu Agency (A.A.) that when an

image is taken from any point in the field, the drone loaded with mortar can be directed to the desired coordinate and left three ammunitions with the release system. Kivrak said:

“We have developed a system that releases one 81 and two 60 mortars. There was a need in this direction, but we could not meet it. As a university and laboratory, we decided to do it ourselves. A very affordable Mortar Release System with the equipment we found on the market and the electronic control system we made ourselves. “We did it, and we made patent applications. We tested it in the process. Our system works very well.” (HaberDergilik/Kara-birliklernin-silahi-havan-dronla-havlandi, 2022)

Expressing that they cooperated with the drone manufacturer Ari Defense in the project, Kivrak noted that the drone, which can carry 25 kilograms, stay in the air for about half an hour, and connect different payloads, is domestic with its software and hardware. (HaberDergilik/Kara-birliklernin-silahi-havan-dronla-havlandi, 2022)

### **Point shooting with a drone**

The radiant drone will be sent, and it will drop three mortar shells on the elements visually. If you try to do it under normal conditions, it is difficult and difficult to shoot these coordinates and adjust the weapon. We will have eliminated the terrorist elements with a very simple and appropriate structure in such a system. When you consider the cost, such a system has a cost of approximately 1500-2000 T.L. (HaberDergilik/Kara-birliklernin-silahi-havan-dronla-havlandi, 2022)

We have very good works related to unmanned aerial vehicles and release systems as a country. It is heard in the world right now. Therefore, if we produce affordable and sustainable products, we will meet the needs of our own armed forces as soon as possible, and we will cure the oppressed nations as we do

now.” (HaberDergilik/Kara-birliklernin-silahi-havan-dronla-havlandi, 2022)

**Figure 6.6: Point Shooting with a Drone**



Source: (HaberDergilik/Kara-birliklernin-silahi-havan-dronla-havlandi, 2022)

#### **Case Study 6.4: Loitering Munitions (LM or L.M.)**

**Figure 6.7: Russian KUB-BLA “Suicide Drone”**





Source: (Knight, 2022)

Russia's ZALA Aero Group, the unmanned aircraft systems (UAS) division of Kalashnikov, unveiled a "kamikaze" drone — the KUB-BLA — at the International Defense Exhibition and Conference (IDEX) in Abu Dhabi on February 17. The small UAS is designed to have a maximum speed of about 80 miles per hour, an endurance of 30 minutes, and an explosive payload of 7 pounds against "remote ground targets." (Wolfe, 2019)

Loitering munitions can have a dwell time of up to six hours and are equipped with sensors to allow the drones to detect and attack targets independently.

"The maker of the lethal drone claims that it can identify targets using artificial intelligence."

A RUSSIAN "SUICIDE drone" that boasts the ability to identify

targets using artificial intelligence has been spotted in images of the ongoing invasion of Ukraine. (Knight, 2022)

Photographs showing what appears to be the KUB-BLA, a type of lethal drone known as a “loitering munition” sold by ZALA Aero, a subsidiary of the Russian arms company Kalashnikov, have appeared on Telegram and Twitter in recent days. The pictures show damaged drones that appear to have crashed or been shot down. (Knight, 2022)

With a wingspan of 1.2 meters, the sleek white drone resembles a small pilotless fighter jet. It is fired from a portable launch, can travel up to 130 kilometers per hour for 30 minutes, and deliberately crashes into a target, detonating a 3-kilo explosive. (Knight, 2022)

ZALA Aero, which first demoed the KUB-BLA at a Russian air show in 2019, claims in promotional material that it features “intelligent detection and recognition of objects by class and type in real-time.” (Knight, 2022)

The drone itself may do little to alter the course of the war in Ukraine, as there is no evidence that Russia is using them widely so far. But its appearance has sparked concern about the potential for A.I. to take a greater role in making lethal decisions. (Knight, 2022)

“The notion of a killer robot—where you have artificial intelligence fused with weapons—that technology is here, and it’s being used,” says Zachary Kallenborn, a research affiliate with the

National Consortium for the Study of Terrorism and Responses to Terrorism (START).

(Knight, 2022)

### **Figure 6.8: KUB-BLA Russian Loitering Munition**



Source: (Front, 2020)

Advances in A.I. have made it easier to incorporate autonomy into weapons systems and have raised the prospect that more capable systems could eventually decide for themselves who to kill. A UN report published last year concluded that a lethal drone with this

capability might have been used in the Libyan civil war. (Knight, 2022)

**Figure 6.9: Russian Suicide Drone Used in Ukraine That Picks its Own Targets Though Advance A.I.**



Source: (Wolfe, 2019)

It is unclear if the drone may have been operated in this way in Ukraine. One of the challenges with autonomous weapons may prove to be the difficulty of determining when full autonomy is used in a lethal context, Kallenborn says. (Knight, 2022)

The KUB-BLA images have yet to be verified by official sources, but the drone is known to be a relatively new part of Russia's military arsenal. Its use would also be consistent with Russia's shifting strategy in the face of the unexpectedly strong Ukrainian resistance, says Samuel Bendett, an expert on Russia's military with the defense think tank CNA. (Knight, 2022)

Bennett says Russia has built up its drone capabilities in recent years, using them in Syria and acquiring more after Azerbaijani

forces demonstrated their effectiveness against the Armenian ground military in the 2020 Nagorno-Karabakh war. “They are an extraordinarily cheap alternative to flying manned missions,” he says. “They are very effective both militarily and of course psychologically.” (Knight, 2022)

Russia seems to have used few drones in Ukraine early on, which may be due to misjudging the resistance or effective Ukrainian countermeasures. (Knight, 2022)

But drones have also highlighted a key vulnerability in Russia’s invasion, entering its third week. Ukrainian forces have used a remotely operated Turkish-made drone called the TB2 to great effect against Russian forces, shooting guided missiles at Russian missile launchers and vehicles. The paraglider-sized drone, which relies on a small crew on the ground, is slow and cannot defend itself, but it has proven effective against a surprisingly weak Russian air campaign. (Knight, 2022)

The Biden administration said it would supply Ukraine with a small US-made loitering munition called Switchblade this week. This single-use drone, equipped with explosives, cameras, and guided systems, has some autonomous capabilities but relies on a person to decide which targets to engage. (Knight, 2022)

But Bennett questions whether Russia would unleash an AI-powered drone with advanced autonomy in such a chaotic environment, especially given how poorly coordinated the country’s overall air strategy seems to be. “The Russian military and its capabilities are now being severely tested in Ukraine,” he says. “If the [human] ground forces with all their sophisticated information gathering can’t understand what’s happening on the ground, how could a drone?”

Several other military experts question the purported capabilities of the KUB-BLA. (Knight, 2022)

“The companies that produce these loitering drones talk up their autonomous features, but often the autonomy involves flight corrections and maneuvering to hit a target identified by a human operator, not autonomy in the way the international community would define an autonomous weapon,” says Michael Horowitz, a professor at the University of Pennsylvania, who keeps track of military technology. (Knight, 2022)

Despite such uncertainties, the issue of A.I. in weapons systems has become contentious because the technology is rapidly finding its way into many military systems, for example, to help interpret input from sensors. The U.S. military maintains that a person should always make lethal decisions, but the U.S. also opposes a ban on developing such systems.

To some, the appearance of the KUB-BLA shows that we are on a slippery slope toward increasing the use of A.I. in weapons that will eventually remove humans from the equation. (Knight, 2022)

“We’ll see even more proliferation of such lethal autonomous weapons unless more Western nations start supporting a ban on them,” says Max Tegmark, a professor at MIT and co-founder of the Future of Life Institute, an organization that campaigns against such weapons. (Knight, 2022)

Others, though, believe that the situation unfolding in Ukraine shows how difficult it will be to use advanced A.I. and autonomy. (Knight, 2022)

William Albergue, Director of Strategy, Technology, and Arms Control at the International Institute for Strategic Studies, says that given Ukraine’s success with the TB2, the Russians are not ready to deploy more sophisticated tech. “We’re seeing Russian morons getting owned by a system that they should not be vulnerable to.” (Knight, 2022)

**Figure 6.10: The Wreckage of Another Russian KUB-BLA Loitering Munition.**



Source: 3/ (Lee) (Lee, 2022)

**Figure 6.11: US Marine firing Switchblade from a pneumatic launch tube**



Source: (Bowman, 2022)

On the other side, Ukraine has been thrust into the forefront of using loitering munitions in defense and is now a testbed for western observers.

Loitering munitions — essentially small suicide drones capable of tracking a target and then striking it — have been around for years. Still, technology emerged as a key weapon in the 2021 conflict between Armenia and Azerbaijan. In Ukraine's urban warfare, the system maybe even more valuable. Two Foundation for Defense of Democracies experts explain why loitering munitions are the perfect tool for Ukraine's resistance and what systems could be sent to Kyiv in a new op-ed. (Bowman, 2022)

Hours after, Ukrainian President Volodymyr Zelenskyy delivered an impassioned plea for help to the U.S. Congress on March 16. President Joe Biden announced that Washington will provide \$800 million in additional security assistance to Ukraine, including 100 Switchblade loitering munitions (L.M.s), commonly referred to as



“suicide drones.” While members of Congress have pushed for the potential transfer to Ukraine of Polish MiG-29s, the White House is wise to prioritize weapon systems that can quickly bolster Ukrainian combat capability while minimizing logistical burdens and vulnerability to Russian attack. (Bowman, 2022)

The problem, however, is Ukraine will likely expend those 100 Switchblades in mere days, and the variant of the Switchblade Washington is most likely sending is of no serious use against Russian armor. Accordingly, Washington should work with NATO allies to urgently provide Ukraine with additional shipments consisting of greater quantities and varieties of loitering munitions, or L.M.s. (Bowman, 2022)

L.M.s are a combination of missiles and aerial surveillance drones. They blend the ability to maneuver, conduct surveillance, and strike targets into a single platform, reducing the time between detection and engagement of a target. That could prove decisive for Ukrainian defenders who may encounter more close-quarters urban combat in the coming days. (Bowman, 2022)

L.M.s vary in size and capability. Loiter time above potential targets can range from minutes to hours, while their munition can be sized to target troops, equipment (with and without armor), or military infrastructure. The systems carry cameras to identify targets and transmit images back to the operator. L.M.s can be difficult for adversaries to detect and destroy because of their low radar, visual, and thermal signatures. (Bowman, 2022)

### **Figure 6.12: Switchblade 600**



Source: (Valpolini, 2020)

Some L.M.s can be mounted on and launched from ground vehicles. Smaller versions, such as the Switchblade, can be carried even in backpacks and employed by individual soldiers. This will provide Ukrainian infantry squads with increased combat power that can be easily transported, concealed, and operated. And unlike manned aircraft and larger drones, L.M.s don't depend on airfields for employment. That will create real problems for Russian forces, which will have to assume that any Ukrainian infantry may have this capability. (Bowman, 2022)

Ukraine has already employed some types of drones during the conflict. The Ukrainians have used their Turkish TB-2 armed drones, which are not loitering munitions, to devastating effect, as demonstrated in numerous videos on social media. Turkey provided Ukraine with a much-needed resupply of these drones during the conflict's first week. TB-2s are quite large, with a wingspan of approximately 12 meters, and must operate from fixed airbases that can and have been targeted by Russia. (Bowman, 2022)

Ukraine has recruited drone hobbyists operating commercial

drones to help address urgent military requirements for smaller drones to conduct reconnaissance. Ukrainians have sometimes resorted to jerry-rigging explosives to the bottom of commercial drones. Ukraine has even created a basic L.M. system by pairing the Punisher drone with a smaller reconnaissance drone called Spectre, which together have reportedly conducted strikes. (Bowman, 2022)

The United States and like-minded allies should immediately send more inexpensive commercial systems instead of forcing Ukraine to rely on Chinese DJI drones, which might compromise the operator's information or be restricted from flying in certain areas via geofencing. But L.M.s can fill an important gap between the TB-2s (which rely on airfields and incur a significant logistical burden) and makeshift commercial drones that take time to prepare and are less effective than L.M.s in targeting ground forces. (Bowman, 2022)

Accordingly, the United States and like-minded allies should systematically equip the Ukrainian military with a large arsenal of purpose-built L.M.s. This is especially important because Russia may be starting to jam the command and control of TB-2 drones. Moscow has also begun to integrate better its reconnaissance and combat drones, including the ZALA KYB loitering munition. (Bowman, 2022)

There are several different L.M.s that countries willing to provide lethal aid to Ukraine have in their arsenal. The U.S., as mentioned earlier, Switchblade has seen service in Afghanistan. But while it is effective in short-range urban combat and ambushes on unarmored convoys, the Switchblade has limited range compared to some other L.M.s. And contrary to some current reporting, the Switchblade 300 variant Washington appears to be sending Ukraine (as opposed to the Switchblade 600 variant) cannot destroy most armored vehicles due to its small munition. The 100 Switchblades announced this week are only a fraction of the quantity of L.M.s that Ukraine needs. (Bowman, 2022)

So, while Congress should press the administration to send Ukraine more American-made LMs, the United States should also solicit help from other countries. Turkey operates the Kargu-2, which has seen combat in Libya, and Australia manufactures the Drone-40, both of which can be useful in an urban environment. Poland's Warmate-series of L.M.s can strike targets out to roughly 9 km. The Warmate's portability and range make it suitable for disrupting Russian supply convoys from a safe distance. (Bowman, 2022)

Notably, Israel operates some of the most advanced L.M. capabilities. Still, it thus far has not provided Ukraine with lethal aid, needing to tread carefully with Moscow given that Russia could hamper Israeli operations in Syria against their archenemy, Iran. Not providing military capabilities to Ukraine may also enable Jerusalem to help mediate an end to the war. However, if Israel decides to permit third-party transfers of Israeli-made weapons to Ukraine, the Harop and Orbiter L.M.s should be at the top of the list. (Bowman, 2022)

L.M.s can provide Ukraine with a robust additional capability to strike Russian forces from the air, especially as those forces linger on roads, consolidate around Ukrainian cities, or move into urban areas. L.M.s can deliver this capability in large quantities at a fraction of the cost and logistical footprint associated with operating and maintaining fighter jets or large drones. (Bowman, 2022)

The U.S. arms shipment announced Wednesday is a positive step, but it should not be the last. Working with allies, Washington should urgently send another tranche of weapons to Ukraine, and that shipment should include a greater quantity and variety of loitering munitions. (Bowman, 2022)

**Figure 6.13: Artist rendition of a switchblade launch**



Source: (Valpolini, 2020)

The case continues to be made for developing effective countermeasures against this new and ever-evolving kind of warfare must be a priority. Lawmakers must be aware of this growing threat that, if left unchecked, these deadly autonomous systems will soon find their way into the hands of a determined individual or team who will use a drone with A.I.-backed capabilities to hunt down anyone they oppose and want to eliminate. The stuff of sci-fi lore is here today and waiting to make a major impact terribly. Common citizens use this technology to bring military juggernauts to their knees in frustration.

Thankfully, the technology does exist to counter these very real threats, and lawmakers must continue to fund their development and seek to acquire not just one solution but many. Artificial intelligence and machine learning (AI / ML) is also used in the counter-drone fight, with excellent results. Identification, classification, and sharing of information are critical in the fight. It

shapes the formation of sensor networks linked to many different kinetic and non-kinetic systems. These systems will then remove drones from the sky safely and effectively with minimal to no collateral damage.

### **Conclusion**

The conclusion is straightforward. Drones are both a perfect delivery payload for explosives, and with the use of A.I., they can be directed at any target of opportunity.

### **Bibliography**

Bowman, R. B. (2022, March 18). *Breaking Defense*. Retrieved from Ukraine is getting Switchblade. It should be just the first wave of loitering munitions for Kyiv: <https://breakingdefense.com/2022/03/ukraine-is-getting-switchblade-it-should-be-just-the-first-wave-of-loitering-munitions-for-kyiv/>.

Crumley, B. (2022, March 11). *DroneDJ*. Retrieved from Ukraine reportedly adapts small drones to drop Molotov cocktails in war with Russians: <https://dronedj.com/2022/03/11/ukraine-reportedly-adapts-small-drones-to-drop-molotov-cocktails-in-war-with-russians/>.

Emir, C. (2022, January 13). *Interesting Engineering*. Retrieved from interestingengineering.com: <https://interestingengineering.com/the-most-brutal-mexican-cartel-used-drones-to-drop-bombs-on-their-rival>

Front, S. (2020, August 12). *southfront.org*. Retrieved from Russia Confirms Usage of Kalashnikov Kamikaze Drone 'KUB-BLA' in Syria: <https://southfront.org/russia-confirms-usage-of-kalashnikov-kamikaze-drone-kub-bla-in-syria/>.

HaberDergilik/Kara-birliklernin-silahi-havan-dronla-havlandi. (2022, March 20). Retrieved from ssdergilik.com: [ssdergilik.com: ssdergilik.com/tr/HbaerDergilik/Kara-birliklernin-silahi-havan-dronla-havlandi](https://ssdergilik.com/tr/HbaerDergilik/Kara-birliklernin-silahi-havan-dronla-havlandi)

Kesslen, B. (2022, March 10). *Ukrainians develop a drone that drops Molotov cocktails*. Retrieved from New York Post: <https://nypost->

com.cdn.ampproject.org/c/s/nypost.com/2022/03/10/  
ukrainians-develop-drone-that-drops-molotov-cocktails/amp/

Knight, W. (2022, March 17). *Wired*. Retrieved from Russia's Killer Drone in Ukraine Raises Fears About A.I. in Warfare: <https://www.wired.com/story/ai-drones-russia-ukraine/>.

Lee, R. (2022, March 14). *Twitter*. Retrieved from Twitter @RALee85: [https://twitter.com/RALee85/status/1503494100233949190?ref\\_src=twsrc%5Etfw](https://twitter.com/RALee85/status/1503494100233949190?ref_src=twsrc%5Etfw)

Valpolini, P. (2020, February 2). *European Defense Review Magazine*. Retrieved from Switchblade 600, the new Medium Range Loitering Munition: <https://www.edrmagazine.eu/switchblade-600-the-new-medium-range-loitering-munition>

Wolfe, F. (2019, February 21). *Aviation Today*. Retrieved from Russia Unveils KUB-BLA Kamikaze Drone at IDEX 2019: <https://www.aviationtoday.com/2019/02/21/russia-unveils-kub-bla-kamikaze-drone-idex-2019/>.





# 7. Deception

**By Professor Randall K. Nichols, Kansas State University**

## **STUDENT OBJECTIVES**[\[1\]](#)

Students will understand and study:

The various deception methods and technologies employed against critical infrastructure assets and computer targets,

Recognize that unmanned aircraft (UAS) are reasonable deployment agents against critical infrastructure and CBRN assets. UAS are expendable, quiet, hard to detect, and can act in numbers (SWARMS) in many deception domains.

Unmanned systems present a lethal risk of deception operations and should be accounted for in security plans.

## **INTRODUCTION**

Picture for a moment you are watching your child playing H.S. football in a state championship game. There are about 22,000 in attendance. The game clock is about 10 minutes after halftime. Yelling, cheering, and screaming for their teams, they hardly notice the three medium-sized drones flying over the stands. The drones start dropping hundreds of small pieces of paper over the crowd and then leave the area. The notes say: "You have 15 minutes to evacuate – the next drones carry fentanyl and Semtex explosives. You are not safe. Evacuate!" 15 minutes later, nearly 50 drones SWARM over the stadium dropping talcum powder and powerful firecrackers on the crowd. This is a terrorist scenario that relies on DECEPTION aimed at causing Panic in a crowd and DISRUPTION.[\[2\]](#) Its goal is to make people fear and lose faith in their local government to protect them. Drones can be the precursor!

Terrorists rely on how crowds behave in a Panic Situation. (Bade, 2009) provided insight into the theories about crowd behavior in

Panic Situations. Table 7.1 shows that crowds don't act as crowds during a panic situation but as a group of individuals. They resort to individual behavior at the expense of all others. They exhibit both Panic Theory and Urgency Theory.

**Panic Theory** embraces four principles:

- Deal primarily with the factors that may make the occurrence of Panic during emergencies,
- The basic premise is that when people perceive danger, their usual conscious personalities are often replaced by the unconscious personalities, which lead them to act irrationally,
- Hysterical flight,
- Ignorance of the environment. (Bade, 2009)

**Urgency Theory** embraces two main principles:

- The occurrences of human blockages of exiting space depend on the levels of urgency to exit
- Three crucial factors could lead to this situation:
  - the severity of the penalty and consequence for not exiting quickly,[\[3\]](#)
  - the time available to exit, and
  - the group size.

A problem arises when the distribution of urgency levels contains a large number with a high urgency to leave; for example, too many people try to exit quickly at the same time ( with limited exits). (Bade, 2009)

**Table 7.1 Characteristics of Emergency Behavior**

| BEHAVIOR                        | SPECIFICATION   |
|---------------------------------|---|
| PANIC                           | Irrationality   |
|                                 | Bewilderment  |
|                                 | Hysterical Flight   |
|                                 | Ignorance of environmental shock<br>numbness  |
| Shock & Inactivity              | No movement (Normal)<br>Original plan execution                                     |
| Normal Behavior                 | No change in behavior directed<br>Normal to fast walk to affiliate                  |
| Directed flight and affiliation | Factors (family, home, etc.)<br>Formation of ad-hoc groups<br>Movement in groups    |
| Maintain affiliation            | Leader following<br>Assisting group members<br>Mutual helping based on social roles |
| Pro-social response - mutual    | Provision of first aid & rescue<br>Self-sacrifice for the sake of helping others    |

Source: (Bade, 2009) Photo by Author from original manuscript to meet PB guidelines.

Two famous Panic Theory / Urgency Theory examples are 1) The Station Nightclub Fire in Rhode Island in 2003, which killed ~100 and injured 200 more. (CBS News, 2021 updated)[4] and 2) May 9, 2001, Accra Sports Stadium Disaster[5] (Chrockett, 2014)

The author has contributed to the science of Panic Attack responses with an article on how to respond before the full-blown Panic arrives. (Nichols R. K., short-circuiting-simple-panic-attacks-quick-guide-out, 2018)

## VULNERABILITIES OF MODERN SOCIETIES TO UAS ATTACK

According to (Dorn, 2021), the federal government has yet to acknowledge the threats posed by UAS, and it barely noticed the USS and UUS's capabilities and the threat platforms they pose. Present-day unmanned systems are faced with a contradictory relationship between their small degree and the likelihood of

detection and the small degree of lethality that a single unmanned system represents. If an unmanned system successfully attacks a congested target, such as a ballgame, it is unlikely to kill more than a few fans. The attack creates a sense of fear in the citizens; terrorism has been brought to their doorsteps, and the uncertainty in the government's ability to prevent such attacks and protect its citizens. (Dorn, 2021) A boosted course of action uses a combination of manned and unmanned systems operating as a team (MUM-T) or in SWARM mode to deliver payloads. (Nichols & Mumm, Unmanned Aircraft Systems in the Cyber Domain, 2nd Edition., 2019) If the terrorist has access to CBRNE agents/weapons, this will present a significant long-term threat to the U.S.

(Kallenborn & Bleck, 2018) exposed that UAS have the potential to be substituted for CBRN agents in an attack. The UAS could be used as a SWARM with explosives, or if CBRN agents are to be used in the attack, a UAS SWARM would be an ideal platform to deliver such agents to a specific target or in a widely dispersed manner.

(Nichols & al., 2020) (Nichols & Sincavage, Disruptive Technologies with Applications in Airline, Marine, and Defense Industries, 2021) suggested that the UAS can be agents of deception, and their payloads can be used to create Panic.

## **BASIC TERMINOLOGY**

The study of deception has a variety of roots. The best text on Deception and Counter Deception principles is (Bennett & Waltz, 2007). Its use has been well researched and published. The idea of using UAS as a deployment vehicle is new and credited to the authors. (R. K. Nichols & et al., 2022) The art/science of deception has its own terminology to distinguish deception activities' principles, means, and effects. The basic DoD accepted terms are: (Daniel & Herbig, 1982)

**Denial** includes those measures designed to hinder or deny the enemy the knowledge of an object by hiding or disrupting the means of observation of the object. The basis for Denial is **dissimulation**, the concealing of truth. (Daniel & Herbig, 1982)

**Deception** includes measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests. The goal of deception is to make an enemy more vulnerable to the effects of weapons, maneuvers, and operations of friendly forces. The basis for deception is a **simulation**, the presence of that which is false. (Daniel & Herbig, 1982)

**Denial and Deception** ( D & D) include integrating both processes to mislead an enemy's intelligence capability. The acronym C3D2 is synonymous with D & D; it refers to **cover, concealment, camouflage, Denial, and deception**. (Daniel & Herbig, 1982)

Deception **means** are those methods, resources, and techniques that can convey information to the deception target. DoD characterizes means as:

*Physical means*: activities and resources used to convey or deny selected information to a foreign power. (Examples are military operations, reconnaissance, force movement, dummy equipment, logistical actions, test, and evaluation activities.)

*Technical means* are defined as: Resources and operating techniques to convey or deny selected information through deliberate radiation, alteration, absorption, reflections of energy; the emission or suppression of chemical or biological odors; and the emission or suppression of nuclear particles.

*Administrative means* are resources, methods, and techniques to convey or deny an enemy's oral, pictorial, documentary, or other physical evidence.

The *Deception target* is the adversary decision-maker with the authority to decide what will achieve the *deception objective* – the desired result of the deception operation.

*Channels* of deception are the information paths by which deception means are conveyed to their targets. (Daniel & Herbig, 1982)

## PERSPECTIVES OF DECEPTION

(Bennett & Waltz, 2007) present 60 pages of Deception research. There are two models of deception that apply to the UAS environment. (Gerwehr & Glenn, 2002) present their *three perspectives on Deception* in Table 7.2.

**Table 7.2 Three Perspectives on Deception**

| Level of Sophistication   | Effect Sought  | Means of Deception  |
|---|--|---|
| <p><i>Static:</i> Deceptions that remain static regardless of state, activities, or histories of either the deceiver or target masking</p>  | <p><i>Masking:</i> Concealing a signal. Ex: camouflage, concealment, and signature reductions.</p>   | <p><i>Morphological:</i> The part of the deception is primarily a matter of substance, shape, coloration, or temperature.</p>   |
| <p><i>Dynamic:</i> Deceptions that become active under specific circumstances. The ruse itself and associated trigger do not change over time nor vary significantly by circumstance or activity.</p> | <p><i>Misdirecting:</i> Transmitting an unambiguous false signal. Ex: feints, demonstrations, decoys, dummies, disguises, and disinformation.<a href="#">[6]</a></p>   |   |
| <p><i>Adaptive</i> are: Dynamic, and the trigger or ruse can be modified with experience. Deceptions that improve with trial and error.</p>   |  | <p><i>Behavioral:</i> The part of the deception is primarily a matter of implementation or function, such as timing, location, or patterns of events or behavior.</p> |
| <p><i>Premeditative:</i> Deception is designed and implemented based on experience, knowledge of the deceiver's capabilities, and the target's sensors and search strategies.</p>                     | <p><i>Confusing:</i> Raising the noise level to create uncertainty or paralyze the target's perceptual capabilities. Ex: voluminous communication traffic, conditioning, and random signals or behavior.</p> |   |

Source: (Gerwehr & Glenn, 2002)

**DECEPTION MAXIMS**

One of the important results of the CIA's ORD Deception Research Program was the paper on Deception Maxims. (MathTech, Inc, 1980) All 10 Maxims are covered in detail in (Bennett & Waltz, 2007) Table 7.3 shows ten interesting Deception Maxims.

**Table 7.3 Deception Maxims**

| MAXIM   | RESULT  |
|---|---|
| <b>#1 Magruder's Principle</b>                                    | <b><i>It is easier for the target to maintain a preexisting belief even if presented with information expected to change that belief.</i></b>   |
| #2 Limitations to human Information processing                    | Limitations to human information processing can be design deception schemes, including the law of small numbers and susceptibility to conditioning  |
| #3 the Multiple forms of surprise                                 | Surprise can be achieved in different forms: location, strength, intention, style, and timing. <a href="#">[7]</a>  |
| <b>#4 Jones' Lemma</b>  | <b>Deception becomes more difficult as the number of channels available to the target increases. The greater the number the deceiver controls the deceiver, the greater the likelihood that the deception will be achieved! <a href="#">[8]</a></b> |
| #5 A choice among types of deceptions                             | The objective of the deception planner should be to reduce the ambiguity in the mind of the target to make the target more certain of a particular falsehood rather than less certain of the truth  |
| #6 Axelrod's contribution: the husbanding of assets               | There are circumstances where deception assets should be husbanded, despite the costs of maintaining them and the risk of the exposure until they can be put to fruitful use  |
| #7 A sequencing rule  | Deception activities should occur in a sequence that prolongs the target's false perceptions of the situation for as long as possible   |
| #8 Importance of feedback   | Accurate feedback from the target increases the deceptions likelihood of success  |
| #9 The Monkeys Paw  | <i>The deception may produce subtle and unwanted side effects.</i> Deception planners should be sensitive to this possibility and attempt to minimize them  |
| #10 Care in designing the planned placement of deceptive material | Great care must be taken when designing schemes to leak notional plans. Apparent windfalls are subject to close scrutiny and are often misbelieved.   |

Source: (MathTech, Inc, 1980)

Take note of Maxims #1, #4, and #9. These are the key to UAS deployment for Deception objectives. [\[9\]](#)



## **SURPRISE**

Jock Haswell, Michael Dewar, and Jon Latimer (all former British officers) have written about purpose, principles, and deception techniques. They all emphasize that the goal of deception in warfare is a surprise. Five principles are common to all three authors' writings:

- Preparation: Successful deception operations require careful intelligence preparation to develop detailed knowledge of the target and the target's likely reaction to each part of the deception.
- Centralized control and coordination: Uncoordinated deception operations can confuse friendly forces (or terrorists, depending on POV) and reduce or negate the effectiveness of the deception.
- Credibility: The deception should produce false and real information and a pattern of events that align with the target's preconceptions and expectations.
- Multiple information channels: False information must be presented to the target through as many channels as possible without arousing the target's suspicions that the information is too good to be true. This is also called *confirmation bias*.
- Security: Access to the deception plan must be carefully restricted. Information released to the target must be revealed so that the absence of normal security precautions does not arouse the target's suspicions. (Haswell, 1985)(Dewar, 1989)(Latimer, 2001)

## **Four Fundamental Principles**

Four Fundamental Principles form the foundation of deception theory in general. These principles relate to how the target of deception acquires, registers, processes, and ultimately perceives

data and information about their world. They are Truth, Denial, Deceit, and Misdirection. (Bennett & Waltz, 2007) See Table 7.4.

- 1. Truth: All deception works within the context of what is true.
- 2. Denial: *Denying the target access to the truth is the prerequisite to all deception.*
- 3. Deceit: All deception requires deceit.
- 4. Misdirection: Deception depends on manipulating what the target registers. See Table 7.4.

**Table 7.4 Deception**

| DECEPTION   | DECEPTION   | DECEPTION   | DECEPTION   |
|---|---|---|---|
| Truth   | Denial  | Deceit  | Misdirection  |
| All deception works within the context of what is true denying  | <i>Denying the target access to the truth is the prerequisite to all deception.</i>   | All deception requires deceit.  | Deception depends on manipulating what the target registers provide   |
| Provides the target with real data and accurate information blocks  | Blocks the target's access to real data and accurate information.   | Provides the target with false data and wrong or misleading information.  | Determines where and when the target's attention is focused: what registers   |
| It influences how the target registers, processes, and perceives data and information and, ultimately, what the target believes and does. | It influences how the target registers, processes, and perceives data and information and, ultimately, what the target believes and does. | It influences how the target registers, processes, and perceives data and information and, ultimately, what the target believes and does. | It influences how the target registers, processes, and perceives data and information and, ultimately, what the target believes and does. |

Deception is the deliberate attempt to manipulate the perceptions of the target. If deception is to work, there must be

a foundation of accurate perceptions that can be manipulated. All deception works within the context of what is true (or honest). (Mitchell, 1986, p358)

Denial and deception (D & D) is the universal description for strategic deception. *Denial* blocks the target's access to real data and accurate information and can be considered a standalone concept; it is the linchpin to deception. Denial's other terms are *security, secrecy, cover, dissimulation, masking, or passive deception*. Denial protects the deceiver's real capabilities and intentions. (Bennett & Waltz, 2007)

All deception requires deceit. The methods of Denial (secrecy, concealment, and signal reduction) reduce or eliminate the real signals that the target needs to form accurate perceptions of a situation. (Dewar, 1989)

Misdirection is the most fundamental principle of all practitioners of magic. In magic, misdirection directs the audience's attention towards the effect and away from the method that produces it.

### **Three examples of UAS Attacks could be Destruction, Disruption, or Deception (D/D/D)**

(Dorn, 2021) presents three attacks on critical infrastructure that could be developed for *Destruction, Disruption, or Deception (D/D/D)*. Depending on the terrorist objectives, the UAS payloads could be structured to deliver weapons for any of the three Ds. The easiest objective (best terrorist case for their investment) would be deception which would provide testing of defenses for ISR purposes. The moderate case would be Disruption of services and personnel. The worst-case and best defended would be to use actual CBRN agents. Chances of lethal success would be minimized. Exposure would be maximized. It all depends on the attacker's objective and how lethal the plans are to accomplish their goals.

Attack 1: Ronald Reagan National Airport (RRNA). DHS designated the area around RRNA a-defend-at-all-costs asset in metropolitan Washington, DC. Multiple large UAS (called motherships) carrying

multiple smaller UAS, all capable of independent action against multiple targets, present themselves. The motherships follow well-established low-level transit routes (LLTR) to blend in with aircraft traffic in and out of RRNA and Joint Base Andrews. The confusion and inaction of FAA controllers would be long enough for the motherships to divert and drop their load of smaller UAS / drones. What distinguishes the D/D/D cases are the payloads. Payloads could be CBRNE agents, talcum powder and firecrackers, or paper leaflets for a PSYOPS deception. In all three, the target will suffer Panic, and the media coverage will guarantee a victory for the terrorists. (Dorn, 2021)

Attack 2: Multiple UAS engage in attacks on multiple nuclear power plants on the east coast.

By launching multiple UAS in a SWARM formation, terrorists would conduct overflights of essential plants within a given region and overwhelm the first responder and LEO assets. The dispersal of powder or liquids would cause Panic only if the plant workers observed it. Assuming a fixed dispersal unit and a CBRN agents payload, plant workers would walk or run through the contaminated area ( parking lot, facility grounds) and carry the agents into the plant. The SOP for nuclear plants would be that the plant would be shut down once a radiation leak alarm was triggered. All personnel would be evacuated. Figure 7.1 shows the approximate locations of 99 operating nuclear power plants within the U.S. These 99 nuclear plants provide 19.7% of the U.S. daily electrical requirements. The two prime targets would be the dome-shaped structures and the outside cooling towers. It is probable that a SWARM attack on multiple nuclear power plants would succeed. (Dorn, 2021) The nuclear reactor is safe and guarded by ten-foot-thick steel-reinforced walls, concrete, and a dome. The plant's turbines, generators, condensers, spent fuel rod facilities, and cooling towers are not built to the same standard. (Dorn, 2021) suggests "that there are no tactics, techniques, and technologies to deter, deny, disrupt, or destroy the threat that UAS poses to the nuclear explosive

ordinance and mitigating the effects of a UAS overflight in which CBRN agents were released on the employees and compound.”

The authors disagree. Classified systems are not covered in this book but certainly exist. Non-classified defenses for critical infrastructure attacks of this sort are covered in detail in (Nichols R. K., 2020). New C-UAS systems are coming on stream every day from multiple vendors and interests as we write this chapter. The scenario is interesting but not so bleak. (Nichols & Sincavage, Disruptive Technologies with Applications in Airline, Marine, and Defense Industries, 2021) (Nichols R. K., 2020)

Attack 3. Expansion of author's introductory stadium attack. Multiple UAS or SWARM equipped with several grams of explosive CBRN agents or fentanyl, Trichloroisocyanuric acid, or carfentanil (extremely lethal in small amounts) could disperse them from above an open stadium filled with spectators during a sporting event. The UASs could be launched out of multiple briefcases, backpacks, large purses, or vehicles outside the stadium. A safe distance is a plus for the terrorists. The same agents could be launched from a USS or UUV land or on the water while passing outside the stadium. (Dorn, 2021)

All three of the above attacks would involve D & D operations to misdirect the defending forces.

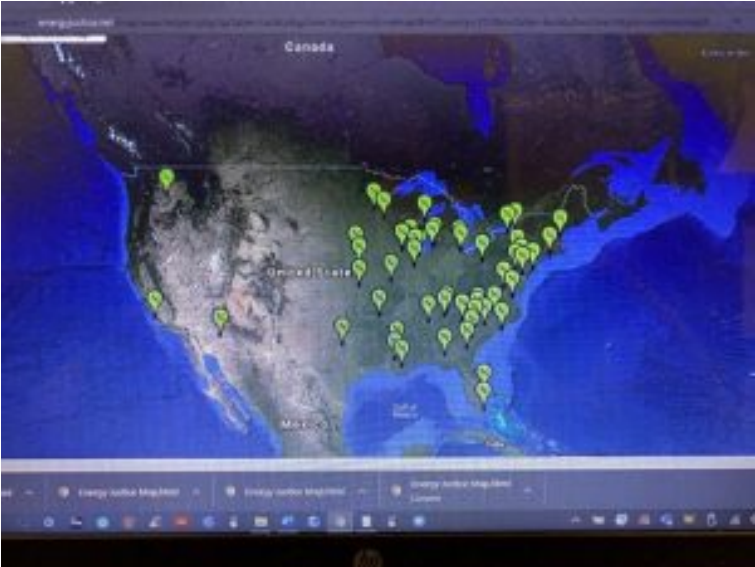
### **Taxonomy of Technical Methods of Deception**

There are four basic toolsets to implement deception objectives. They are:

1. Methods to influence sensing channels, either by human senses directly or through remote sensors employed to extend the human senses.
2. Methods employed to deceive signal and computer processes
3. Deceptive methods employed in the human intelligence (HUMINT) trade exploit intelligence organizations' information channels. (Bennett & Waltz, 2007)

See Table 7.5 for more detail.

**Figure 7.1 Operating Nuclear Power Plants within the U.S.**



Source: (EnergyJustice.net, 2022)

**Table 7.5 Categories of Deception Channels and Methods**

| Tool Set  | Channels Manipulated   | True / False | Reveal<br>In Deception Matrix   | Conceal<br>In Deception Matrix   |
|---|--|--------------|---|--|
| Channels<br>CC&D<br><br><i>Camouflage, Concealment, Deception</i> | Physical sensors (technical & human sense)   | True         | Reveal limited real units & activities to show strength, influencer enemy sensor coverage, sensitivities;                   | Camouflage paint & nets; radar nets, thermal, audio, radar signature suppression<br>Activities in facilities underground to avoid surveillance or hidden dual-usage facilities |
|   | Governing principles: Physics, Manipulate physical phenomena, electromagnetic spectra. | True         | Reveal true commercial capability of dual-use facilities, provide true “cover” to misdirect from noncommercial weapons. use |  |
| Channels<br>CC&D<br><br><i>Camouflage, Concealment, Deception</i> |  | False        | Thermal, radar, audio signature simulation. Physical vehicle & facility decoys  | Maintain OPSEC on existing methods & extent of CC&D capabilities (equipment, nets, decoys, ECM support).   |
| Signals / Channels / D & D  | Channels: Abstract symbolic representations of information                             | True         | Reveal limited alluring information on honeypots (deceptive network servers) to lure attackers and conduct sting operations | Cryptographic & steganographic hiding messages; Polymorphic (dynamic disguise) of worm code or <i>cyber weapons</i> (Nichols & Ryan, 2000)                                     |

|                        |  |       |  |  |
|------------------------|--|-------|--|--|
|                        | Governing Principles:<br>Logic/game theory;<br>manipulate information & timing of information          | True  |  |  |
|                        |  | False | Communication traffic simulation. Reveal false flag /feed information on honeypots. Decoy software agents & traffic – also apply to decoy UAS (Nichols & Sincavage, Disruptive Technologies with Applications in Airline, Marine, and Defense Industries, 2021). | Maintain OPSEC on known opponent vulnerabilities & penetration capabilities human  |
| Human & Media channels | Channels:<br>Human interpersonal interaction; individual& public                                       | True  | Reveal valid sources of classified ( but non-damaging) information to provide <i>Bona Fides</i> to double agent  | Agent channel cover stories conceal the existence of agent operations; Covert ( black) propaganda organizations & media channels hide the true source & funding of operations. |
|                        | Governing principles:<br>psychology; manipulate human trust, perception, cognition, emotion & volition |       |  |  |



|                        |       |  |  |
|------------------------|-------|--|--|
| Human & Media channels | False | False reports, feeds, papers, plans, codes, False agent channels to distract counterintelligence | Maintain OPSEC on agent operations; monitor assets to validate productivity, reliability & accuracy. |
|------------------------|-------|--|--|

---

Source: (Bennett & Waltz, 2007) pp.114 modified from Table 4.1

Table 7.5 exposes a wide variety of Channels and methods for deception. UAS can interface with much of the matrix to support active deployment logistics. Let's contemplate how UAS might be used with the deception categories. There are two main categories that UAS can be used to achieve a deception objective: CC&D sensory channels and D&D signal channels.

### **Technical Sensor Camouflage, Concealment, and Deception (CC&D)**

UAS systems sync well with the first category of manipulated channels. (Nichols R. K., Chapter 18: Cybersecurity Counter Unmanned Aircraft Systems (C-UAS) and Artificial Intelligence, 2022) Technical camouflage, concealment, and deception (CC&D) have a long history in warfare, hiding military personnel and equipment from long-range human observation within the visible spectrum. Modern CC&D includes a variety of electro-optical, infrared, and radar sensors that span the electromagnetic spectrum. (Adamy D. L., EW 104: EW against a new generation of threats, 2015) (Adamy D. L., EW 103: Tactical Battlefield Communications Electronic Warfare, 2009) (Adamy D. L., Space Electronic Warfare, 2021) From a military POV, UAS may be used to prevent detection by surveillance sensors, then to deny / or disrupt targeting by weapons systems, and ultimately to disrupt precision-guided munitions. The focus of CC&D is to use physical laws to suppress physical phenomena and observable signatures that enable remote

detection by discrimination of the target's signature from a natural background. (Bennett & Waltz, 2007)

(Bennett & Waltz, 2007) defines the elements of CC& D as:

*Camouflage* uses natural or artificial material on personnel, objects, or tactical positions to confuse, mislead, or evade the enemy. The primary phenomena suppressed by camouflage include:

- A spectral signature, which distinguishes a target by its contrast from background spectra or shadows,
- A spatial signature, which distinguishes the spatial extent, shape, and texture of the object from the natural background objects,
- Spatial location, which is relative to background context, identifies a target, and
- Movement distinguishes an object from the natural background and allows detection by moving target indicator (MTI) sensors that discriminate phase shift of reflected radar or laser energy.

*Concealment* is the protection from observation or surveillance. It can include *blending*, where parts of the scene are combined to render the parts indistinguishable. It may also include *cover* measures to protect a person, plan, operation, formation, or installation from enemy ISR and information leakage.

*Deception*: performs the function of misdirection, modifying signatures to prevent recognition of true identity or character of asset or activity and providing *spoofed (false)* or *decoy* signatures to attract the attention of sensors away from the real assets or activities.

Approaching from above at night without lights, little sound, on a waypoint navigation mode, and lethal payloads, UAS are a significant penetration element with CC&D in situ. (Nichols & Mumm, Unmanned Aircraft Systems in the Cyber Domain, 2nd Edition., 2019)

UAS plays an interesting part in sensor deception, suppression of signals of ground targets, and blending their signatures into background clutter. UAS can use active CC&D to deceive radar electro-optical sensors in the air. At sea, UAS can deceive sonar operations or inject cyber weapons into ship navigation systems to spoof location fixes. (Nichols & Sincavage, *Disruptive Technologies with Applications in Airline, Marine, and Defense Industries*, 2021) (Bennett & Waltz, 2007)

Before we detail the Signal and IS D&D relationships, we review the Cyber-Electromagnetic Activities environment. (CEA)

### **CEA**

A closely related science intersects with EW, and that is Cyber. There are distinct parallels and intersections between Cyber and EW. For instance, the sister of signal spreading techniques is encryption. Figure 7.2 shows the intersection of Cyber, EW, and Spectrum Warfare designated as Cyber Electromagnetic Activities (CEA) (Army, FM 3-38 Cyber Electromagnetic Activities, 2014). Figure 7.3 puts CEA in the perspective of total war. (Askin, 2015) Note that CEA is characterized by signal and communications. Strategic sensory deception protects large-scale, long-term, high-value national assets (e.g., WMDD programs, advanced research, and production facilities, related construction and testing activities, proliferation activities) and large-scale military activities. (Bennett & Waltz, 2007)

### **Information Operations (IO)**

There are two sides to the coin when discussing IO. and deception with UAS / UUV as the deployment mechanisms. On one side UAS have many cyber vulnerabilities that can be exploited. These are covered in detail in: (Nichols R. K., Chapter 18: Cybersecurity Counter Unmanned Aircraft Systems (C-UAS) and Artificial Intelligence, 2022). On the other side, the UAS can be considered the deployment agent for deception's broad network information

channel. Most of the methods and attack tools can exploit the network channels. Deception in IO. includes: (DoD-02, 2018)

*Communications electronic warfare (CEW)* CEW protects and attacks communication networks. Signal deception is employed to intercept, capture, and manipulate free-space communications' signal envelopes and internal contents. (Poisel, 2002)

*Computer network exploitation (CNE)*. CNE employs intelligence operations to:

- Obtain information resident in files of threat automated information systems (AIS)
- Gain information about potential vulnerabilities,
- Access critical information resident within foreign AIS that benefits friendly forces.

CNE operations employ deceit to survey, penetrate, and access targeted networks and systems. (CJCSI, 2022)

*Computer network attack (CNA)* CNA employs operations using information systems to disrupt, deny, degrade, or destroy information resident in computers and computer networks or computers and networks themselves. (USAF, January 4, 2002)

CNA also broadly covers SCADA attacks on UAS, GPS, and GNSS systems (Nichols & Mumm, Unmanned Aircraft Systems in the Cyber Domain, 2nd Edition., 2019). CNA is also used in Spoofing attacks on vessels at sea. (Humphreys & al., 2008) (Nichols & al., 2020)

In CEW, CNE, and CNA domains, deception is applied to *exploit a vulnerability* such as

- 1) Spoof an I.P. address by direct exploitation of the protocol's lack of authentication or
- 2) Exploit a buffer overflow vulnerability to insert code to enable subsequent access;

Or *induce a vulnerability* in a system to cause a network firewall misconfiguration to enable access or escalate privileged access – move from unauthorized to root access. CNA attackers use deceit on both human and computer assets. The essential elements are invading trust or destroying integrity. (Bennett & Waltz, 2007)

UAS are often used as the deployment vehicle for cyberweapons and CNA. (Nichols & al., 2020) Table 7.6 Shows the Computer network operations (CNO) deception matrix methods and terminology adopted by the Community.

**Table 7.6 Representative CNO Deceptive Operations**

| <b>Deception Matrix Quadrant</b> | <b>Deceptive Mechanism</b>           | <b>Description / Example</b>  |
|----------------------------------|--------------------------------------|---|
| Conceal facts (dissimulation)    | Cryptography                         | Openly hide A by encryption process protected by public or private key (Nichols R. K., ICOSA Guide to Cryptography, 1999)   |
|                                  | Steganography                        | Secretly hide A within open material protected by a secret hiding process and private key (Wayner, 2008)  |
|                                  | Trojan or Backdoor concealment hides | Hide C within A: conceal malicious code within a valid process; dynamically encrypt code ( polymorphic) or wrap code while not running memory to avoid a static signature detection; reduce trace logs (Skoudis, 2004). |
| Reveal fiction (simulation)      | Masquerade (decoy)                   | Present C as B to A: spoof IP address or repeating captured authentication information (Skoudis, 2004)  |
|                                  | Buffer overflow                      | Present C as B to A; spoof a service, A, to execute a code C when appearing to request B by exploiting a vulnerability in the service (Skoudis, 2004)   |
|                                  | Session Hijack                       | Capture session information/ credentials from B and present A as B (Skoudis, 2004)  |
|                                  | Session co-intercept                 | Intercept and replay security-relevant information to gain control of the session, channel, or process; co-opt a browser before a user can access it (Schneier, 1995)   |
|                                  | Man-in-the-Middle (MIM)              | Present C to B as A, then C to A as B. Establish trusted links. Control information exchange (Schneier, 1995)   |
|                                  | Honeypot / Honeynet                  | Present C as a valid service; track all users to lure, monitor users' activity without authorization (Rowe, 2004)   |

|                         |  |  |
|-------------------------|--|--|
|                         | Denial of Service (DOS)                      | Request excessive services from A, issue false requests from distributed hosts, clog the system. (R.K. Nichols & Lekkas, 2002) |
|                         | Reroute                                      | Route traffic intended for A to B: control routing information to intercept, disrupt or deny traffic requests (Skoudis, 2004). |
| Conceal fiction         | Withhold operational deception capabilities. | Maintain COMSEC, OPSEC, TRANSEC to protect CNA and CND capabilities  |
| Reveal fact (selective) | Selective disclosure and conditioning        | Publish limited network capabilities – reduce attacker sensitivity   |

Note: Table gives general descriptions of actions on computer hosts or services or servers A, B, and C. Each method has one reference. There are many in each category, and certainly updated as we march forward.

Source: Modified from Table 4.5 p 124 of (Bennett & Waltz, 2007)

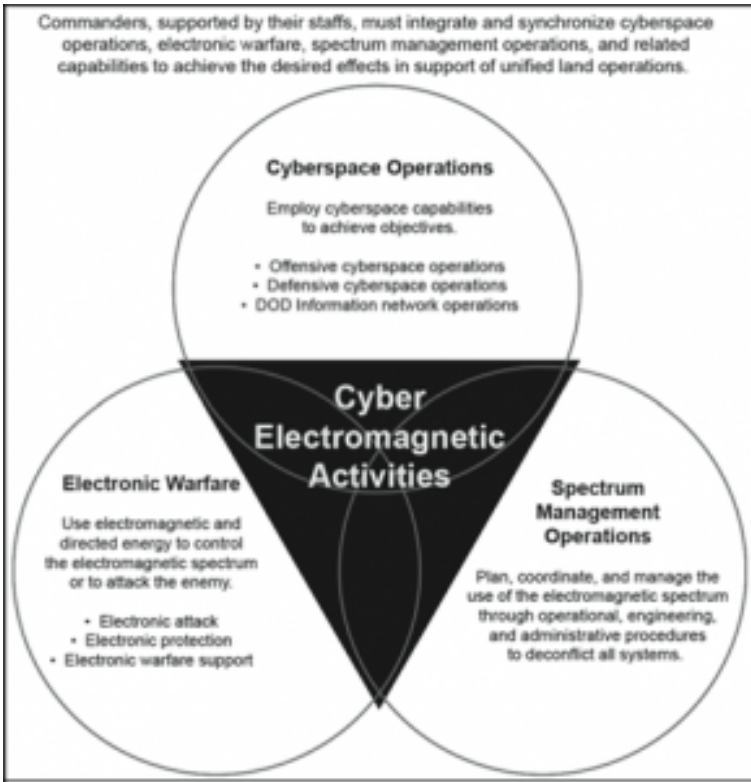
**Figure 7.2 Cyber Electromagnetic Activities**



Source: (Army, FM 3-38 *Cyber Electromagnetic Activities*, 2014)

**Figure 7.3 CEA / CEW in the view of Total War**





Source: (Askin, 2015)

Sensor deception activities in the CEW sphere are designed to D&D national technical means such as space reconnaissance and surveillance, global fixed sensor detection networks, and clandestine sensors. They thwart intelligence discovery and analysis.

### **Signal and Information Systems (IS) Denial and Deception**

UAS is exceptionally well suited to Signal and Information Denial & Deception (D&D) Operations. This category of technical methods seeks to deceive the information channel provided by electronic

systems. These methods issue deceptive signals and processes that influence automated electronic systems rather than the sensors of physical processes. (Bennett & Waltz, 2007) UAS /UUV are the new lynchpins for electronic warfare (EW) and cyberwarfare (CW) in air and sea. (Nichols & Mumm, Unmanned Aircraft Systems in the Cyber Domain, 2nd Edition., 2019) [\[10\]](#)

The second category (Table 7.5) of technical methods seeks to deceive the information channel provided by electronic systems. These methods use deceptive signals and processes that influence automated electronic systems rather than physical sensors. Deception involves the manipulation of signals and symbols to defy logic processing. (Bennett & Waltz, 2007)

### **Electronic Warfare (EW)**

The subject of E.W. is covered by one of my most revered mentors in his EW series. (Adamy D. -O., 2015) (Adamy D., 2009) (Adamy D. EW 101 A First Course in Electronic Warfare, 2001) (Adamy D. L., 2004) (Adamy D. L., EW 103: Tactical Battlefield Communications Electronic Warfare, 2009) (Adamy D. L., EW 104: EW against a new generation of threats, 2015) (Adamy D. L., Space Electronic Warfare, 2021) Our series also looks at E.W. in (Nichols & Mumm, Unmanned Aircraft Systems in the Cyber Domain, 2nd Edition., 2019) (Nichols & Ryan, 2000) (R.K. Nichols, 2020) (R.K. Nichols & Lekkas, 2002) looks into the wireless security field and its interrelationships with satellite telemetry, EW, and Cyber security.

### **EW Generalities**

**Electronic warfare (EW)** is defined as the art and science of preserving the use of the **electromagnetic spectrum (EMS)** for friendly use while denying its use by the enemy. (Adamy D., EW 101 A First Course in Electronic Warfare, 2001) The EMS is from D.C. to light and beyond.

### **Legacy EW definitions**

- EW was classically divided into (Adamy D., EW 101 A First Course in Electronic Warfare, 2001)
- ESM – Electromagnetic Support Measures – the receiving part of EW;
- ECM – Electromagnetic Countermeasures – jamming, chaff, flares used to interfere with operations of radars, military communications, and heat-seeking weapons;
- ECCM -Electronic Counter-Counter Measures – measures are taken to design or operate radars or communications systems to counter the effects of ECM.[\[11\]](#)

Not included in the EW definitions were Anti-radiation Weapons (ARW) and Directed Energy Weapons (DEW).

USA and NATO have updated these categories:

- ES – Electronic warfare Support (old ESM) to monitor the R.F. environment;
- EA – Electronic Attack – the old ECM includes ARW and D.E. weapons; to deny, disrupt, deceive, exploit, and destroy adversary electronic systems.
- EP – Electronic Protection – (old ECCM) (Adamy D., E 101 A First Course in Electronic Warfare, 2001) to guard friendly systems from hostile attack.[\[12\]](#)

ES is different from Signal Intelligence (**SIGINT**). SIGINT comprises Communications Intelligence (**COMINT**) and Electronic Intelligence (**ELINT**). All these fields involve the receiving of enemy transmissions. (Adamy D., EW 101 A First Course in Electronic Warfare, 2001)

**COMINT** receives enemy communications signals to extract intelligence.

**ELINT** uses enemy non-communications signals to determine the enemy's EMS signature so that countermeasures can be developed. ELINT systems collect substantial data over large periods to support detailed analysis.

**ES/ESM** collects enemy signals, either communication or non-communication, with the object of doing something immediately about those signals or the weapons associated with those signals. The received signals might be jammed, or the information sent to a lethal responder. Received signals can be used to type and locate the enemy's transmitter, locate enemy forces, weapons, distribution, and electronic capability. (Adamy D., EW 101 A First Course in Electronic Warfare, 2001) [\[13\]](#)

The *information channels* of EW include radar and data link systems, satellite links, navigation systems, and electro-optical (EO) systems (e.g., laser radar and EO missile seekers.) (Nichols & Mumm, Unmanned Aircraft Systems in the Cyber Domain, 2nd Edition., 2019)

**EA** methods include jamming techniques that degrade signal processing systems' detection and discrimination performance and complementary deception techniques. (Bennett & Waltz, 2007)

**Electromagnetic deception (EMD)** is defined as the deliberate radiation, re-radiation, alteration, suppression, absorption, Denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information to an enemy or enemy electromagnetic-dependent weapons, thereby degrading or neutralizing the enemy's combat capability. (Army, Joint Doctrine for Electronic Warfare – Joint Pub 3-51, April 7, 2000) These deceptive actions include exploiting processing vulnerabilities, inserting too many signatures in the detection buffer, and spoofing. Table 7.7 present a taxonomy of EMD techniques within the format

of the deception matrix. (Adamy D., EW 101: A First Course in Electronic Warfare, 2001) (Adamy D. L., EW 104: EW against a new generation of threats, 2015)

## **Spoofing – GPS Spoofing**

**Spoofing – A Cyber-weapon attack that generates false signals to replace valid ones. GPS Spoofing is an attack to provide false information to GPS receivers by broadcasting counterfeit signals similar to the original GPS signal or by recording the original GPS signal captured somewhere else at some other time and then retransmitting the signal. The Spoofing attack causes GPS receivers to provide the wrong information about position and time. (T.E. Humphrees, 2008) (Tippenhauer & et.al, 2011)**

### **Spoofing Techniques**

According to (Haider & Khalid, 2016), there are three common GPS Spoofing techniques with different sophistication levels. They are simplistic, intermediate, and sophisticated. (Humphreys & al., 2008)

The *simplistic spoofing attack* is the most commonly used technique to spoof GPS receivers. It only requires a COTS GPS signal simulator, amplifier, and antenna to broadcast signals towards the GPS receiver. It was performed successfully by Los Alamos National Laboratory in 2002. (Warner & Johnson, 2002) Simplistic spoofing attacks can be expensive as the GPS simulator can run \$400K and is heavy (not mobile). The available GPS signal does not synchronize simulator signals, and detection is easy.

In the *intermediate spoofing attack*, the spoofing component consists of a GPS receiver to receive a genuine GPS signal and a spoofing device to transmit a fake GPS signal. The idea is to estimate the target receiver antenna position and velocity and then broadcast a fake signal relative to the genuine GPS signal. This type of spoofing attack is difficult to detect and can be partially prevented by using an IMU. (Humphreys & al., 2008)

In sophisticated spoofing attacks, multiple receiver-spoofers

devices target the GPS receiver from different angles and directions. The angle-of-attack defense against GPS spoofing in which the angle of reception is monitored to detect spoofing fails in this scenario. The only known defense successful against such an attack is cryptographic authentication. (Humphreys & al., 2008) [14]

Note that prior research on spoofing was to *exclude* the fake signals and focus on a single satellite. ECD ( next section) *includes* the fake signal on a minimum of four satellites and then progressively / selectively eliminates their effect until the real *weaker* GPS signals become apparent. (Eichelberger, 2019)

### **EICHELBERGER'S CD - COLLECTIVE DETECTION MAXIMUM LIKELIHOOD LOCALIZATION APPROACH (ECD)**

Returning to the spoofing attack discussion, Dr. Manuel Eichelberger's CD - *Collective detection maximum likelihood localization approach*, his method not only can *detect* spoofing attacks but also *mitigate* them! The ECD approach is a robust algorithm to mitigate spoofing. ECD can differentiate closer differences between the correct and spoofed locations than previously known approaches. (Eichelberger, 2019) COTS has little spoofing integrated defenses. Military receivers use symmetrically encrypted GPS signals, subject to a "replay" attack with a small delay to confuse receivers.

ECD solves even the toughest type of GPS spoofing attack, consisting of spoofed signals with power levels similar to the authentic signals. (Eichelberger, 2019) ECD achieves median errors under 19 m on the TEXBAT dataset, the de-facto reference dataset for testing GPS anti-spoofing algorithms. (Ranganathan & al., 2016) (Wesson, 2014) The ECD approach uses only a few milliseconds worth of raw GPS signals, so-called snapshots, for each location fix. This enables offloading of the computation into the Cloud, allowing knowledge of observed attacks.[1] Existing spoofing mitigation methods require a constant stream of GPS signals and tracking those signals over time. Computational load increases because fake

signals must be detected, removed, or bypassed. (Eichelberger, 2019)

**Table 7.7 Standard Taxonomy of Representative  
Electromagnetic (EM) Deception Techniques**

| Deception Matrix Quadrant     | Electromagnetic Deception Categories  | EW Deception Techniques   |
|-------------------------------|---|---|
| Conceal Facts (dissimulation) | Type 1 manipulative EM deception: eliminate revealing, EM telltale indicators that hostile forces may use radar | <p>Radar Cross Section (RCS) suppression by low observable methods: radar absorption materials or radar energy redirection to reduce effective RCS</p> <p>Conceal signals within wideband spread-spectrum signals (sequence, frequency hopping)</p> <p>Radar chaff and cover jamming to reduce signal quality and mask the target's signature</p> |
|                               | Imitative EM deception: introduces EM energy into enemy systems imitates enemy emissions                        | Radar signature, IFF [15] spoofing; store, repeat, or imitate RCS, power signatures, or IFF codes to appear as the enemy system signals,  |
| Reveal fiction (simulation)   | Type 2 manipulative EM deception: convey misleading EM telltale indicators that hostiles may use deceptive      | <p>Deceptive jamming to induce error signals within receiver-processor logic or range estimation errors</p> <p>Navigation beaconing: intercept and rebroadcast beacon signals on the same frequency to cause inaccurate bearings and navigation solutions</p>   |
|                               | Simulative EM deception: simulate friendly or actual capabilities to mislead hostile forces                     | Saturation and Seduction decoys to misdirect, overload signal generators, or cause fire control to break the lock on the intended targets conceal   |
| Conceal fiction               | Withhold deception capabilities until the surprise project  | Protect electronic deception emissions and modes—husband assets.  |
| Reveal facts                  | Surveillance conditioning display   | Display signatures and selected capabilities to desensitize radar/overwatch surveillance  |



Sources: (Adamy D. L., EW 104: EW against a new generation of threats, 2015) (Army, Joint Doctrine for Electronic Warfare – Joint Pub 3-51, April 7, 2000) (Bennett & Waltz, 2007)

## **Signals Intelligence (SIGINT)**

Deception techniques are also employed with SIGINT agents/community. SIGINT employs deceptive methods to intercept, collect, and analyze external and communications intelligence (COMINT). Cryptanalytic deception methods to gain keying information or disrupt or bypass encrypted channels.[\[16\]](#) (Nichols R. K., Chapter 18: Cybersecurity Counter Unmanned Aircraft Systems (C-UAS) and Artificial Intelligence, 2022) (Nichols R. K., ICSA Guide to Cryptography, 1999) (Schneier, 1995) (Army, FM 3-38 Cyber Electromagnetic Activities, 2014) (Bennett & Waltz, 2007) To wit:

*Ciphertext replay:* Unencrypted ciphertext is recorded, modified, and replayed with a valid key interval to disrupt the target system.

*Key spoofing:* Impersonates key distribution server and issues false keys to target, then decrypts traffic issued under the false key.

*Man-in-the-Middle (MIM)* Secure a trusted position between two parties and issue spoofed keys to both. Then intercepts all traffic and can change at will.

The above methods may be used to intercept/disrupt hostile communication by inserting false/misleading transmissions to deceive or reduce the integrity of communication channels. (Bennett & Waltz, 2007)

## **CONCLUSIONS**

Deception planning requires careful application of multiple methods across channels to limit a target's ability to compare multiple sources for conflicts, ambiguities, uncertainties, or feedback cues to simulated or hidden information. (Bennett & Waltz, 2007) UASs are reasonable agents to deliver deceitful payloads

against CBNE targets, assets, and critical national infrastructure. (DHS, 2018)

## **Bibliography**

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

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

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

Adamy, D. L. (2015). *EW 104: EW against a new generation of threats*. Norwood, MA: Artech House.

Adamy, D. L. (2021). *Space Electronic Warfare*. Norwood, MA: Artech House.

Army, U. (2014). *FM 3-38 Cyber Electromagnetic Activities*. Washington: DoD.

Army, U. (April 7, 2000). *Joint Doctrine for Electronic Warfare – Joint Pub 3-51*. Washington: DoD.

Askin, O. I. (2015). Cyberwarfare and electronic warfare integration in the operational environment of the future: cyber, electronic warfare. . *Cyber Sensing 2015* (14 May 2015) (pp. Proceedings Vol 9458, Cyber Sensing 2015; 94580H (2015) SPIE Defense + Security, 20). Washington: Askin, O., Irmak, R, and Avseyer, M. (14 May 2015) Cyber warfare and electronic war 94580H (2015) SPIE Defense + Security, 20.

Bade, H. S. (2009). *Analysis\_of\_Crowd\_Behaviour\_Theories\_in\_Panic\_Situation*. Retrieved from <https://www.researchgate.net/publication/>

224099630 - Intern. Conf. on Information and Multimedia Technology: [https://www.researchgate.net/publication/224099630\\_Analysis\\_of\\_Crowd\\_Behaviour\\_Theories\\_in\\_Panic\\_Situation](https://www.researchgate.net/publication/224099630_Analysis_of_Crowd_Behaviour_Theories_in_Panic_Situation)

Bennett, M., & Waltz, a. E. (2007). *Counter Deception: Principles and Applications for National Security*. Norwood, MA: Artech House.

CBS News. (2021 updated, October 24). *the-station-nightclub-fire-rhode-island-what-happened-and-whos-to-blame/*. Retrieved from <https://www.cbsnews.com/news/>: <https://www.cbsnews.com/news/the-station-nightclub-fire-rhode-island-what-happened-and-whos-to-blame/>

Chrockett, Z. (2014, June 16). *deadliest-soccer-disasters*. Retrieved from <https://priceonomics.com/>: <https://priceonomics.com/historys-deadliest-soccer-disasters/>

CJCSI. (2022). CJCSI 3210.01A -Ref f. Washington: USDOJ.

Daniel, D., & Herbig, a. K. (1982). Propositions on Military Deception. In J. Gooch, & a. A. (eds), *Military Deception and Strategic Surprise* (pp. pp. 155-156). Totowa, NJ: Frank Cass & Co.

Dewar, M. (1989). *The Art of Deception in Warfare*. Devon, UK: David & Charles Pub.

DHS. (2018, May 22). *Cybersecurity Risks Posed by Unmanned Aircraft Systems*. Retrieved from <https://www.eisac.com/>: <https://www.eisac.com/cartella/Asset/00007102/OCIA%20-%20Cybersecurity%20Risks%20Posed%20by%20Unmanned%20Aircraft%20Systems.pdf?parent=115994>

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](http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf)

Dorn, T. (2021). *Unmanned Systems: Savior or Threat*. Conneaut Lake, PA: Page Publishing.

Eichelberger, M. (2019). *Robust Global Localization using GPS and Aircraft Signals*. Zurich, Switzerland: Free Space Publishing, DISS. ETH No 26089.

EnergyJustice.net. (2022, February 10). *Nuclear Operating Plants*

in the US. Retrieved from <http://www.energyjustice.net/map/>:  
<http://www.energyjustice.net/map/nuclearoperating>

Gerwehr, S., & Glenn, a. R. (2002). *Unweaving the Web: Deception and Adaptation in Future Urban Operations*. Santa Monica, CA: RAND.

Haider, Z., & Khalid, & S. (2016). Survey of Effective GPS Spoofing Countermeasures. *6th Intern. Ann Conf on Innovative Computing Technology (INTECH 2016)* (pp. 573-577). IEEE 978-1-5090-3/16.

Haswell, J. (1985). *The Tangled Web: The Art of Tactical and Strategic Deception*. Buckinghamshire, UK: John Goodchild Pub.

Humphreys, T., & al., e. (2008). Assessing the spoofing threat: Development of a portable GPS civilian spoofer. In *Radionavigation Laboratory Conf. Proc.*

Kallenborn, Z., & Bleck, a. P. (2018). Swarming destruction: drone swarms and chemical, biological, radiological, and nuclear weapons. *The nonproliferation review*, pp. Vol 25, Issue 5-6, pp. 523-543.

Latimer, J. (2001). *Deception in War: The Art of the Bluff, the Value of Deceit, and the most thrilling Episodes of Cunning in Military History, from the Trojan War to the Gulf War*. Woodstock, NY: Overlook Press.

MathTech, Inc. (1980). *Deception Maxims: Fact and Folklore*. Princeton, NJ: Everest Consulting Associates and MathTech, Inc.

Mitchell, R. W. (1986, p358). In *Epilogue: Deception Perspectives on Human and Nonhuman Deceit*. Albany, NY: State University of New York Press.

Nichols, R. K. (1999). *ICSA Guide to Cryptography*. New York City: McGraw Hill.

Nichols, R. K. (2018, March 27). *short-circuiting-simple-panic-attacks-quick-guide-out*. Retrieved from <https://www.linkedin.com/pulse/>: <https://www.linkedin.com/pulse/short-circuiting-simple-panic-attacks-quick-guide-out-nichols-dtm/>

Nichols, R. K. (2020). *Counter Unmanned Aircraft Systems Technologies & Operations*. Manhattan, KS: [www.newprairiepress.org/ebooks/31](http://www.newprairiepress.org/ebooks/31).

Nichols, R. K. (2022). Chapter 18: Cybersecurity Counter Unmanned Aircraft Systems (C-UAS) and Artificial Intelligence. In D. M. R. K. Barnhart, *Introduction to Unmanned Aircraft Systems*, 3rd Edition (pp. 399-440). Boca Raton, FL: CRC.

Nichols, R. K., & Mumm, H. C. (2019). *Unmanned Aircraft Systems in the Cyber Domain*, 2nd Edition. Manhattan, KS: [www.newprairiepress.org/ebooks/27](http://www.newprairiepress.org/ebooks/27).

Nichols, R. K., & Sincavage, S. M. (2021). *Disruptive Technologies with Applications in Airline, Marine, and Defense Industries*. Manhattan, KS: New Prairie Press #38.

Nichols, R., & al., e. (2020). *Unmanned Vehicle Systems and Operations on Air, Sea, and Land*. Manhattan, KS: New Prairie Press #35.

Nichols, R., & Ryan, D. &. (2000). *Defending Your Digital Assets Against Hackers, Crackers, Spies and Thieves* San Francisco: McGraw Hill, RSA Press.

Poisel, R. (2002). *Introduction to Communications Electronic Warfare Systems*. Norwood, MA: Artech House.

R.K. Nichols & Lekkas, P. (2002). *Wireless Security; Threats, Models & Solutions*. NYC: McGraw Hill.

R.K. Nichols, e. a. (2020). *Unmanned Vehicle Systems & Operations on Air, Sea & Land*. Manhattan, KS: New Prairie Press #35.

R. K. Nichols, & et al. (2022). DRONE DELIVERY OF CBNRECy – DEW WEAPONS, *Emerging Threats of Mini-Weapons of Mass Destruction and Disruption (WMDD)*. Manhattan, KS: New Prairie Press #TBA.

Ranganathan, A., & al., e. (2016). SPREE: A Spoofing Resistant GPS Receiver. *Proc. of the 22nd ann Inter Conf. on Mobile Computing and Networking*, ACM, pp. 348-360.

Rowe, N. C. (2004). Honeynet Project- Research on Deception in Defense Information Systems. *Proc DoD Command and Control Research Program Conf*. San Diego, CA: DoD.

Schneier, B. (1995). *Applied Cryptography: Protocols, Algorithms and Source Code in C*. New York John Wiley & Sons.

Skoudis, E. (2004). *Malware: Fighting Malicious Code*. Upper Saddle River, NJ: Prentice-Hall.

T.E. Humphries, e. (2008). Assessing the Spoofing Threat: Development of a portable GPS Spoofing Civilian Spoofer. ION (pp. Sept 16-19). Savana, GA: ION.

Tippenhauer, N., & et.al. (2011). On the requirements for successful spoofing attacks. *Proc. of the 18th ACM Conf. on Computing and communications security (CCS)*, 75-86.

USAF. (January 4, 2002). *Air Force Doctrine Document AFDD 2-5, Information Operations*. Washington: USAF.

Warner, J., & Johnson, & R. (2002). A Simple Demonstration that the system (GPS) is vulnerable to spoofing. *J. of Security Administration*. Retrieved from <https://the-eye.eu/public/Books/Electronic%20Archive/GPS-Spoofing-2002-2003.pdf>

Wayner, P. (2008). *Disappearing Cryptography: Information Hiding: Steganography and Watermarking*, 3rd ed. Baltimore: Morgan Kaufmann.

Wesson, K. (2014, May). *Secure Navigation and Timing without Local Storage of Secret Keys*. Ph.D. Thesis.

## Endnotes

[1] This chapter does not discuss counter-deception strategies and methods. It would require a book by itself. But be aware that there are counter-deception strategies employed by military and LEO forces globally for any deception technique or technology.

[2] This is the 2nd D in WMDD.

[3] In our introductory example. The penalty is death or trampling,

[4] There are fascinating reconstructions and images of the crowds panicking – trying to get out and only one long passageway to funnel the hundreds escaping.

[5] On May 9, 2001, Ghana's two most prominent teams — Accra Hearts and Asante Kotoko — came together for a match at Accra Sports Stadium that would become the deadliest sporting disaster in African history.

Due to the heated nature of the rivalry, extra security had been ordered, and trouble had been anticipated. When the match ended in a 2-1 Accra Hearts victory, the match lived up to its expectations: angry Kotoko fans began ripping plastic chairs out of the ground and hurling them onto the pitch. As with the Estadio Nacional Disaster, police responded by launching tear gas and firing plastic bullets into the crowd — not just at those guilty of hooliganism, but at everyone present. A massive stampede of 40,000 fans rushed to exit the stadium, resulting in packed corridors; by the time the masses had cleared, 127 lay dead, most from compressive asphyxiation.

[6] The introductory ballpark example exploits disinformation.

[7] These concepts are important to the use of UAS in deception operations.

[8] Think F.B., Instagram, and every social media outlet.

[9] One doesn't have to look far in today's society to see the bandwagon effects of pushing an agenda and having government, big tech, and the majority of news outlets harping on anyone's deception. Truth shines the light on all situations but usually is found out too late.

[10] EW and IO. are covered in detail in Chapter 14 (Nichols & Mumm, Unmanned Aircraft Systems in the Cyber Domain, 2nd Edition., 2019). Cyber operations are covered in detail in (Nichols R. K., Chapter 18: Cybersecurity Counter Unmanned Aircraft Systems (C-UAS) and Artificial Intelligence, 2022), and Maritime security involving Cyber is discussed vigorously in (Nichols & Sincavage, Disruptive Technologies with Applications in Airline, Marine, and Defense Industries, 2021)

[11] ECCM was considered T.S. classified with most secret protocols and design algorithms. TS = Top Secret

[12] EW, E.S., E.P., E.A. definitions were adjusted via (Bennett & Waltz, 2007) to be consistent with our UAS weapons deployment theme.

[13] Adamy (2001) is correct when he suggests that the “key to understanding EW principles (particularly the R.F.) part is to understand radio propagation theory. Understanding propagation leads logically to understanding how they are intercepted, jammed or protected.” (Adamy D., 2001)

[14] (Nichols & al., 2020) have argued the case for cryptographic authentication on civilian UAS /UUV and expanded the INFOSEC requirements.

[15] IFF = Identify Friend or Foe challenge system

[16] Multiple sources pose this solution.



PART II

# SECTION 2: DIRECTED ENERGY WEAPONS (DEW) AND PAYLOADS



# 8. DEW Primer

**By Professor Randall K. Nichols, Kansas State University**

## **Student Objectives**

- To study the basic principles for Directed Energy Weapons (DEW)
- To recognize that DEWs can be launched from ground or air against CBRN assets or UAS / UAV
- To understand energy propagation and interaction are key elements in the analysis of weapons utility,
- To understand the common framework for DEW analysis, which is mostly insensitive to the weapon type,
- To look at how a DEW deposits energy in a target and then considers energy deposition and loss rates to determine the criteria for damaging the target.

## **INTRODUCTION**[\[1\]](#)

This chapter is about the *effects* of directed energy weapons (DEW). We are interested in how they propagate to and interact with targets. *Propagation and target interaction* are the key elements in analyzing a weapon's utility to accomplish a given mission. The yield of its warhead determines the effectiveness of a nuclear missile and the accuracy of its guidance. The effectiveness of a rifle is determined by the type of round fired, the range to target, and the skill of the shooter who fires it. DEW weapons are no different. (Nielsen, 2012)[\[2\]](#)

In this textbook, the authors recognize that unmanned aircraft or

underwater vehicles (UAS / UUV) are capable deployment agents for weapons (DEW included) – especially against CBRN assets and facilities or hostile airborne or underwater assets. (Nichols & Sincavage, 2021) This chapter is a primer on DEW effects. It sets the stage for the next five chapters in our book: Chapter 9: Kinetic Energy Weapons, Chapter 10: Lasers, Chapter 11: Microwaves, Chapter 12: Hypersonic Drones, and Chapter 13: Acoustic Weapons and Piracy. Chapters 14: Satellite Killers and Chapter 15: Cyber Weapons and CBRNE are special cases.

Weapons are devices that **deliver sufficient energy** to targets to **damage them**. Effective design requires a knowledge of the weapons and their characteristics. (Nielsen, 2012) Designers create the means of projecting energy onto the targets that planners choose to destroy. Weaponry is not a precise science. Propagation paths and target details are never known precisely. Using a 22 caliber against a bear might penetrate the skin (precisely) until you find a beer-bellied bear with thick full skin sitting around his cave watching TV to wait out the winter. This operational scenario might invalidate the precise calculations by the designer for weapon energy propagation.

## COMMON FRAMEWORK

*Weapons may be understood as devices that deposit energy on targets. The energy that must be deposited to achieve a given level of damage is relatively insensitive to the type of weapon employed. Nuclear weapons may be characterized in terms of megatons, bullets in terms of muzzle velocity, and particle beams in terms of amperes of current. Still, when reduced to common units for the energy absorbed by the target, similar levels of damage are achieved at similar levels of energy deposited.* (Nielsen, 2012)

## EFFECTS OF DIRECTED ENERGY WEAPONS (DEW)

Directed energy weapons make up various weapons such as lasers, particle beams, microwaves, and even bullets. All DEW are just devices that deposit energy in targets. That energy that must be deposited to achieve a given level of damage is relatively insensitive to the type of weapon employed. (Nielsen, 2012)<sup>[3]</sup> American DE weapons may change the way future wars will be fought. (Beason, 2005)

Energy cannot be deposited in a target unless it is *first delivered* to the target. This delivery mechanism is called the *propagation* of energy. This subject was covered in (Adamy D. 2001) (Adamy D., 2009) and (Nichols et al., 2019). There is always some loss of energy during propagation. The DEW must *deliver more energy than needed to damage the target to compensate for the loss along the way*. DE weapon design depends on the anticipated target, determining the energy required for damage. Second, the anticipated scenario (range, environment, time, etc. See Table 8.1) determines how much energy must be produced to ensure that adequate energy is delivered in the time available. (Nielsen, 2012)

### **Table 8.1 Battlespace Dimensions**

| Dimension | Function                   | Action                     |
|-----------|----------------------------|----------------------------|
| Latitude  | Friendly Force Location    | Direction of Weapons       |
| Longitude | Enemy Force Location       | Maneuver of Forces         |
| Elevation |                            |                            |
| Time      | Speed of Maneuver          | Timeliness of Attack       |
|           | Timing of Weapon Release   | Enemy Vulnerability        |
| Frequency | Bandwidth Required         | Rate of Information Flow   |
|           | Bandwidth Available        | Interference               |
|           | Frequency of Transmissions | Vulnerability to Jamming   |
|           |                            | Vulnerability to Intercept |

Source: (Adamy D. -0., 2015)

### THE BELOVED BTU GIVES WAY TO JOULES

Weapons designers favor metric units, where length is in meters, mass in kilograms, and time in seconds. Energy is expressed in Joules. A Joule is approximately the energy required to lift a quart of milk a distance of three feet, or 1/50000 (2 x 10<sup>-5</sup>) of the energy it takes to brew a cup of coffee. [\[4\]](#) [\[5\]](#)

### ENERGY REQUIRED FOR DAMAGE

Damage may be defined as *soft* damage. For example, attacking a UAS in the air might upset the UAS computers compared to *hard* damage meaning the complete vaporization of the UAS in the air.

The former is sensitive to the details of the attack, the hardness of chips, the computer(s) details, communications, circuits, and sub-circuits. Vaporization produces immediate feedback as to the target status – catastrophic. Two things must be known in determining how much energy a weapon must produce to damage a target. *How much energy it takes to damage the target and what fraction of the energy generated will be lost in propagating it.* (Nielsen, 2012)

## ICE CUBE

Consider the energy required (damage level) to vaporize an ice cube. [6] Pull an ice cube from the refrigerator. If its temperature is below the temperature, it will melt. First, we must raise the temperature to melt temperature. The energy required is proportional to both the necessary  $\Delta T$  rise and the amount of ice in the cube. From thermodynamics, the expression (specific heat calculation) covering this is:  $E = m \times C (T_m - T_i)$ , where  $E$  is the energy required in Joules,  $m$  = mass of ice cube in grams,  $T_i$  = the initial temperature in Celsius,  $T_m$  = melting temperature,  $C$  is the heat capacity constant of proportionality ( $J/gm \times ^\circ C$ ). For this example,  $C = 4.2 (J/gm \times ^\circ C)$  and ice cube = 50 gm,  $T_i = -10 (^\circ C)$ ,  $T_m = 0 (^\circ C)$ . ( $L_m$  for water = 334 Joules / gm. So, 16,700 additional Joules are necessary to melt the ice cube of 50gm.  $T_v$  = vaporization temperature, ( $100 ^\circ C$ ) So,  $E = 2,100$  Joules of energy required to raise it to the melting point. This energy is not enough. We must melt the ice cube. The heat of fusion ( $L_m$ ) is the energy required to convert 1 gm of solid to 1 gm of liquid. With an additional 16,700 Joules, we now have a small water puddle. But our object is to vaporize the ice cube – *hard* damage. Using the specific heat equation again,  $E = m \times C (T_v - T_m)$ , we require an additional 21,000 Joules to raise the ice cube as molten water to vapor at the same temperature by supplying the heat of vaporization,  $L_v = 2,440$  Joules per gm of water. This means an additional 122,000 Joules of energy are required. The total energy needed to vaporize an ice cube of 50 gm is 161,000

Joules. Lv accounts for about 75% of the required energy. One little ice cube. In BTUs, this is only 152.7 BTUs.[\[7\]](#) [\[8\]](#)

10,000 JOULES

(Nielsen, 2012) gives a table of thermal properties of Aluminum, Copper, Magnesium, Iron, and Titanium. It shows that most solid materials (See Table 8.2) have a density on the order of 1 – 10 gm /cubic centimeter and that **10,000 Joules is sufficient energy to vaporize about one cubic centimeter of anything!** 10,000 Joules is a magic number because it is close to the energy delivered by a wide range of DEWs. (Nielsen, 2012) A typical rifle round has about 10 gm and is fired at a muzzle velocity of 1000 m/s. (Halsam, 1982) This corresponds to kinetic energy (KE) of  $(mv^2 / 2)$  of 5,000 Joules. A roman Catapult could throw a 20 Kg stone over 200 meters. The KE required for this use is about 40,000 Joules. (Foley, March 1979) A medieval crossbow could launch an 85-gm bolt over 275 meters. This required 13,000 Joules. (Vernard Foley, January 1985)

Table 8.2 Thermal Properties of Common Materials

| Material  | Density<br>Gm/<br>cm3 | Melting<br>Point,<br>Tm<br>oC | Vaporization<br>Point, Tv<br>oC | Heat<br>Capacity<br>(J/<br>gm0C) | Heat<br>of<br>Fusion<br>(J/gm) | Heat of<br>Vaporization<br>(J/gm) |
|-----------|-----------------------|-------------------------------|---------------------------------|----------------------------------|--------------------------------|-----------------------------------|
| Aluminum  | 2.7                   | 660                           | 2500                            | 0.9                              | 400                            | 1100                              |
| Copper    | 8.96                  | 1100                          | 2600                            | 0.38                             | 210                            | 4700                              |
| Magnesium | 1.74                  | 650                           | 1100                            | 1.0                              | 370                            | 5300                              |
| Iron      | 7.9                   | 1500                          | 3000                            | 0.46                             | 250                            | 6300                              |
| Titanium  | 4.5                   | 1700                          | 3700                            | 0.52                             | 320                            | 8800                              |

Source: Table 1-1 (Nielsen, 2012)

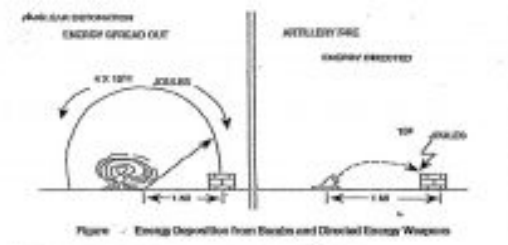


## ENERGY ALONE SUFFICIENT FOR HARD DAMAGE?

In a nutshell, no. A nuclear bomb releases a lot of energy. One Kiloton yields 4,000,000,000,000

Joules. Well above the 10,000 Joule criterion, but at a distance of less than a mile from detonation, a concrete structure is undamaged. Over the same range, an artillery shell with only 10,000 Joules of energy could easily destroy such a structure. Also, consider the sun. It delivers about 5,000 Joules of energy over every square centimeter of the earth's surface, yet we see no cars melting or people fried. *The energy must be delivered over a small region and in a short time to the target. Energy is not the silver bullet for damage.* We must also consider the density of energy on the target (Joules per square centimeter),<sup>[9]</sup> the rate of energy delivery, or power (Joules/ sec or Watts). The nuclear bomb is not a DE weapon like the artillery shell. Much of the energy released does not intersect with the concrete structure and is “wasted.” The artillery shell is a DE and concentrates its energy on the target in question. Suppose we spread the bomb's energy over a sphere's surface at a range of one mile. In that case, the energy density is only 13 Joules per square centimeter, far less than the DE artillery shell density of 10,000 Joules per square centimeter. The nuclear bomb is consistent with other weapon types, with the Spreading of blast energy accounted for. (Nielsen, 2012)<sup>[10]</sup> See Figure 8.1.

**Figure 8.1 Energy Deposition from Bombs and DEW**



Source: Adapted from Figure 1-2 in (Nielsen, 2012)

## ENERGY DELIVERY RATE

If energy is delivered over too long a period, it is not effective in damaging the intended target. The target can shed energy as rapidly as it is deposited. Cars in a parking lot heat up in the sun (unfortunately fatal to youngsters or animals left in the car) until they become so hot that they radiate energy away as rapidly as it's deposited, so they don't heat up to the point of sustained damage. After that, they heat up to a constant temperature. If energy is delivered more rapidly than the target can handle, the damage will *ensue*. (Nielsen, 2012)

From thermodynamics, we know that energy can be transferred away (lost in propagation) from a target by thermal conduction, convection, and radiation.

## THERMAL CONDUCTION

Thermal conduction losses (energy flow or “downhill” temperature gradient (slope of the curve of temperature v distance) from hot regions to cold regions, moving the temperature to equilibrium in the system). The steeper the slope, the faster the energy will flow. The equation for thermal conduction is

$$U = -k( dT / dx)$$

**Equation 8.1**

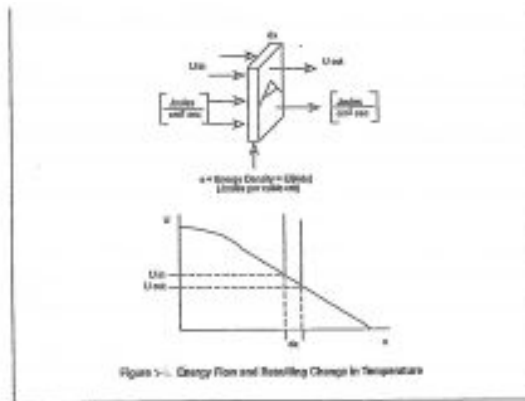
Where  $U$  = rate of flow of energy across a surface, J/cm<sup>2</sup> sec  
 $dT / dx$  = the slope (derivative of Temperature / distance) of the temperature curve,

degrees / cm

$k$  = constant of proportionality called thermal conductivity[11] in J/ sec cm deg

The thermal conductivity can vary greatly from one material to another. As a result of the energy flow  $U$ , the temperature  $T$  in different target regions will change. See Figure 8.2.

**Figure 8.2 Energy Flow and Resulting Change in Temperature**



Source: Adapted from Figure 1-4 (Nielsen, 2012)

Energy flows until the temperature is the same everywhere in the system, called equilibrium. Figure 8.2 shows how knowing  $U$  throughout a target can calculate the rate of temperature change within it. (Nielsen, 2012) Figure 8.2 shows a thin region within the target having cross-section  $A$  and a thickness of  $dx$ . There is a flow of energy (Joules /square centimeter per second) into the region,  $U_{in}$ , and flow out of the region, denoted  $U_{out}$ . If these two quantities are not equal, then the amount of energy within the region will increase or decrease ( will change), and the temperature will rise or fall ( it will also change). In Figure 8.2, the flow out is less than the flow in, which means the temperature will increase. The rate of change in temperature is found using the thermal diffusion equation 8.2 (Nielsen, 2012)

$$\frac{dT}{dt} = \left( \frac{k}{C\rho} \right) \left( \frac{d^2T}{dx^2} \right) \quad \text{Equation 8.2}$$

where:  $(U_{in} - U_{out})$  is the energy flow into and out of the region  
 $dT / dx$  is the change in temperature gradient across the region  
 $C$  the heat capacity

$k$  = thermal conductivity

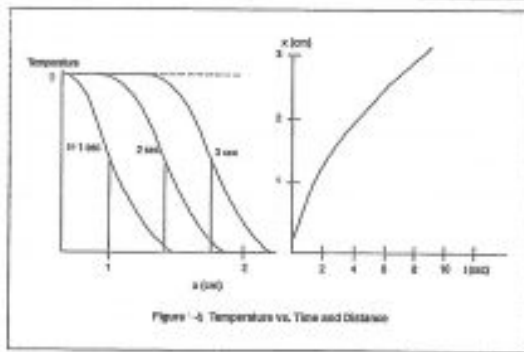
$\rho$  = density of target material (gm/cm<sup>3</sup>)

$k/C_p$  = thermal diffusivity =  $D$  [12]

### CONSTANT SURFACE TEMPERATURE CASE

Although the diffusion equation is second order and usually requires a computer to assist in solutions, there is one special case of interest in studying DEW effects. Figure 8.3 shows how the temperature on the interior of a solid varies with time if the surface is maintained at a constant temperature. (Nielsen, 2012)

**Figure 8.3 Special Case: Constant Surface Temperature**



Source: Adapted from Figure 1-5 (Nielsen, 2012)

The heated region propagates into the target on the left side of the figure, eventually being heated to a temperature of  $T$ . The

distance to the target to which the heat is propagated is plotted as a function of time on the right side. The distance obeys a simple law:

$$x \sim \sqrt{Dt}$$

**Equation 8.3**

$k/C\rho$  = thermal diffusivity =  $D$

$t$  = time

$x$  = distance

$C$  the heat capacity

$k$  = thermal conductivity

$\rho$  = density of target material (gm/cm<sup>3</sup>)

The distance to the target is approximately equal to the square root of the Diffusivity times the elapsed time. This equation is used in developing criteria for target damage from different weapon concepts (laser, microwave, and particle beams). (Nielsen, 2012)

## CONVECTION

Thermal conduction arises because of the random motion of molecules. Hot molecules give up energy by motion; cold molecules warm up by gaining energy. The movement of both types of molecules is always towards equilibrium  $T$ .

Convection (heat loss by the macroscopic motion of molecules). Think of an attic fan moving hot air out of the attic, where the fan blades induce motion. The macroscopic flow of air induced by the fan can carry away hot air from the attic and lower the temperature more efficiently than conduction. Convection is an important source of energy loss. Many targets, such as airplanes, drones, boats, or UAVs, can move rapidly through the air. (See Figure 8.4) The wind of motion (think sailboat or airplane) across the surface of the target is an important factor in establishing the damage threshold. Weapons like lasers deposit energy primarily

on the surface of the target. Hot air rises and is lighter than cold air. The process of heating a region itself can set air into motion, affecting the threshold and extent of the damage. (Nielsen, 2012)

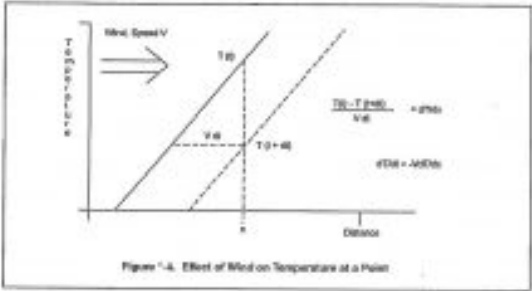
The expression for wind induced convection for temperature v distance:

$$dT / dt = - V dT/ dx$$

Equation 8.4

Where V = wind velocity  
T = temperature in time at point x  
dT /dx is the rate of change of temperature in time at point x

Figure 8.4 Effect of Wind v Temperature



Source: Adapted from Figure 1-6 (Nielsen, 2012)

**WIND vs. TEMPERATURE CONVECTION HEAT**

Figure 8.4 shows how convection heat is handled.  $dT / dx$  is a region of space in which the temperature gradient varies with distance. Wind of velocity  $V$  and time  $dt$  blows the temperature profile downstream to the point indicated by the dotted line. The temperature at point  $x$  drops in time  $dt$  from  $T$  to  $T - V (dT / dx) dt$ . The gradient or rate of change of  $T$  in time at point  $x$  is  $dT / dt = - V dT / dx$ . This expression for the effect of wind on the temperature at a point is clever. If the wind velocity  $V$  is stronger, the temperature drops more rapidly, and if the temperature is the same everywhere, the gradient  $dT / dx$  is zero. The wind serves only to replace hot air with more hot air temperature stays the same. (Nielsen, 2012)

### **VACUUM BLACK BODY RADIATION**

To lose energy by conduction or convection, a target must be immersed in the atmosphere, water, or some fluid medium to supply the necessary molecules to carry the energy away. (Adamy D. L., 2004) Targets in a vacuum of outer space can lose energy through *radiation*.

Molecule movement is not just random; they vibrate, rotate, and incorporate energy in their internal structure. The energy that temperature represents resides in internal degrees of freedom. Molecules can give up internal energy by emitting electromagnetic radiation such as light, radio waves, and microwaves.

Black Body radiation can occur in space or a vacuum. Black Body radiation is an ideal mathematical surface that absorbs all radiation incident. In equilibrium, it would radiate more energy than any other object. (Nielsen, 2012)

The total *Intensity* of radiation emerging from the surface of a Black Body,  $S$  (Watts/cm<sup>2</sup>), is:

$$S = \sigma T^4$$

$$\text{Equation 8.5}$$



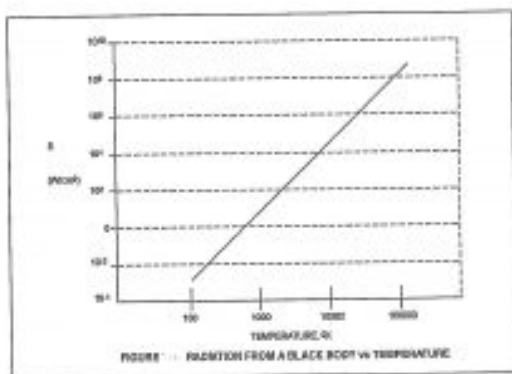
Where  $\sigma$  = Stefan-Boltzmann constant =  $5.67 \times 10^{-12}$  (Watts/cm<sup>2</sup> K<sup>4</sup>),

K= Kelvin temperature.

S = radiation emerging from the surface of a Black Body (Watts/cm<sup>2</sup>)

Figure 8.5 shows the strong dependence of Black Body radiation on temperature. Radiation loss is not important until higher temperatures are reached. Black Body radiation is the upper bound and represents the perfect case.

**Figure 8.5 Black Body Radiation**



Source: Adapted from Figure 1-7 (Nielsen, 2012)

## IMPLICATIONS

*Damaging targets depend not only on delivering energy but also on concentrating the energy in both space and time. In space, we deliver*

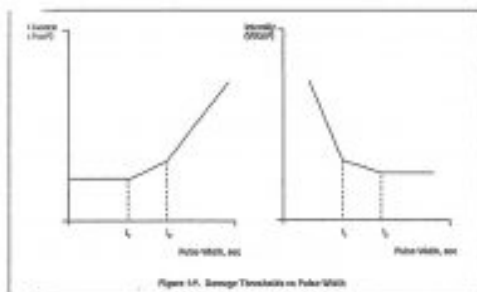
about 10,000 Joules per  $\text{cm}^2$  of the target surface, either at a single point (bullet) or over the whole surface, as in a nuclear weapon. In time, energy must be delivered more rapidly than the target can shed energy through conduction, convection, and radiation loss mechanisms. The fluence (Joules /  $\text{cm}^2$ ) or Intensity (Watts /  $\text{cm}^2$ ) necessary to damage a target will vary with the time or pulse width that the weapon engages the target. (Nielsen, 2012)

The goal is to look at how a DEW deposits energy in a target and then consider energy deposition and loss rates to determine the criteria for damaging the target.

### FLUENCE AND INTENSITY

Two concepts are used frequently in determining criteria for target damage assessments. **Fluence** is the energy per area (Joules /  $\text{cm}^2$ ) necessary to damage a target. **Intensity** is the power per area (Watt /  $\text{cm}^2$ ) necessary to damage a target. Both vary with time or pulse width that the weapon engages the target and have the form shown in Figure 8.6. For extremely short times, energy is deposited into the target so rapidly that there is no way for radiation, conduction, or other energy loss mechanisms to carry it away. For short pulse widths less than  $t_1$ , the fluence necessary to damage the target is constant, and the Intensity necessary to damage it decreases linearly. At longer interaction times,  $t_1$  and  $t_2$ , some of the energy deposited is carried away before contributing to the damage. The fluence in this case to achieve damage begins to rise with pulse width. Beyond the long width  $t_2$ , energy is deposited too slowly to damage unless some minimum intensity is exceeded, and the energy threshold is proportional to the pulse width. (Nielsen, 2012)

**Figure 8.6 Fluence and Intensity**



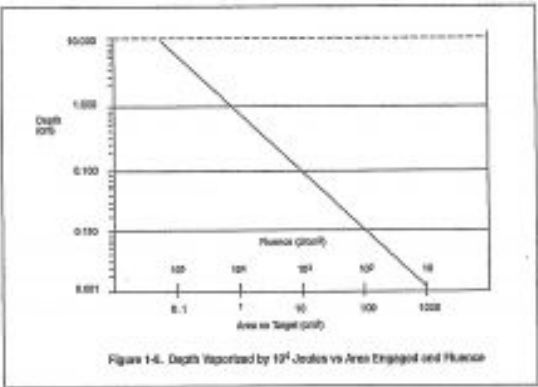
Source: Adapted from Figure 1-8 (Nielsen, 2012)

## ALL-PURPOSE DAMAGE CRITERIA

10,000 Joules is a reasonable first approximation damage criteria in developing weapon parameters that are likely to achieve damage. This is certainly true for hard damage mechanisms like melting or vaporization. We are talking about delivering a fluence ( $104 \text{ J/cm}^2$ ) which for most weapons will damage targets on time scales too short for the energy to be rejected. (Nielsen, 2012) This was evidenced in Table 8.2. Figure 8.7 suggests the reason for this magic number. It shows the depth to which 104 Joules vaporizes a target as a function of the area over which the energy is spread. 104 Joules can only vaporize a significant depth of target when over which it is spread has a fluence on the order of  $104 \text{ J/cm}^2$ . At significantly lower fluences, the depth vaporized would not be sufficient even to penetrate the skin of most targets. (Nielsen, 2012) Nielsen suggests that  $104 \text{ Joules / cm}^2$  is the magic criterion because so many weapons place energies on the order of  $104 \text{ J / cm}^2$ . Making a hole in a target to the depth of 1 centimeter is sufficient to damage almost anything. Many targets are less than 1 cm thick if we count the thickness of the solid matter that must be penetrated to prevent the

target from functioning. The outer surface of a car is sheet metal less than 1 centimeter. If a weapon ( $104 \text{ J} / \text{cm}^2$ ) were to propagate through the air and penetrate the surface near the gas tank, the car might blow up or catch fire. The same weapon would not affect the engine block. (Nielsen, 2012)

**Figure 8.7 Depth Vaporized by 104 Joules v Area Engaged and Fluence.**



Source: Adapted from Figure 1-9 (Nielsen, 2012)

**ENERGY SPREAD AND LOSS IN PROPAGATION**

There are two types of energy losses in propagation: the *Spreading of energy such that it does not interact with the target and the wasting of energy in interactions with a physical medium, such as the atmosphere, through which it passes to destroy the target.* Type one occurs whether the weapon or target is located on earth or in

the vacuum of space. Type two occurs primarily when a weapon or target lies within the atmosphere. Table 8.3 shows the Energy losses in propagation as a function of weapon type and loss mechanisms.

**Table 8.3 Energy losses in propagation**

| Weapon Type                       | Energy Loss Mechanism                    |
|-----------------------------------|--|
| Kinetic Energy (bullets, rockets) | Atmospheric Drag                         |
| Lasers                            | Absorption by molecules                  |
|                                   | Scattering by molecules                  |
|                                   | Absorption by aerosols (small particles) |
|                                   | Scattering by aerosols                   |
| Microwaves                        | Absorption by molecules                  |
|                                   | Scattering by molecules                  |
|                                   | Absorption by water droplets             |
|                                   | Scattering by water droplets             |
| Particle Beams                    | Energy losses to electrons               |
|                                   | Scattering from nuclei                   |
|                                   | Scattering from electrons                |
|                                   | Radiation                                |

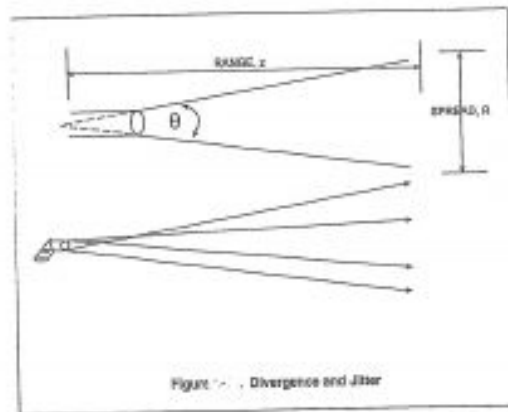
Source: (Nielsen, 2012)

**ENERGY SPREAD**

There are opposite ends of weapon types to consider in discussing damage criteria. DEW, in which all the energy

transmitted is brought to bear on the target, and bombs in which the energy is spread out indiscriminately over an ever-expanding space. Real weapons fall in between these extremes. (Nielsen, 2012) Every weapon has an inherent “spread” of energy associated with its propagation. The terms divergence and jitter describe the two types of spread usually observed. The former has to do with natural phenomena like the diffraction of light from a laser. The latter term, for instance, has to do with the lack of repeatability of the shot group with bullets fired by a skilled shooter at a target at a range  $z$ . See Figure 8-8 for clarity of energy *spread*. Both Divergence and jitter are measures of departure from perfect energy propagation aimed at a target. (Nielsen, 2012)

**Figure 8.8 Divergence and Jitter**



Source: Adapted from Figure 1-11 (Nielsen, 2012)

## CONCLUSIONS

In essence, the study of DEW is a study of energy – how it propagates to, interacts with, and is redistributed within a target. The goal of using a DEW – especially aimed at CBRN from the air via drones – is to determine under what conditions sufficient energy will accumulate within a target to damage it. To achieve damage, energy must be concentrated both in space and time. (Nielsen, 2012) Fundamentally we have:

1. The necessary fluence for a hard target kill is on the order of 10,000 J / square cm. [\[13\]](#)
2. For 10,000 Joules / square cm to achieve damage, it must be concentrated in time so that it cannot flow and be redistributed within the target.
3. The loss and redistribution of energy occur through conduction, convection, and radiation. Either fluence or Intensity becomes a limiting threshold when these heat loss mechanisms are in play.
4. DEW ideally propagates energy directly at a target. Real-life spreads energy through Divergence and jitter.
5. In the atmosphere, various loss mechanisms ( absorption, scatter, etc.) cause a fraction of the energy directed at a target to be lost in the propagation to it,
6. DEW must be capable of giving up energy over the range of propagation to the target and still place sufficient fluence or Intensity on the target to damage it. (Nielsen, 2012)
7. UAS /Drones and UUV are capable of deploying/delivering energy to a target – especially CBRN assets because of their high value and impact on human life. (Nichols R. K., Hardening US Unmanned Systems Against Enemy Counter Measures, 2019)

## Bibliography

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

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

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

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

Beason, D. (2005). *The E-Bomb: How America's new directed energy weapons will change the way future wars will be fought*. Cambridge, MA: Da Capo Press.

Foley, W. S. (March 1979). Ancient Catapults. *Scientific American*, 240, 150.

Glasstone, S. &. (1977). The Effects of Nuclear Weapons, 3rd Edition. In S. &. Glasstone, Chapter V, Figures 5.20, 5.22 & 5.23. Washington, DC: UGPO.

Halsam, C. M.-S. (1982). *Small Arms and Cannons*. Oxford: Brassey's Publishers.

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., & Sincavage, S. M. (2021). *Disruptive Technologies with Applications in Airline, Marine, and Defense Industries*. Manhattan, KS: New Prairie Press #38.

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](http://www.newprairiepress.org/ebooks/27)

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

Vernard Foley, G. P. (January 1985). The Crossbow. *Scientific American*, 252, 104.



## ENDNOTES

[1] Nielson's book is an inspiration for a few chapters in our book. (Nielson, 2012) has been chosen by the Director of the UAS Cybersecurity graduate program as a textbook. We are indebted to Phillip E. Nielsen for his work.

[2] Philip E. Nielsen is a director and senior technical advisor for MacAulay-Brown, Incorporated, a defense engineering services firm headquartered in Dayton, Ohio. Before joining MacAulay-Brown, Dr. Nielsen served on active duty with the U.S. Air Force (USAF) for 26 years, retiring as a colonel. During this period, he served in various positions related to the research, development, and acquisition of advanced weapon systems. He received the USAF Research and Development Award for his contribution to high-energy laser physics in 1975. Phillip E Nielsen was associated with the National Defense University (1987-1988) and The USAF Studies and Analyses Agency. Dr. Nielsen has produced a brilliant discussion of DEW. The authors of this book give full attribution to Dr. Nielsen for his contributions.

[3] Nuclear weapons may be characterized by megatons, bullets in terms of muzzle velocity, and particle beams in terms of amperes of current. The commonality is the amount of energy absorbed by the target, which leads to similar levels of damage achieved at similar levels of energy deposited. (Nielsen, 2012)

[4] No self-respecting American chemical engineer would think in terms of metrics or Joules. English units are preferred (remember the '60-'70s gas pump fiascos in liters?) So,  $1\text{ m} = 3\text{ ft.}$ ,  $1\text{ BTU} = 1,054.35\text{ J}$ ,  $1\text{ lb} = 0.454\text{ kg}$ . However, the literature calls for Joules – so be it. Protest noted.

[5] See (Nielsen 2012) Appendix A for standard units used in this chapter or any modern physics reference.

[6] For us old-time American engineers for reference points: 1 BTU = 1055 J; 1 Calorie = 4.19 J; 1kw hr =  $3.6 \times 10^6$  J; 1eV =  $1.6 \times 10^{-19}$  J and 1 erg =  $10^{-7}$  J.

[7] Hmm, maybe weapons designers have inflated egos. Joules sound more impressive. One ice cube. This is a standard type of chemical engineering problem. The ice cube is raised enough to make it a puddle of water (soft design). The object is to vaporize the target completely. This means we have to keep adding energy to change states, raise the ice +water to water to water plus steam, and finally to only steam. The total energy balance is  $2,100 + 16,700 + 21,000 + 122,000 = 161,800$  Joules. The Latent heat of vaporization accounts for ~ 75% of the destruction. A lot of energy goes into separating the bonds and structure of the molecules to disperse them into vapor. A plot of Temperature v energy deposited in Watts (Watts = Joules/sec) demonstrates that the majority and time and energy are taken up vaporizing the molten cube (*hard design*).

[8] A standard ton of air conditioning removes 12,000 BTUs/ hr (3.5 kW). Industrial towers remove 15,000 BTUs /hr = 1 ton to account for inefficiency in the compressor. As a comparison, a rule of thumb is ~ 420 kJ / Kg (970 BTU/LB) of heat energy absorbed for evaporated water in an open circuit cooling tower.

[9] Aka called “Fluence” Units of fluence are  $1 \text{ J/cm}^2 = 104 \text{ J/m}^2$  and  $1 \text{ W /cm}^2 = 104 \text{ W/ m}^2$

[10] The effect of the area can be better understood by looking at the energy delivery from the two atom bombs delivered against Hiroshima and Nagasaki. (Glasstone, 1977) Both weapons had yields of about 20kT; they released about  $8 \times 10^{13}$  Joules of energy. At a range of z of 0.1 mile (=  $1.6 \times 10^4$  cm), the energy density would be approximately  $8 \times 10^{13} \text{ Joules} / 4\pi z^2 = 2.5 \times 10^4 \text{ J /cm}^2$  or fluence. So, when the Spreading of the blast energy is accounted for, the result is consistent with other weapon types. Our damage energy density sufficiency is  $10,000 \text{ J / cm}^2$  or fluence.

[11] Thermal conductivity varies for materials. Copper (good conductor) =  $4.2 \text{ J/cm sec deg}$  whereas air (thermal insulator) has a value of  $0.00042 \text{ J /cm sec deg}$ . (Nielsen, 2012) Thermal conductivity is not just a simple single-order equation. Other effects are observed changes in regional temperatures, thermal conductivity, diffusion/diffusivity, and temperature propagation v time

[12] Thermal diffusivity does not vary much from one material to another.

[13] This serves as the upper bound since many targets of interest will be damaged at lower fluences.

# 9. DE Weapons, Projectiles, Damage

By Professor Randall K. Nichols, Kansas State University

## STUDENT OBJECTIVES

- To further understand the parameters of kinetic energy weapons design.
- To explore different types of projectiles and their common bases in the laws of physics and thermodynamics
- To study both the propagation of projectiles and interaction causing damage to the target.

## INTRODUCTION

When we think of kinetic energy weapons, we think of the larger space devoted to *directed energy weapons (DEW)*. Under this banner, high technology devices like lasers, microwaves, particle beams, EMP, rockets, and hypersonic missiles. In a subset of DEW, we find guns, mortars, catapults, crossbows, bullets, torpedoes, shape charges, and spears, to name a few. The common factor is kinetic energy. “Kinetic” comes from the Greek word “*kinesis*,” which means “to move.” (Nielsen, 2012) So, DEW – its energy is directed toward a target and intercepts a small fraction of the target’s surface area. What is now included in this classification are unmanned aircraft systems (drones) and unmanned underwater vehicles. They are perfect deployment vehicles for small-scale CBRNE weapons. The former is covered for the reader. The latter is covered in (Nichols & al., Unmanned Vehicle Systems, and Operations on Air, Sea, and

Land, 2020) and (Nichols & Sincavage, Disruptive Technologies with Applications in Airline, Marine, and Defense Industries, 2021). In this chapter, we expand on chapter 8, fundamental concepts about KEW, discuss the propagation towards a target, preview the interaction with a target, and complete the mechanisms by which the target is damaged. We will discuss a variety of projectiles balls, bullets, shape charge explosives, and Tae Kwon Do strikes.

## **COMMON FRAMEWORK (Chapter 8 Recap)**

*Weapons may be understood as devices that deposit energy on targets. The energy that must be deposited to achieve a given level of damage is relatively insensitive to the type of weapon employed. Nuclear weapons may be characterized in terms of megatons, bullets in terms of muzzle velocity, and particle beams in terms of amperes of current. Still, when reduced to common units for the energy absorbed by the target, similar levels of damage are achieved at similar levels of energy deposited. (Nielsen, 2012)*

## **FUNDAMENTALS OF KEW**

Motion causes kinetic energy. Mathematically, the kinetic energy of an object having a mass of  $M$  and velocity of  $v$  is

$$K = \frac{1}{2} Mv^2$$

**Equation 9.1**

Where  $M$  is in kg,

$V$  is m/s

$K$  is in Joules,  $J = \text{kg m}^2\text{s}^{-2}$

The object with greater mass at the same velocity would have more energy than less mass. An object moving at a greater velocity has more energy. An object is given kinetic energy when outside forces act upon it, doing work and accelerating. An object loses kinetic energy when it exerts forces and works on a second object.

The energy lost from an object one can take the form of additional kinetic energy on the second object (car hitting a car); as heat or loss of energy; disruption of the second object, such as a bullet hitting a deer.

Kinetic energy is gained or lost when an object is accelerated according to Newton's law:

$$\mathbf{F = Ma}$$

**Equation 9.2**

Where F = force in Newtons (MKS system)

M = mass in kg

A = acceleration in m/sec<sup>2</sup>

Force is a vector quantity with magnitude and direction. Both must be specified for a complete solution.[\[1\]](#)

Acceleration due to gravity is 9.80665 m/sec<sup>2</sup>. Gravity exerts a force on all objects, accelerating them towards the center's center regardless of their direction of motion.

## **HUNTING WILD BOARS**

Picture a hunter shooting a wild boar at 300 yards with a rifle that shoots 308 Barnes 175-grain LRX BT centerfire bullets. (Barnes, 2022) We can calculate the trajectory of this specific bullet by a sum of the forces on the bullet leaving the rifle. The bullet exits the rifle at velocity v (use fps) in a straight line and will continue until some other force acts upon it. The force of gravity drives the bullet down at a rate of 32.1741 ft/s<sup>2</sup>. Atmospheric drag induces a force opposite in direction to the bullet's velocity. This force decelerates the object, reducing its velocity. The bullet takes on a curved path of a shorter range with gravity. We can calculate the kinetic energy by slide rule or cheat and use the manufacturing tables (Barnes, 2022). The latter tells us that the KE on target for 300 yards is 1731 FT-LBs,[\[2\]](#) Based

on a muzzle velocity leaving at 2432 FPS and arriving at 300 yards of 2111 FPS. The rifle is zeroed in at 100 yards, so the trajectory (drop) is zero. However, at 300 yards, the drop is - 14.5 inches. This particular bullet has a Ballistic Coefficient of 0.521 (BC). BC of a bullet measures its ability to overcome air resistance in flight (drag force). A high BC means the bullet will slow down less. The normal range for bullets is 0.12 - 1.0 LB/in<sup>2</sup> (kg/m<sup>2</sup> in MKS). Good thing the boar is a large animal because the BC drop on the Barnes 175 gr 308 is significant and would require adjustments to the scope. Most scopes have adjustments in MOA for up-down drop and left-right windage. MOA means the minute of the angle measured in degrees, specifically 1/60 of a degree. One MOA is one inch at 100 yards (or 3 inches at 300 yards). These are calibrated in 1/8, ¼ or ½

increments. Since the drop is -14.5 inches, the up-down control (assume 1/4 increments) would require 3 in/full click x 4 = 12 inches (4 full clicks) + ¾ of a full click = 14.25. Assume wind = negligible and less than five mph. This also assumes the boar is polite enough not to move. The key takeaway is that the KE at 300 yards is 896 FT-LBs less than when it left the rifle's muzzle.

It lost 34% of its rated energy to drag and gravity. BTW, wild boar skin is quite tough and has plenty of fat buildup. The 308 is a good choice for a wild boar under average conditions, from a mid-range distance, with a medium grain expanding bullet and correct shot placement. [\[3\]](#)

## **AT THE BOAR SKIN**

The shielding thickness in older wild boars is approximately 2 inches thick. This very thick skin makes the wild boar resistant to holes. When a projectile encounters a target, our interest shifts from the forces felt by the projectile to those felt by the target. The forces are mirror imaging. Two principles come into play when evaluating the interaction between a KEW and its target. One is the *conservation of energy*, which says that energy is conserved. The energy lost from the projectile must be transferred (given to

/picked up by) the target. If the bullet enters the target at one velocity and emerges from the other side with a lower velocity, the energy transferred to the target is the difference in the kinetic energies on entry and exit. In the case of a boar, the bullets enter the boar, slow down as it passes through 2 inches of tough skin, find their way to vital organs, and stop. The kinetic energy entering the skin is about 896 FT-LBs at 300 yards, and all of that energy is picked up by the boar. The exit velocity is zero. Assuming a heart or kidney shot, that is quite a punch. The loss of kinetic energy through the two inches of boar skin is a function of the drag coefficient,  $C_d$ , which is equal to the drag force  $D$  divided by the density  $\rho$ , times  $1/2$  the velocity,  $v$  squared time the reference area  $A$ . It expresses the ratio of drag force to the force produced by dynamic pressure times the area.

$$F_d = mg = D = \frac{1}{2} C_d \rho A v^2$$

**Equation**

**9.3**

Where:

$$A = m^2 = (2 \text{ in} = 0.0508 \text{ m}) = 0.00258 \text{ m}^2$$

$P = \text{kg/m}^3$  (use density of water at 997  $\text{kg/m}^3$  & not Air density of 1.21  $\text{kg/m}^3$  )

$$M = \text{kg} = m\text{-boar} = 80 \text{ kg}$$

$$g = 9.80 \text{ m/s}^2$$

$$C_d = 0.43$$

Eq 9.3 can be used to determine the difference in velocities in and out of the 2 inches of skin.

We can assume that the boar is as tough as a Dodge Ram pickup (in the field coming at you at 20 mph, you will think it is a tank or APC). The  $C_d$  is 0.43.



$$F_{net} = mg - F_d = \frac{1}{2}$$

$$C_d \rho A v^2$$

**Equation 9.4**

$$\text{Where: } v^2 = (v_{in} - v_{out})^2$$

**Equation 9.5**

$$v_{net} = \sqrt{2 mg / \rho C_d A} = \sqrt{2 (80 \text{ kg}) (9.80 \text{ m/s}^2) / (997 \text{ kg/m}^3) (0.43) (0.00258 \text{ m}^2)}$$

$$v_{net} = \sqrt{1568 / 1.106} = \sqrt{1417.72} = 37.65 \text{ m/s}^2 \text{ net}$$

The 308 hit the skin at 2118 FPS lost ~ 38 FPS through the skin = 2080 FPS into the organs. This loss of velocity is small based on the fluid density of water. Neither water nor air density coefficients are correct. They are merely range OM[4] identification/approximations.[5] The actual density of boar skin & fat is unknown. A reasonable approximation of the loss of kinetic energy through the skin could be based on the BC. Therefore, 896 FT-LBs at 300 yards x 0.521 = 467 FT-LBs of kinetic energy. [6]

The second principle is *the conservation of momentum*. Momentum is calculated as the product of mass and velocity,  $Mv$ . Conservation of momentum requires that the total momentum of the bullet and target be the same before and after they interact. If the boar is initially at rest, and hit by the 308 bullets, with  $M_{vo}$ , the boar's momentum and that of the bullet after the hit will sum to  $M_{vo}$ . Velocity is a vector quantity, so direction is important, as is magnitude.

## DAMAGE

Rather than think in terms of gross features of velocity and energy, the boar experiences pain or *damage*. Damage is the internal disruption of a target. Physical damage of a target is determined by the *pressure* it feels, the area over which it is applied, and the

time for which the pressure is applied. Pressure is the force the boar (target) feels, divided by the area over which that force is applied. (Nielsen, 2012) The target area over which pressure is applied is important. The total force felt by a target is the pressure applied multiplied by the area over which it is applied.

Practical self-defense example: [7] Against any two-handed push, the defender can step back and scoop downward and out, bringing the opponent's torso down and forward. *The defender carries the momentum of the scoop into the blow, directed to the ears with cupped hands.* This technique can be executed (several times) with a K'ihap (short shout) in 7/10 of one second. The medical implications of this defense are significant: unconsciousness or a concussion, rupture of the tympanic membrane with intense pain, possible fracture or dislocation of the jaw, and contusion of the facial nerves and veins. (Adams, 1985) The damage is over a small area, the ear canals.

The time over which a force is also important in determining the target's response. The force times the time over which the force is applied is known as *Impulse*. The key parameters for assessing target damage are momentum and energy of a KEW and resulting force, pressure, and Impulse. See Table 9.1

**Table 9.1 Parameters affecting Target Response and Damage**

| Parameter      | Symbol | Units             | Definition   | Comment   |
|----------------|--------|-------------------|--------------|---|
| Kinetic Energy | K      | Joules (J)        | $Mv^2 / 2$   | Mv projectile mass, velocity                      |
| Momentum       | $\rho$ | kg m/sec          | Mv           | K and $\rho$ are conserved when particles collide |
| Force          | F      | Newtons (Nt)      | $M dv/dt$    | $F = dp/dt$                                       |
| Pressure       | P      | Nt/m <sup>2</sup> | Force / Area | Force/ Area = Energy/ Volume (Nt/m <sup>2</sup> ) |
| Impulse        | I      | Nt sec            | Force x Time |   |

Source: Adapted from Table 2.1, p33 in (Nielsen, 2012)

## SACRIFICIAL DRONES

Raytheon demonstrated the counter-drone capability of its **Coyote** Block 2+ drone in a newly [released](https://www.youtube.com/watch?v=RrRScxnDfrk&t=18s) YouTube video at <https://www.youtube.com/watch?v=RrRScxnDfrk&t=18s>, showing the unmanned vehicle blasting an unmanned aerial platform. (BISHT, 2022) See Figures 9.1 & 9.2. The Coyote is designed to take out small airborne targets.

The video shows the drone launch from a 4×4 Oshkosh Mine-resistant ambush-protected vehicle (M-ATV) and fixed palletized launch system, exploding just before contact with an incoming unmanned platform, destroying it mid-air. The video reveals that the M-ATV is linked to Ku-720 mobile sensing radars while the fixed launcher is fitted with KuRFS precision targeting radar. KuRFS [uses](#) multiple small antennas to “spot, locate, and track small targets at long range,” including incoming mortars, rockets, and drones. (BISHT, 2022)

Israel has been in a battle with Hezbollah for many years.

Hezbollah has the nasty habit of shooting missiles over Israeli cities. Beyond the Iron Dome defenses, Israel counters with **IAI Harop** loitering munitions (drone). Developed by the MBT division of Israel Aerospace Industries, it is an anti-radiation drone that can autonomously home in on radio emissions. This SEAD-optimized[8] loitering munition is designed to loiter the battlefield and attack targets by self-destructing them. The drone can operate fully autonomously, using its anti-radar homing system, or work in a human-in-the-loop mode. If a target is not engaged, the drone will return and land itself back at base. It has been designed to minimize its radar signature through stealth (low-observability). This anti-radiation drone is designed to target enemy air-defense systems in the first line of attack. The small drone (with its small radar cross-section) can evade SAMs and radar detection systems designed to target much larger aircraft or intercept fixed-trajectory missiles.

The IAI Harop has a loiter (flying) time of 6 hours and a range of 1,000 km both ways. It is a larger version of the IAI Harpy and is launched from the ground- or sea-based canisters but can be adapted for air launch. The Harop can operate fully autonomously or take a man-in-the-loop mode, controlled by a remote operator. The Harop features two guidance modes: it can home in on radio emissions by itself with its anti-radar homing system, or the operator can select static or moving targets detected by the aircraft's electro-optical sensor. This latter mode allows the HAROP to attack radars that are presently shut down, therefore not providing emissions for the aircraft to automatically home in on. If a target is not engaged, the drone will return and land itself back at base. See Figure 9.3. (Herzog, 2022)

**Figure 9.1 Coyote Unmanned Aircraft System.**



Source: Raytheon Missiles and Defense (BISHT, 2022)

**Figure 9.2 Coyote unmanned aircraft system on the tarmac of Avon Park Air Force Range in Florida.**



Source: Image: National Oceanic and Atmospheric Administration (BISHT, 2022)

**Figure 9.3 IAI Israeli HAROP**



Source: (Herzog, 2022) [https://en.wikipedia.org/wiki/IAI\\_Harop#:~:text=By%20Julian%20Herzog%2C%20CC%20BY%204.0%2C%20https%3A%2F%2Fcommons.wikimedia.org%2Findex.php%3Fcurid%3D26893414](https://en.wikipedia.org/wiki/IAI_Harop#:~:text=By%20Julian%20Herzog%2C%20CC%20BY%204.0%2C%20https%3A%2F%2Fcommons.wikimedia.org%2Findex.php%3Fcurid%3D26893414)

Sacrificial drones are examples of KEW against other drones or missiles. They propagate through the lower atmosphere. The earth's atmosphere extends to an altitude no greater than 100 km. (62.137 miles = 328,084 ft). Depending on the class, UASs fly from 400 ft to 75,000 ft (0.1219 km – 30.48 km). The ceiling on the IAI Harop is 44,600 m = 15,000 ft. It is armed with a 51 LB = 23 kg warhead and travels at 417 km/h = 259 mph = 225 kn. Its range is 1000 km = 620 mi. It has a circular error probable (CEP), a measure of precision, < 1 m (3ft 3 in) with a 16 kg (35 LB) warhead.

## PROPAGATION IN AN ATMOSPHERE

Kamikaze (suicide) drones are KEW in the atmosphere. They are so near to the surface of the earth we can assume that the force of gravity,  $F = GmM / r^2$ , does not vary significantly for projectiles (whose flight is limited to altitudes within the earth's atmosphere – our Kamikaze's)

The Law of Universal Gravitation describes the effects of gravity on the motion of an object. In Eq 9.6,

$$F = GmM / r^2$$

**Equation 9.6**

Where:

M & m are the masses of two bodies, kg

r is the distance separating them, m

G is the gravitational constant =  $6.67 \times 10^{-11}$  Nt m<sup>2</sup> /kg<sup>2</sup>

F is the attractive force in nt.

The simpler form of this equation is  $F = mg$ , and the direction is towards the earth with an acceleration due to gravity = 9.8 m/sec<sup>2</sup> in MKS units. (Nielsen, 2012)

Another assumption for low-level drone flight is that the earth's curvature is negligible. Artillery rounds have an effective range of about 30 km. Bullets are normally VLOS. [9] 1000 yards is the effective limit. Ballistics is the study of projectile motion. The Barnes chart provides ballistic data out to 500 yards for calibers 223 Remington to 458 Winchester. (Barnes, 2022)

Hitting one drone with another is an exterior ballistics problem. It is not as hard as shooting a golf ball at an ICBM, but it does require

some understanding of Propagation effects and damage caused by them.

### **SIR ISAAC NEWTON (1643-1727)**

Newton's three laws of motion explain the relationship between a physical object and the forces acting upon it. They are:

- 1) An object at rest remains at rest; an object in motion remains in motion at a constant speed and in a straight line unless acted on by an unbalanced force.
- 2) The acceleration of an object depends on the object's mass and the amount of force applied.
- 3) Whenever one object exerts a force on another object, the second object exerts an equal and opposite on the first.

### **NEWTON'S FIRST LAW**

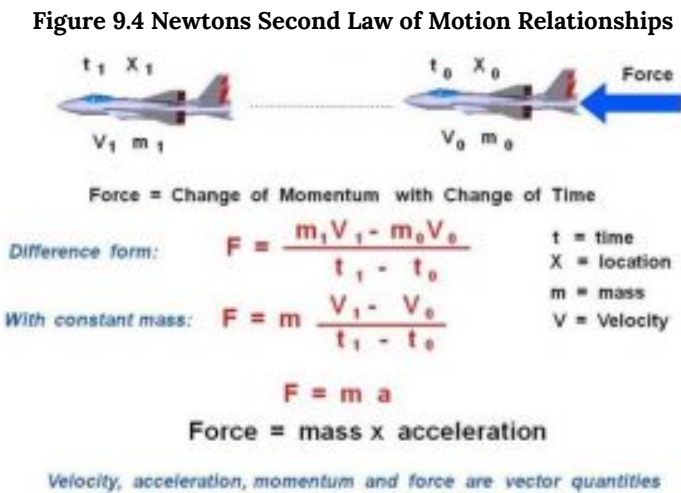
Newton's first law gave the concept of *Inertia*, or the tendency to resist changes in the state of motion. There is no net force acting on an object (if all the external forces cancel each other out). The object will maintain a constant velocity. If that velocity is zero, the object remains at rest. If external forces act on an object, the velocity will change because of the force. An example of *Inertia* involving aerodynamics is the motion of a killer drone changing the throttle setting of the engine to dive down on its target drone. (Glenn Research Center, 2022)

### **NEWTON'S SECOND LAW**

Newton's second law defines a force as equal to a change in momentum (mass times velocity) per change in time. Momentum



is defined as the mass  $m$  of an object times its velocity  $V$ . Explore Figure 9.4.



Source: (Glenn Research Center, 2022)

Let us assume that we have an *unmanned* airplane at a point “0” defined by its location  $X_0$  and time  $t_0$ . The airplane has a mass of  $m_0$  and travels at a velocity of  $V_0$ . An external force  $F$  to the airplane shown above moves it to point “1”. The unmanned airplane’s new location is  $X_1$  and time  $t_1$ .

The mass and velocity of the airplane change during the flight to values  $m_1$  and  $V_1$ . Newton’s second law can help us determine the new values of  $V_1$  and  $m_1$  if we know how big the force  $F$  is. Let us just take the difference between the conditions at point “1” and the conditions at point “0”.

$$F = (m_1 * V_1 - m_0 * V_0) / (t_1 - t_0)$$

9.7

**Equation**

Newton's second law talks about changes in momentum ( $m * V$ ), so, at this point, we can't separate how much the mass changed and how much the velocity changed. We only know how much product ( $m * V$ ) changed.

Let us assume that the mass stays at a constant value equal to  $m$ . This assumption is good for an unmanned airplane; the only change in mass would be the fuel burned between point "1" and point "0". The weight of the fuel is probably small relative to the weight of the rest of the airplane, especially if we only look at small changes in time. If we were discussing the flight of a baseball, then the mass remains a constant. But if we were discussing the flight of a bottle rocket, then the mass does not remain a constant, and we can only look at changes in momentum. For a constant mass  $m$ , Newton's second law looks like this:

$$F = m * (V_1 - V_0) / (t_1 - t_0)$$

9.8

**Equation**

The change in velocity divided by the change in time is the definition of the acceleration  $a$ . The second law then reduces to the more familiar product of a mass times acceleration:

$$F = m * a$$

**Equation 9.9**

Remember that this relation is only good for objects with a constant mass. This equation tells us that an object subjected to an external force will accelerate and that the amount of the acceleration is proportional to the size of the force. The amount of acceleration is also inversely proportional to the object's mass;

for equal forces, a heavier object will experience less acceleration than a lighter object. Considering the momentum equation, a force causes a change in velocity; likewise, a change in velocity generates a force. The equation works both ways.

The velocity, force, acceleration, and momentum have both a magnitude and a direction associated with them. Scientists and mathematicians call this a vector quantity. The equations shown here are vector equations and can be applied in each component direction. We have only looked at one direction, and, in general, an object moves in all three directions (up-down, left-right, forward-back).

Example of force involving aerodynamics: An aircraft's motion resulting from aerodynamic forces, aircraft weight, and thrust. (Glenn Research Center, 2022)

### **NEWTON'S THIRD LAW**

Newton's third law states whenever one object exerts a force on a second object; the second object exerts an equal and opposite force on the first. His third law states that for every action (force) in nature, there is an equal and opposite reaction. If object A exerts a force on object B, object B also exerts an equal and opposite force on object A. In other words, forces result from interactions. Examples of action and reaction involving aerodynamics: the motion of lift from an airfoil, the air is deflected downward by the airfoil's action, and in reaction, the wing is pushed upward, or the motion of a jet engine produces thrust and hot exhaust gases flow out the back of the engine, and a thrusting force is produced in the opposite direction. (Glenn Research Center, 2022)

### **SHOOTING IN THE AIR**

Let's try to take down the UAS with a rifle bullet. This is analogous to solving Newton's second law under the influence of gravity. The motion is broken down logically into two parts – in the downrange direction, denoted by  $z$ , and the up or down in altitude, denoted by  $h$ . There is a corresponding velocity downrange,  $v_z$ , and rising to falling,  $v_h$ . After the bullet is fired, at some time  $t$ , the bullet has propagated a distance  $z$  downstream and is at an altitude  $h$  above the earth's surface. Refer to Figure 9.4. The bullets' velocity,  $v$ , is two components:  $v_z$ , the rate at which  $z$  is increasing, and  $v_h$ , the rate at which  $h$  is increasing or decreasing. For  $v_h$  positive, the bullet is rising, and for  $v_h$  negative, the bullet is falling back to earth. [10] (Nielsen, 2012)

Equation 9.10 solves Newton's law for  $v_h$ ,  $v_z$ ,  $h$ , and  $z$  when the force of gravity acts upon a bullet (projectile):

$$V_h = v_{oh} - gt$$

$$V_z = v_{oz}$$

$$H = v_{oh} * t - gt^2 / 2$$

$$Z = v_{oz} * t \quad \text{Equation 9.10 (group)}$$

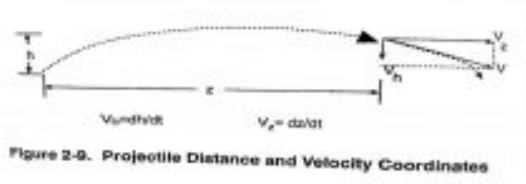
$v_{oh}$  and  $v_{oz}$  are the bullet's initial velocities in the  $h$  and  $z$  directions, respectively. Gravity does not affect  $v_z$ , and the bullet moves downrange at a constant velocity, with  $z$  growing linearly in time.  $v_h$  steadily decreases in time due to gravity until it becomes negative and the bullet falls. The range of the bullet can be found by solving  $h$  for  $t$  at  $h=0$ . Plugging the answer back into the equation for  $z$  gives the result:

$$T_o = 2 v_{oh} / g \quad \text{and} \quad z_r = 2 v_{oh} * v_{oz} / g$$

(Nielsen, 2012)

The initial velocity components ( $v_{oh}$ ,  $v_{oz}$ ) determine the range of the bullet. They are not independent. The gun will release at a total muzzle velocity. This is broken down into  $v_{oh}$  and  $v_{oz}$  by setting the elevation angle of the launcher.

**Figure 9.5                      Projectile Distance and Velocity Coordinates**



Source: Courtesy and Adapted from Figure 2-9 p46 in (Nielsen, 2012)

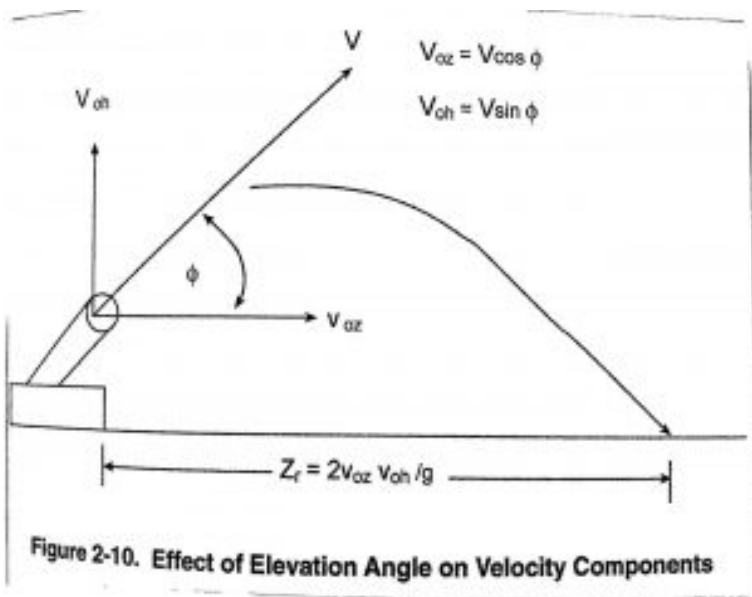
Figure 9.6 shows the effect of elevation angle on velocity components. At a given elevation angle,  $\varphi$  produces vertical and horizontal component vectors. At  $\varphi = 90^\circ$  the shooter aims directly up and comes back down to the launch point. At  $\varphi = 45^\circ$ , the maximum range is achieved. The shape and mass do not enter this analysis nor affect the propagation. (Nielsen, 2012)

## **DRONE VS DRONE IN AIR – COMPLEXITY**

The bullet prorogation is a simple case to demonstrate forces on a projectile aimed at a target.

The picture is more complex when we have a suicide drone trying to intercept another drone. First, we need 3 – dimensional accurate position fixes in space (X, Y, Z ). Both drones are moving. So, the fixes are concerning time. The paths will have to be constantly updated with both feedback and feedforward information to align the drones for target damage. This can be done by radar or sonar pulses. The equations are second-order differential. We are constantly calculating the differentials and then integrating them back to identify the area of attacks and closure rates. They require onboard computing horsepower or offloading to the ground station and return signal interpretation. The computer has to calculate an accurate collision point. Normally we calculate the probable collision point to AVOID collision. In the Kamikaze scenario, we try to cut the distance to zero and make the collision happen. The target is not going to play nice in the sandbox. It detects the intruder and moves at extreme angles to avoid the pursuer. Another factor is AOA or angle of attack. Both drones will be using their AI and C3 systems to produce synchronous or asynchronous movements for attack and defense. It is a beautiful set of solutions to equations in real-time. [11] Think about shooting down an incoming missile with a nuclear MIRV warhead if you want to get a real sense of the mathematics' difficulty. See / digest: (N & Blauwkamp, 2010)

### **Figure 9.6 Effect Of Elevation Angle On Velocity Components**



Source: Courtesy of and Adapted from Figure 2-10 p 47 in (Nielsen, 2012)

## FLIGHT EQUATIONS WITH FORCES [\[12\]](#)

Refer to Figure 9.7 for the following discussion courtesy of Glenn Research Center.

### Figure 9.7 Flight Equations with Drag

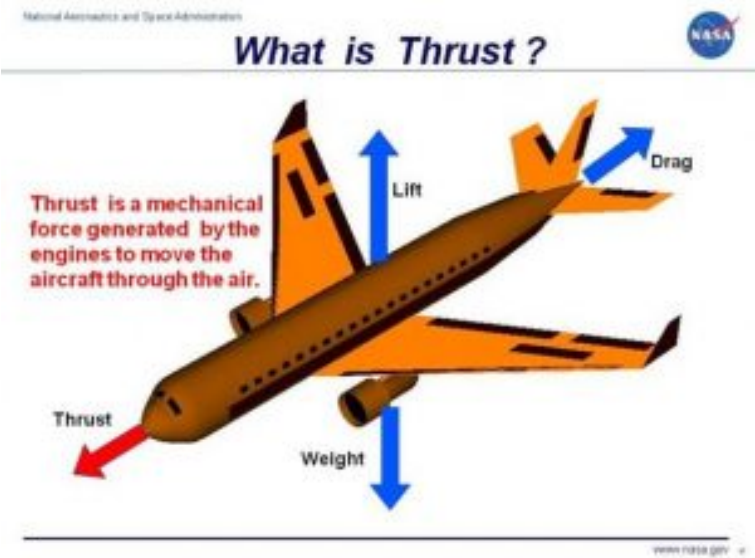




**THRUST**

Thrust is the force that moves an aircraft or UAS through the air. Thrust is used to overcome the *drag* of an airplane or UAS and to overcome the weight of a rocket. Thrust is generated by the engines of the aircraft or UAS through some kind of propulsion system. (NASA, 2022) See Figure 9.8

**Figure 9.8 Thrust**



Source: courtesy of (NASA, 2022)

**Vertical Location**

At launch, the ball is inclined at some angle to the vertical, so we resolve the initial velocity into a vertical and horizontal component. Unlike the ballistic flight equations, the horizontal equation includes the action of aerodynamic drag on the ball. We first consider the vertical component and then develop the equations for the horizontal component.

In the vertical plane, the only forces acting on the ball are the forces of *weight and drag*. There is a characteristic velocity that appears in many of the equations. It is called the *terminal velocity* because it is the constant velocity the object sustains during a coasting descent. Terminal velocity is noted by the symbol  $V_t$ .

### Vertical Descent

During the vertical descent, for a light object,<sup>[13]</sup> The weight and drag of an object are equal and opposite. There is no net force acting on the ball, and the vertical acceleration is zero.

$$a = 0$$

$$W = D$$

Where  $a$  is the acceleration,  $W$  is the weight, and  $D$  is the drag. The weight equation gives the weight of any object:

$$W = m * g$$

Where  $m$  is the mass of the object and  $g$  is the gravitational acceleration equal to 32.2 ft/sec<sup>2</sup> or 9.8 m/sec<sup>2</sup> on the earth's surface. The drag equation gives the drag:

$$D = .5 * C_d * \rho * A * V_t^2 \quad \text{Equation 9.11}$$

Where  $\rho$  is the gas density,  $C_d$  is *the drag coefficient which*

characterizes the effects of the shape of the ball or bullet or projectile,  $A$  is the cross-sectional area of the ball, and  $V_t$  is the terminal velocity. [14] (Glenn Research Center, 2022)

### Velocity

Terminal velocity is calculated:

$$V_t = \sqrt{(2 * m * g) / (C_d * \rho * A)} \quad \text{Equation 9.12}$$

$$\text{Where: } m * g = .5 * C_d * \rho * A * V_t^2$$

Turning to the ascent trajectory, the ball travels at an initial vertical velocity  $V_o$ . With the positive vertical coordinate denoted by  $y$ , the net vertical force  $F_{net}$  acting on the ball is given by:

$$F_{net} = -W - D$$

Because the weight of the object is a constant, we can use the simple form of Newton's second law to solve for the vertical acceleration:

$$F_{net} = m * a = -W - D$$

$$m * a = -(m * g) - (.5 * C_d * \rho * A * v^2)$$

$$a = -g - (C_d * \rho * A * v^2) / (2 * m)$$

Notice that the acceleration changes with time. Multiply the last term by  $g/g$  and use the definition of the terminal velocity to obtain:

$$a = -g * (1 + v^2 / V_t^2) \quad \text{Equation 9.13}$$

### Acceleration

The acceleration is the time rate of change of velocity:[15]

$$V/V_t = (V_o - V_t * \tan(g * t / V_t)) / (V_t + V_o * \tan(g * t / V_t))$$

**Equation 9.14**

### **Vertical Ascent**

This is the equation for the velocity during the vertical ascent. At the top of the trajectory, the velocity is zero. We can solve the velocity equation to determine the time when this occurs:

$$V_o/V_t = \tan(g * t(v=0) / V_t) \text{ and}$$

$$t(v=0) = (V_t / g) * \tan^{-1}(V_o/V_t)$$

$$\text{so,} \quad y = (V_t^2 / (2 * g)) * \ln((V_o^2 + V_t^2)/(V^2 + V_t^2)) \quad \text{Equation 9.15}$$

Notice that the location equation is pretty messy! For a given time  $t$ , we would have to find the local velocity  $V$  and then plug that value into the location equation to get the location  $y$ . At the maximum height  $y_{\max}$ , the velocity is equal to zero:[\[16\]](#)

$$y_{\max} = (V_t^2 / (2 * g)) * \ln((V_o^2 + V_t^2)/V_t^2) \quad 9.16$$

### **Horizontal Location**

The horizontal equations are a little less messy since the only net force acting on the ball is the drag:

$$\mathbf{F_{net}} = \mathbf{m a} = - \mathbf{D} \quad \text{Equation 9.17}$$

The horizontal velocity is inversely dependent on the time. We can solve for the location  $x$  at any time by integrating the terminal velocity equation 9.12 to get:

$$x = (Vt^2 / g) * \ln( (Vt^2 + g * Uo * t) / Vt^2 ) \quad \text{Equation 9.18}$$

## SUMMARY: PROPAGATION IN THE ATMOSPHERE

We have bounced around between balls, bullets, UAS, aircraft, and projectiles in the lower atmosphere. Eighteen equations later, what have you found? Here are five takeaways:

1. Gravity and drag are the main forces that affect the propagation of a projectile in the atmosphere. Since we are close to the earth, gravity is a constant and vectored downward to the earth. Drag opposes the forward motion of a projectile and is proportional to its area as viewed from the bow ( front), the density of air or fluid, and the square of its velocity.
2. Without drag, a projectile will have a max range when launched at an elevation  $\varphi = 45^\circ$ . Drag reduces both the range and altitude achieved by a projectile launched at a given elevation angle.
3. The drag coefficient is a constant of proportionality which measures how well streamlining has reduced the pressure of air on the bow (front) of the projectile. Projectiles moving at supersonic speeds exhibit greater drag coefficients.
4. Winds blow projectiles off course, changing the equations by imparting latitude and longitude dependent forces. [\[17\]](#)
5. Another reasonable deduction pertains to stability. Recall that buzz bombs over London during WWII were very unstable in their initial designs. It was Hanna Reitsch, Germany's female ace test pilot, that solved the instability issues for the "flying bombs." (Patton, 2022) Projectiles will be unstable and tumble in flight (or pull hard to the starboard or port sides) if the center

of the pressure lies ahead of the center of gravity. Designs for projectiles include tail fins or spinning. This is not an isolated problem. The Japanese designers created finned torpedoes that could perform “a feat like an acrobat high-diving in shallow water.” This was to overcome the aerial torpedoes plunging 150 feet before climbing back to an attack depth of 40 feet. (Pearl Harbor Thunderfish in the Sky Japan’s Type 91 Modification, 2015)

## **INTERACTION WITH TARGETS – DAMAGE**

The projectile will strike its target after propagation through the lower atmosphere (maybe). A significant amount of the projectile’s kinetic energy will be transferred to the target (Newton’s Third Law), damaging it! Some of the parameters to be considered to affect the probability of exceeding the threshold for damage are Pressure and Impulse, Angle of Attack, and Target Material and Shape.

### **Pressure and Impulse**

Pressure is the force applied per unit area as the projectile strikes the target. *Impulse* is the integral of the force over time (the force applied multiplied by the time for which it is applied). High pressure and high Impulse are more effective in damaging targets than low equivalents. How much pressure and Impulse a round delivers to a target depends upon its KE, shape, and material. (Nielsen, 2012) Later in the chapter, we will look at the theory of Shaped Charges and how they can be used to destroy tanks or blow-up rock formations and promote commercial drilling operations. (Clipii, 2022) (Shekhar, 2012)

### **The Angle of Attack (AoA)**

A glancing blow will deliver less punch than a direct one. The angle with which the projectile strikes a target is important in determining the effectiveness of the attack and the response of both the projectile and target. At a high AoA, the bullet may ricochet and have little effect, but at a low AoA, the bullet may cause severe damage. (Nielsen, 2012)

### **Target Material and Shape**

The material and shape of a projectile will affect the pressure and Impulse it delivers; the material and shape of the target will affect its response.

All three of these factors can be seen as a practical demonstration. In Tae Kwon Do,[\[18\]](#) [\[19\]](#) students learn the Theory of Power to defend themselves:

- Concentration
- Reaction – Force
- Breathing Control
- Balance
- Speed

They are essentially combining the penetration factors of Pressure, Impulse, AoA, and knowledge of the Target to affect a turbulent defense of life. (Nichols R. K., Self Defense Concepts by U-Dan-Ja-Nim Randy Nichols, 3rd Dan (R), 2003)[\[20\]](#)

Figure 9.9 demonstrates the application of the Theory of Power and the Principles of KEW.

**Figure 9.9 Smashing two Bricks without spacers for 2nd Degree Black Belt Test**





Source: (Nichols R. K., 2nd Degree Black Belt Test – Decided)

Look closely at neck muscles and concrete splatter as the palm heel attack violently breaks the two hard concrete blocks. That's pressure and a perfect AoA. From Table 9.2, the energy of penetration required for striking the solar plexus of an unprotected man is 80 Joules. Figure 9.8 shows two bricks at ~2 inches thick /each placed together (no air space). The energy being generated to penetrate the bricks is (4 inches = 10.16 centimeters) / 0.5 cm @ 1500 Joules = **30,400 Joules**. The energy generated breaks the concrete blocks (target) over a concentrated area of attack about the size of ~ 1 in x 3 in the palm heel surface of the right hand.

**Table 9.2 Kinetic Energy Required for a 7.62 mm Projectile to Penetrate Targets.**

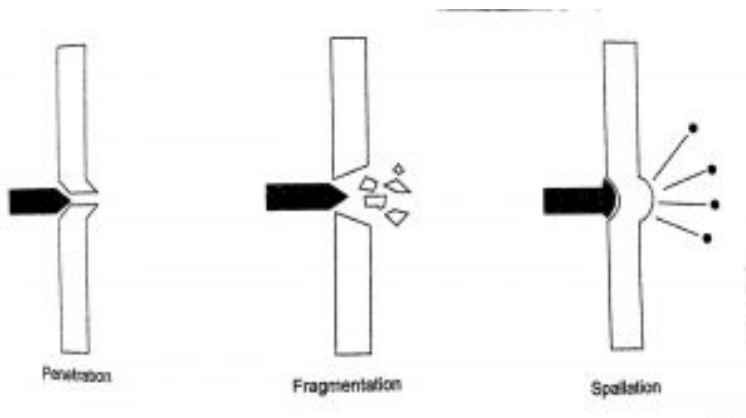
| Target Type                           | Energy for Penetration (Joules) |
|---------------------------------------|---------------------------------|
| Unprotected Man                       | 80                              |
| 23 cm Timber                          | 200                             |
| Very light armor                      | 770                             |
| 0.5 cm concrete                       | 1500                            |
| 1.2 cm Brick                          | 3000                            |
| 4 inches Concrete Blocks (no spacers) | 30,400                          |

Sources: (Nielsen, 2012) (Nichols R. K., Self Defense Concepts by U-Dan-Ja-Nim Randy Nichols, 3rd Dan (R), 2003)

**WHAT IS DAMAGE?**

Given the three parameters that affect damage (Pressure and Impulse, Angle of Attack, and Target Material and Shape), what is the optimum way to combine these parameters to achieve a given level of damage? There are at least three possible effects of kinetic energy projectiles' These are shown in Figure 9.10 They are *penetration* (going through the surface and rattling around for internal damage), *fragmentation* (shattering the target material and the projectile), and *spallation* (although penetration is not accomplished, the shock waves will propagate through the target and throw flakes of material off the back surface. (Nielsen, 2012) Predicting exactly the effects of kinetic energy projectiles on target composition and shape is complex and beyond the scope of this chapter. [21] [22]

**Figure 9.10 Possible Effects Of Kinetic Energy Projectiles**



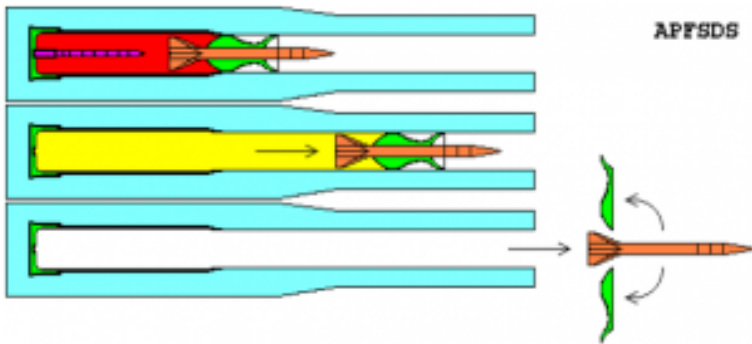
Source: Adapted from Figure 2-18 p61 in (Nielsen 2012)

## **SABOT PROJECTILE DESIGN**

Figure 9.11 shows the Sabot APFSDS (Armor-piercing fin-stabilized discarding sabot) projectile. The modern projectile design uses projectiles that change their configuration during the different phases of their operation. This makes the target interaction optimal. The Sabot round is armor-piercing. The projectile has features designed for each flight portion from tube to target. (Nielsen, 2012)

The function of a sabot is to provide a larger bulkhead structure that fills the entire bore area between an intentionally designed sub-caliber flight projectile and the barrel, giving a larger surface area for propellant gasses to act upon than just the base of the smaller flight projectile. The efficient aerodynamic design of a flight projectile does not always accommodate the efficient interior ballistic design to achieve high muzzle velocity. This is especially true for arrow-type projectiles, which are long and thin for low drag efficiency but too thin to shoot from a gun barrel of equal diameter to achieve high muzzle velocity. *The physics of interior ballistics demonstrates why a sabot is advantageous to achieving higher muzzle velocity with an arrow-type projectile.* Propellant gasses generate high pressure, and the larger the base area that pressure acts upon, the greater the net force on that surface. Force (pressure times area) provides acceleration to the projectile's mass. Therefore, a lighter projectile can be driven from a barrel to a higher muzzle velocity than a heavier projectile for a given pressure and barrel diameter. However, a lighter projectile may not fit in the barrel because it is too thin. To make up for this difference in diameter, a properly designed sabot provides less parasitic mass than if the flight projectile were made full-bore, in particular providing dramatic improvement in muzzle velocity for APDS (Armor-piercing discarding sabot) and APFSDS ammunition. (Bednarik, 2022)

**Figure 9.11 SABOT APFSDS Projectile**



The function of an APFSDS sabot (Armor-piercing fin-stabilized discarding sabot)

red: propellant

orange: long rod penetrator

yellow: propellant gases

green: sabot

blue: gun barrel

Source: (Bednarik, 2022)

### Shaped Charges [\[23\]](#)

One last item to be covered is the versatility of projectile design. One of the most useful designs is the shaped charge used in military and non-military applications.

A shaped charge is an explosive charge shaped to focus the effect of the explosive's energy. Different types of shaped charges are used for various purposes such as cutting and forming metal, initiating nuclear weapons, penetrating armor, or perforating wells in the oil and gas industry.

A typical modern shaped charge, with a metal liner on the charge cavity, can penetrate armor steel to a depth of seven or more times the diameter of the charge (charge diameters, CD), though greater depths of 10 CD and above have been achieved. Contrary to a widespread misconception (possibly resulting from the acronym HEAT, short for high-explosive anti-tank), the shaped charge does not depend in any way on heating or melting for its effectiveness; that is, the jet from a shaped charge does not melt its way through armor, as its effect is purely kinetic – however, the process does create significant heat and often has a significant secondary incendiary effect after penetration. (Wikipedia, 2022)

### **Modern military**

The common term in military terminology for shaped-charge warhead is high-explosive anti-tank warhead (HEAT). HEAT warheads are frequently used in anti-tank guided missiles, unguided rockets, gun-fired projectiles (both spun and unspun), rifle grenades, land mines, bomblets, torpedoes, and various other weapons. (Wikipedia, 2022) See Figure 9.12 for a HEAT example.

**Figure 9.12 HEAT Projectile**



Source: (Wikipedia, 2022)

### **Non-military**

In non-military applications, shaped charges are used in the explosive demolition of buildings and structures, particularly for cutting through metal piles, columns, beams, and boring holes. In steelmaking, small, shaped charges are often used to pierce taps that have become plugged with slag. They are also used in quarrying, breaking up ice, breaking log jams, felling trees, and drilling post holes. Shaped charges are used most extensively in the petroleum and natural gas industries, particularly in completing oil and gas wells. They are detonated to perforate the well's metal casing at intervals to admit the influx of oil and gas.

## **SHAPE CHARGE FUNCTIONS**

A typical device consists of a solid explosive cylinder with a metal-lined conical hollow in one end and a central detonator, array of detonators, or detonation waveguide at the other end. Explosive energy is released directly away from (normal to) the surface of an explosive, so shaping the explosive will concentrate the explosive energy in the void. If the hollow is properly shaped (usually conically), the enormous pressure generated by the detonation of the explosive drives the liner in the hollow cavity inward to collapse upon its central axis. The resulting collision forms and projects a high-velocity jet of metal particles forward along the axis. Most of the jet material originates from the innermost part of the liner, a layer of about 10% to 20% of the thickness. The rest of the liner forms a slower-moving slug of material, which is sometimes called a “carrot” because of its appearance. (Wikipedia, 2022)

Because of the variation and the liner's collapse velocity, the jet's velocity also varies along its length, decreasing from the front. This variation in jet velocity stretches it and eventually breaks it into particles. Over time, the particles tend to fall out of alignment, which reduces the depth of penetration at long standoffs. (Wikipedia, 2022)

At the cone's apex, which forms the very front of the jet, the liner does not have time to be fully accelerated before it forms its part. This results in its small part of the jet being projected at a lower velocity than the jet formed later behind it. As a result, the initial parts of the jet merge to form a pronounced wider tip portion. (Wikipedia, 2022)

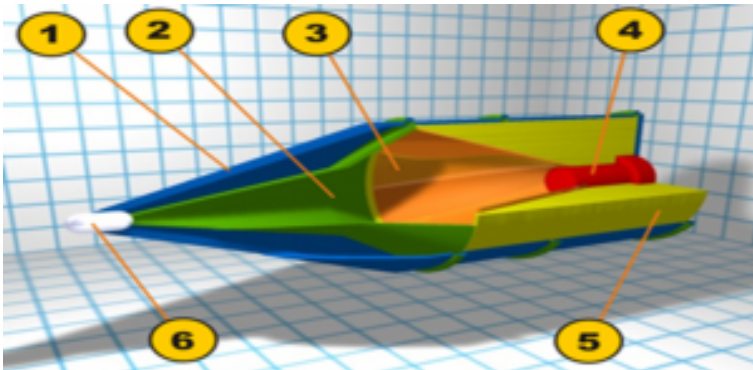
Most of the jet travels at hypersonic speed. The tip moves at 7 to 14 km/s, the jet tail at a lower velocity (1 to 3 km/s), and the slug at a still lower velocity (less than 1 km/s). The exact velocities depend on the charge's configuration and confinement, explosive type, materials used, and the explosive-initiation mode. At typical velocities, the penetration process generates such enormous pressure that it is considered hydrodynamic. (Wikipedia, 2022)

The location of the charge relative to its target is critical for optimum penetration for two reasons. If the charge is detonated too close, there is not enough time for the jet to fully develop. But the jet disintegrates and disperses after a relatively short distance, usually well under two meters. At such standoffs, it breaks into particles that tend to tumble and drift off the axis of penetration so that the successive particles tend to widen rather than deepen the hole. At very long standoffs, velocity is lost to air drag, further degrading penetration. (Wikipedia, 2022)

The key to the effectiveness of the hollow charge is its diameter. As the penetration continues through the target, the width of the hole decreases, leading to a characteristic “fist to finger” action, where the size of the eventual “finger” is based on the size of the original “fist.” In general, shaped charges can penetrate a steel plate as thick as 150% to 700%<sup>[44]</sup> of their diameter, depending on the charge quality. Figure 9.13 is for basic steel plate, not for the composite armor, reactive armor, or other types of modern armor. (Wikipedia, 2022)

Figure 9.13 shows the internals of the Shaped Charge Projectile.

**Figure 9.13 Charge Projectile Detail**



Source: (Wikipedia, 2022)

### **SUMMARY: TARGET INTERACTION**

1. Unlike propagation, which follows some clean physical laws, interaction is messy and highly scenario dependent. The effect of a projectile striking a target will depend on such weapon parameters as momentum, energy, and shape; such target parameters as material, thickness, and construction; and scenario parameters as AoA between the projectile and target.
2. The target's response is determined by the stress applied to it and the resulting strain or deformation it suffers. Both stress and strain are related mathematically to pressure and impulse.
3. Projectile design involves tradeoffs among factors that



influence acceleration, propagation, and interaction. (Nielsen, 2012)

## **Bibliography**

Adams, B. (1985). *Deadly Karate Blows The Medical Implications*. Burbank, CA: Unique Publications.

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

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

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

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

Barnes. (2022, February 19). *Barnes Master Ballistics Charts- Rev 2021-03-23*. Retrieved from [www.barnesbullets.com](http://www.barnesbullets.com): [www.barnesbullets.com](http://www.barnesbullets.com)

Beason, D. (2005). *The E-Bomb: How America's new directed energy weapons will change the way future wars will be fought*. Cambridge, MA: Da Capo Press.

Bednarik, K. (2022, February 20). *Sabot Projectile*. Retrieved from <https://commons.wikimedia.org/>: By The original uploader was Karl Bednarik at German Wikipedia. - [Trhttps://commons.wikimedia.org/w/index.php?curid=4071358](https://commons.wikimedia.org/w/index.php?curid=4071358)

BISHT, I. S. (2022, January 12). *Raytheon-coyote-destroys-drone/*. Retrieved from <https://www.thedefensepost.com>: <https://www.thedefensepost.com/2022/01/12/raytheon-coyote-destroys-drone/>

Clipii, T. (2022, February 20). *On mathematical Modeling of Shaped Charge Penetration*. Retrieved from <http://www.diva-portal.org/>: <http://www.diva-portal.org/smash/get/diva2:18367/FULLTEXT01.pdf>

Foley, W. S. (March 1979). Ancient Catapults. *Scientific American*, 240, 150.

Glasstone, S. &. (1977). The Effects of Nuclear Weapons, 3rd Edition. In S. &. Glasstone, *Chapter V, Figures 5.20, 5.22 & 5.23*. Washington, DC: UGPO.

Glenn Research Center. (2022, February 20). *flight-equations-with-drag/*. Retrieved from <https://www1.grc.nasa.gov/https://www1.grc.nasa.gov/beginners-guide-to-aeronautics/flight-equations-with-drag/>

Glenn Research Center. (2022, February 20). *Newtons Three Laws of Motion*. Retrieved from <https://www1.grc.nasa.gov/https://www1.grc.nasa.gov/beginners-guide-to-aeronautics/newtons-laws-of-motion/>

Halsam, C. M.-S. (1982). *Small Arms and Cannons*. Oxford: Brassey's Publishers.

Herzog, B. J. (2022, February 19). IAI HAROP. Retrieved from <https://commons.wikimedia.org/https://commons.wikimedia.org/w/index.php?curid=26893414>

N, F. P., & Blauwkamp, R. &. (2010, January 29). *Modern Homing Missile Guidance Theory and Techniques*. Retrieved from [https://www.jhuapl.edu/Content/techdigest/pdf/V29-N01/29-01-Palumbo\\_Homing.pdf](https://www.jhuapl.edu/Content/techdigest/pdf/V29-N01/29-01-Palumbo_Homing.pdf): [https://www.jhuapl.edu/Content/techdigest/pdf/V29-N01/29-01-Palumbo\\_Homing.pdf](https://www.jhuapl.edu/Content/techdigest/pdf/V29-N01/29-01-Palumbo_Homing.pdf)

NASA. (2022, February 20). *Simple Forces on an Aircraft or UAS*. Retrieved from <https://www.grc.nasa.gov/WWW/K-12/airplane/thrust1.html>: <https://www.grc.nasa.gov/WWW/K-12/airplane/thrust1.html>

Nichols, R. K. (2003). *Self Defense Concepts by U-Dan-Ja-Nim Randy Nichols, 3rd Dan (R)*. Quantico, VA: INFOSEC Technologies.

Nichols, R. K. (2021). Chapter 14: Maritime Cybersecurity. In R. K. Nichols, & J. J. Ryan, *Unmanned Vehicle Systems & Operations on Air, Sea, Land* (pp. 330-356). Manhattan, KS: New Prairie Press #35.

Nichols, R. K. (2022). Chapter 18: Cybersecurity Counter Unmanned Aircraft Systems (C-UAS) and Artificial Intelligence. In D.

M. R. K. Barnhart, *Introduction to Unmanned Aircraft Systems*, 3rd Edition (pp. 399-440). Boca Raton, FL: CRC.

Nichols, R. K. (n.d.). *2nd Degree Black Belt Test – Decided*. Chois Tae Kwon Do School, Corpus Christi, TX.

Nichols, R. K., & Mumm, H. C. (2019). *Unmanned Aircraft Systems in the Cyber Domain*, 2nd Edition. Manhattan, KS: [www.newprairiepress.org/ebooks/27](http://www.newprairiepress.org/ebooks/27).

Nichols, R. K., & Sincavage, S. M. (2021). *Disruptive Technologies with Applications in Airline, Marine, and Defense Industries*. Manhattan, KS: New Prairie Press #38.

Nichols, R. K., Mumm, H. C., Lonstein, W. D., Ryan, J. J., Carter, C., & 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](http://www.newprairiepress.org/ebooks/27)

Nichols, R., & al., e. (2020). *Unmanned Vehicle Systems and Operations on Air, Sea, and Land*. Manhattan, KS: New Prairie Press #35.

Nichols, R., & Ryan, J. M. (2020). *Unmanned Vehicle Systems & Operations on Air, Sea & Land*. Manhattan, KS: New Prairie Press #35.

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

Patton, R. E. (2022, February 20). *Hanna-reitsch-Hitlers-female-test-pilot.htm*. Retrieved from <https://www.historynet.com/>: <https://www.historynet.com/hanna-reitsch-hitlers-female-test-pilot.htm>

*Pearl Harbor Thunderfish in the Sky Japan's Type 91 Modification*. (2015, December 28). Retrieved from <https://www.pearlharboravationmuseum.org/>: <https://www.pearlharboravationmuseum.org/>

Shekhar, H. (2012, September 2). *Theoretical Modelling of Shaped Charges in the Last Two Decades (1990-2010): A Review*. Retrieved from <https://ipo.lukasiewicz.gov.pl/wydawnictwa/wp-content/uploads/2021/03/Shekhar2-2.pdf>: <https://ipo.lukasiewicz.gov.pl/wydawnictwa/wp-content/uploads/2021/03/Shekhar2-2.pdf>

Vernard Foley, G. P. (January 1985). The Crossbow. *Scientific American*, 252, 104.

Wikipedia. (2022, February 20). *Shaped\_charge*. Retrieved from [https://en.wikipedia.org/wiki/https://en.wikipedia.org/wiki/Shaped\\_charge](https://en.wikipedia.org/wiki/https://en.wikipedia.org/wiki/Shaped_charge)

[1] In English units,  $v = \text{fps}$ ;  $m = \text{gr}$  (convert to pounds, lb);  $\text{KE} = \text{FT-LB}$ ; trajectory is in in; Ballistic coefficient, unitless

[2] The energy at the muzzle leaving is 2627 FT-LBs (Barnes, 2022)

[3] Author experience while on safari in India.

[4] OM = Order of Magnitude approximation

[5] The highest density range would be pure air and the lowest would-be pure water. Boar skin and fat density should be between these two values because the boar fluids combine with additional solids to change the density factor.

[6] Staring a wild boar down as it moves through the brush with you as his dinner in his mind, these calculations have little interest. Breathing, keeping the scope on the target, squeeze, center mass, one-shot, stance, training, be ready to jump into the APC vehicle if you miss – these are the mental calculations made.

[7] The author is a 3rd Dan Black Belt in Tae Kwon Do Moo Duk Kwan style. He previously taught self-defense courses.

[8] (SEAD = Suppression of Enemy Defenses)

[9] VLOS = visual line of sight. You need to be a marine or army sniper to take on a target above 1000 yards.

[10] Surprisingly, terrorists who shoot their AK-47s into the air haven't studied this principle of gravity and change in height. With due respect, the gene pool of the group might be affected.

[11] Although fascinating, the required mathematics is out of the scope of this chapter. Be aware that the problem is quite complex; however, several firms have solved it and deployed their solutions in real-time.

[12] This section is taken from (Glenn Research Center, 2022) with grateful thanks from the author.

[13] Both UAS and bullets fit this assumption.

[14] NASA and Glenn Research Center seem to have some affinity for a "ball" discussion as a projectile; however, the equations fit almost any projectile, bullet, missile, or Kamikaze drone.

[15] Integration and substitutions in this derivation are left for the student to read (Glenn Research Center, 2022)

[16] See for a full messy discussion (Glenn Research Center, 2022)

[17] Although not specifically discussed, the effects are reasonable. See: (Nielsen 2012)

[18] Tae Kwon Do (TKD) means Tae – To jump, kick, or smash with the foot; Kwon – To punch or destroy with the hand or the fist; Do – The way or the method.

[19] The author is a 3rd Dan Black Belt (R). He taught self-defense courses for women and private students. At the peak of his career, he was honored to be elevated to ring judge in the TKD Nationals in San Antonio, TX.

[20] This Self Defense presentation(PPTX) is available free to readers, request from the author at [profrknichols@ksu.edu](mailto:profrknichols@ksu.edu).

[21] (Nielsen 2012) does discuss the subject; however, there is plenty of advanced research to be studied. Recommend contacting your local or educational library to access the many databases and papers.

[22] Since Chapter 12 is devoted to hyper-sonics or hypervelocity impacts ( velocities well in excess of the speed of sound), this topic is tabled.

[23] Wikipedia provides 85 references on the subject of Shaped Charges. Good start.

# 10. DE Weapons, MASERS/ LASERS

By **Randall W. Mai, Kansas State University**

## **STUDENT OBJECTIVES:**

- A look at the simple LASER Pointer and how sweet it is from a drone's POV.
- Peruse a short history of LASER-based technology's origin, functioning, and applications.
- Develop an understanding of the many types of LASER weapons and their capabilities of affecting a target.
- Summarize the technical capacities of LASERS from Nielson's Chapter 3). (Nielson, 1994)
- Examine ways LASERS could be attached to an sUAV and larger UAVs and what damage could be expected from their use.
- Observe the political implications of LASERS
- Think asymmetrically about how to defeat swarming drones with LASER.

## **LASER POINTER**

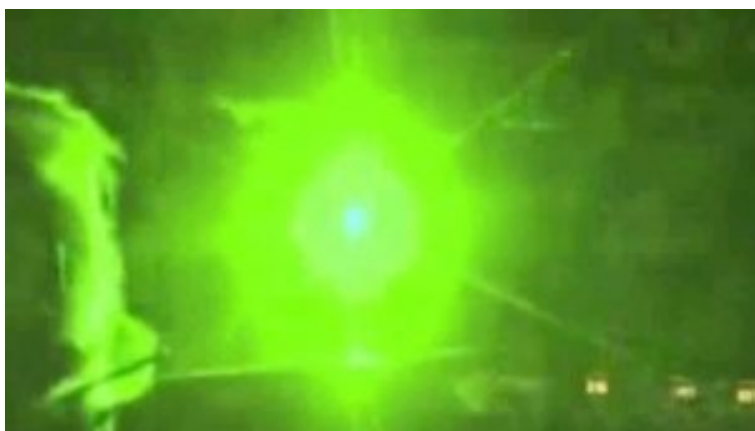
We are familiar with light, a special case of electromagnetic radiation (EMR). Other examples of EMRs include radio waves, x-rays, and microwaves. EMR propagates through space from its source as a wave, much as water propagates through a pond from its source (perhaps a rock thrown into the pond). Chapters 8 & 9 of this textbook cover the theory behind DEW.

A LASER is fundamentally nothing more than a device that can produce an intense or highly energetic light beam.

Perhaps the simplest form of LASER that our students see in many classrooms is the LASER pointer. There is a dark side to these educational devices – blinding commercial pilots.

Laser pointers can be cool toys, posing a serious blinding risk. Figures 10.01 & Figure 10.02 show the view from a pilot's perspective when someone shines a light on an airplane. We put pilots in charge of transporting hundreds of people in an airplane safely to a destination; surely, the last thing you want when you are on the plane is a blind pilot. (laser-pointers-blind-pilots, 2015)

**Figures 10.01 & 10.02 LASER Pointers – Pilot View**







Source: (laser-pointers-blind-pilots, 2015)

### **CAN A LASER POINTER BE USED TO BRING DOWN A DRONE?**

The interesting question is, “can a LASER pointer be used to bring down a drone rather than cut through it” (Can a LASER pointer bring down a drone? 2022)

**Figure 10.00 LASER Pointer (small)**



Source: (Will-a-Laser-Pointer-Bring-Down-a-Drone-Answered, 2022)

Yes, *high-powered lasers* could bring down a drone. Laser rays create heat and can cause the outer body of the drone to melt and damage the drone's internal wiring. Standard laser pointers can interfere with the drone's sensors and emit bright lights, which can blind the camera, thus obstructing the operator's view, potentially causing a crash. (Can a LASER pointer bring down a drone? , 2022)

Laser Pointers are pen-like devices that project a narrow beam of light. All the projected light waves feature similar wavelengths, and they travel together in a phase. Laser light does not spread much, concentrating its energy on a small area. This light concentration is responsible for the heat up and field of view obstruction mentioned above.

### **INFRARED INTERFERENCE**

Drones are flown at low altitudes, creating the need for sensors. This is why most drones feature infrared sensors to help them accurately judge the surface below them. The drone relies on this for auto-landing and obstacle avoidance features. However, the functionality of the downward infrared sensors can be interfered with by laser pointers. They cause the image of the surface below the drone to be blurry. This means the drone cannot reliably sense the surfaces or potential obstacles in its path, leading to a crash.

### **BRIGHT LIGHTS**

A drone operator relies on the drone's camera to get a clear idea of the drone's flight path when flying. Lasers can inhibit the vision of the drone pilot if they emit their bright narrow beams of light to blind the camera. As a result, the drone pilot's view through the camera feed will be disrupted. This might further cause the pilot to lose control of the drone, leading to a collision or crash.

## **HEAT DAMAGE**

Every laser pointer carries some heat, whether it's an ordinary or Industrial-grade laser, due to the direct focus of the light beam. Therefore, there will be heat generation when it comes into contact with the surface of a drone.

If the heat accumulates for long enough, it can melt the plastic housing of the drone, thus revealing and damaging its internal wiring. Some plastic and metal parts can even come loose and fall off. This might lead to erratic behavior or a crash landing.

## **IS TAKING A DRONE DOWN WITH A LASER ILLEGAL?**

Yes. According to the FAA and various state laws, taking a drone down with a laser is illegal. Drones are considered aircraft, and therefore you can be jailed or fined if you use lasers to bring a drone down. Using a laser pointer interferes with the drone pilot's ability to fly and the drone's communication systems. This damages someone else's property, but it can also lead to other potentially harmful events such as crash landing on people or property. Here are some of the defensive systems.[\[1\]](#)

## **RAFAEL DRONE DOME**

Rafael Advanced Defense Systems developed the Rafael Drone Dome system. It is used to secure the airspace by identifying, tracking, and bringing down suspicious drones. *Rafael Drone Dome is an all-weather laser pointer* that cannot be evaded even by rapidly moving drones. Once it has identified a drone, it follows its trajectory and emits laser beams. Additionally, this laser pointer can bring down multiple drones because it emits very high energy. It also blocks the drone's remote control's command and signal. This laser pointer also jams video transmission from the aircraft to the pilot. (Rafael Drone Dome – c-uas-counter-unmanned-aircraft-systems/, 2022)

## **RAYTHEON DRONE-KILLING LASER**

The Raytheon laser often brings down suspicious drones in the United States. Being a *high-energy laser beam machine*, Raytheon can target many drones at a go. Once it targets a drone, it can retarget another one with its speed of light engagement. It is highly effective because it detects, tracks, and shoots down drones using a multi-spectral targeting system.

Several authorities of defense and aviation are using Raytheon Drone-killing lasers to counter drone threats. The good side of this laser pointer is that it can be positioned anywhere or even mounted on a vehicle. (raytheon-drone-killing-laser, 2022)

## **ATHENA**

This advanced high-energy laser beam can bring down both rotary drones and those with fixed wings. These laser pointers do not explode drones; instead, they function by burning the outer parts of the drone. It disables the device or makes it prone to breakup. The Athena laser system has come in handy in bringing down drones flying over commercial or defense airspace with malicious intent. (Airforce Technology, 2022)

## **EVASIVE MEASURES USED BY DRONES**

A laser pointer can damage a drone regardless of how powerful it is. Fortunately, technology has brought protective laser pointers to help drones protect themselves from harmful ones. These evasive lasers are mounted on drones.

This might sound counter-intuitive, but the evasive laser pointers are incredible. The drone protects laser *works by detecting a laser beam coming towards it, taking note of its wavelength, power, and impulse*. After that, the laser projection system mounted on the drone releases its laser pointers and counterattacks the incoming laser beam. The counter protective laser pointer uses two ways to protect the drone. First, it causes the attacking laser pointer to go

astray while convincing the attackers that they have hit their target. Second, there will be a production of light burst once it directly hits the incoming beam. This again will convince the attacker that the targeted drone has been hit.

## **WHICH LASER COLORS ARE THE MOST DANGEROUS AND WHY?**

According to the FAA, **blue and violet** are the most dangerous laser colors to the human eye. This is because the human eye is initially less sensitive to them. Unlike a green or red laser, the eyes take time before reacting to them. A drone operator might take longer before blinking or turning away from blue or violet lasers, thus posing a greater injury risk.

### **WHY ARE BLUE LASER POINTERS MORE DANGEROUS?**

The easy absorption of blue lasers by retina pigments is the most dangerous. Once absorbed, they damage the eye by burning the macula, a highly sensitive retina center.

### **WHAT LASER POINTER COLOR IS THE MOST POWERFUL?**

In terms of brightness, **green is the most powerful laser color**. See Figure 10.01. When compared with other colors, it will always outshine them. This is because the human eye's sensitivity increases in the green region of the spectrum. Colors like red have longer wavelengths, thus decreasing the eye's sensitivity to them.

## **CLASSES OF LASER POINTERS**

Laser pointers are classified according to their damage-causing potential. There are four classes of laser pointers, as discussed below.

### **Class 1 Laser Pointers**

The laser pointers in this category are safe and won't cause eye damage to operators. They don't have much light, and therefore

there are no hazardous effects even when exposed to them. Class 1 lasers are exempted from control measures.

### **Class 2 Laser Pointers**

These laser pointers have low power, and you can see the radiation they emit. Although they are more powerful than Class 1 lasers, they are less harmful to the eyes and will not cause any harm to the skin. You can be safe from them by blinking your eyes or turning away from their light.

### **Class 3 Laser Pointers**

This class consists of two levels – class 3B and class 3R. 3R is harmful to the eyes, and most laser pointers at this level are powerful. Class 3B can severely damage your eyes, especially if you get exposed to them for long. Lasers in this category are used in research and physiotherapy treatments. 3B lasers should not be used in public.

### **Class 4 Laser Pointers**

Lasers in this category are highly powered and feature a power output of more than 500 mW. They are hazardous to the eyes and skin. They can also cause fire hazards, and therefore you should enclose their laser beam path.

### **LASER Pointer Summary**

A laser pointer can bring a drone down, especially the high-powered ones. They heat the drone, damage its wiring system, and interfere with the pilot's field of view. However, using a laser pointer to interfere with a drone is illegal, and you can be imprisoned or pay a hefty penalty for the crime. It is, therefore, not wise to use a laser pointer on a drone. (Can a LASER pointer bring down a drone? , 2022)

So, where did the concept of LASER develop from?

## A LITTLE HISTORY

The word LASER is an acronym for *Light Amplification Stimulated Emission of Radiation*. Theodore Maiman was credited with the building of the first operating LASER. Before Maiman's discovery, Charles Townes and Jim Gordon were credited with the invention of the MASER. It is an acronym as well; Microwave Amplification Stimulated Emission of Radiation.

Immediately after the Second World War, physicists in several laboratories began working on the microwave spectroscopy of molecules. The field grew rapidly but was soon given up by industrial labs as they saw no useful applications for the work and moved to universities at that time. (Townes C. H., 2004)

- – Almost everyone in the field wanted to obtain shorter waves because the wealth of molecular lines and their Intensity of absorption increased rapidly as one moved from centimeter to millimeter wavelengths and then down into submillimeter or infrared wavelengths. Harmonic generation with electronic equipment could achieve millimeter wavelengths but not the submillimeter range. (Townes C. H., 2004) At Columbia University, New York, several years of hard work were spent looking for ways to obtain shorter waves without much success. The US Navy was also interested in short waves. In the early 1950, Townes was asked to form a national committee to search for ways of extending radar technology into the shorter wavelength region. Many centers and laboratories in the United States and Europe were looked at for good ideas for producing short waves. None surfaced. (Townes C. H., 2004)

High temperatures would be needed to excite sufficient numbers of molecules. Too high, and the molecules would all disassociate. Townes then assumed that not all molecules are in thermal equilibrium. He assumed that they would have no limit to their potential radiation intensity. (Townes C. H., 2004)

Townes decided to test the idea in his lab by first making an

oscillator at longer centimeter wavelengths, where ammonia has intense resonances. If successful, he could then push into the submillimeter or infrared region. Townes looked for a student who might give it a try, and before long, Jim Gordon, an outstanding student, turned up. With postdoc Herbert Zeiger, they were set to start. Two years later, Gordon and Zeiger had still not obtained oscillation. At that time, Polycarp Kusch, the departmental chairman, and Isidor Isaac Rabi, his predecessor, went into Charles Townes's office and convinced him that the experiment would not work. (Townes C. H., 2004)

**Figure 10.1: Charles Townes (left) and Jim Gordon with a beam type MASER.**



**Charles Townes (left) and Jim Gordon with a beam-type maser.**

Source: (Townes C. H., 2004)



Two months later, Gordon dashed into the classroom and declared: “it’s working.” The whole class left to go to the lab to witness the demonstration. The new kind of oscillator was named a MASER for *microwave amplification by stimulated emission of radiation*.

Most scientists didn’t believe the MASER idea could be extended to such short wavelengths because of the much higher decay rate of excited atoms or molecules as the wavelength became shorter. By the fall of 1957, Towns had figured out just how an optical MASER (LASER) could be built. On a consulting visit to Bell Labs, Townes ran into Schawlow again and told him about his ideas for an optical MASER. Townes planned to optically excite atomic gas, have it radiated by stimulated emission, and use a cavity as a resonator. He wasn’t completely happy with the cavity, as it would probably have multiple mode oscillations. Schawlow said, “Oh, I’ve also been wondering if that could be done,” and suggested using two parallel mirrors, a Fabry-Perot, as a resonator. After a short delay, while Bell Labs fixed up an appropriate patent, we published our ideas in 1958. There was immediate excitement. The MASER had convinced the industry that this was a valuable field, and very quickly, there were many efforts to build a LASER. The field of quantum electronics had begun. (Townes C. H., 2004)

Theodore Maiman was the first individual to build the first operating LASER in 1960 physically. Many applications have been produced from his operating LASER and are now part of our daily lives. (Townes, 2007) From medicine to communications, completely discoveries have been made. The remaining focus will be on Directed Energy Weapons (DEW), with Drones as the vehicle to deliver applications that stretch from ground-based LASERs to outer space systems.

### **Figure 10.2: Theodore Maiman**



Source: (Townes, 2007)

Stimulated emission of radiation, the critical process behind the LASER, was first recognized by Albert Einstein as early as 1918. But it was only in 1951 that its use for practical amplification of electromagnetic waves was recognized, and in 1954 the first such device, the MASER operating at centimeter wavelengths, was constructed. (Townes, 2007)

LASERS remained at the backwaters of scientific optical

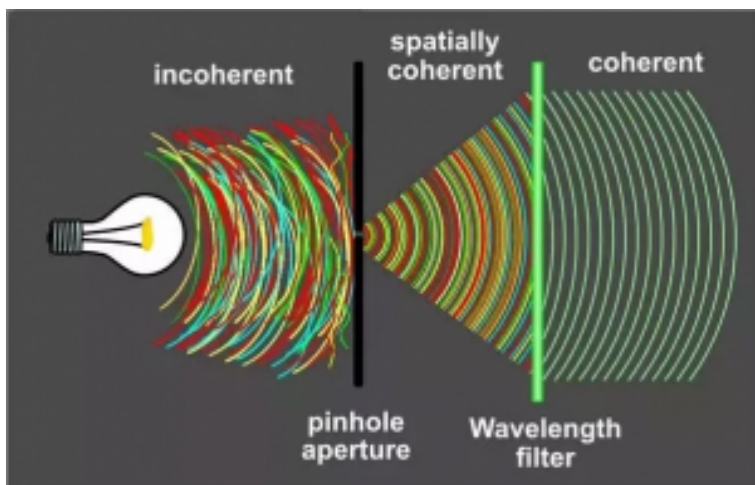
endeavors as a novelty for many years; however, they are now in almost every important aspect of life. Communications, medicine, measurement, optics, and many electronics rely on the special light emitted by LASERs. The characteristic of coherence of LASER light is what makes it very special. LASER light has three distinct characteristics:

1) Monochromatic, it is produced in one wavelength/color. White light is the opposite; it is a blend of wavelengths/colors.

2) It is directional instead of multidirectional like a light bulb, where light comes from every angle.

3) LASER light is Coherent. That is to say, the wavelengths of light are in phase in 3-dimensional space and time.

**Figure 10.3: LASER Coherence**



Source: (Laser Coherence, 2022)

Since discovering the ability to raise various substances to radiate

excited light-producing particles with the three main ingredients; monochromatic, spatially directional, and Coherent, many uses have been developed. LASERs uses are becoming more, and the ways to produce LASER light are becoming better as the electronics that produce them get better.[\[2\]](#)

What exactly is a LASER? A LASER is a device that emits light of identical wavelengths, known as coherent light, in a very narrow beam. The LASER beam's energy can vary widely, from the low power used in LASER pointers to the high heat used to cut metal. (Monte, 2021) Figure 10.3. [\[3\]](#)

### **MILITARY INTERESTS**

By 1962 the US military was spending about \$50 million on LASER development. With all this money flowing in, the US military had certain expectations about a LASER that would serve as a weapon; however, LASERs at the time were unable to emit sufficient energy levels to make a suitable weapon. By 1968 some experts concluded they had hit a wall. The engineering was extremely complicated, forcing them to question if they were trying to violate the LaWS of physics. (Monte, 2021) Unlike regular missile systems that explode, providing rather large fragments of material, LASER light particles are very small in terms of material and transfer lesser amounts of force. Even being propelled at the speed of light, these partials struggle to do much damage to materials that might even be reflective. In the 1970s, the military finally got a weapon—not the war of the Worlds weapon it wanted but a close combat LASER assault weapon (**C-CLAW**). (Monte, 2021) (Arkin, 1 May 1995) It could be used to blind enemy pilots, soldiers, and optical sensors from distances greater than a mile. Under the direction of the US Army, its development continued into the 1980s. A 1983 article in the Washington Post described its application: “The portable LASER beam would sweep back and forth across a battlefield blinding anyone who looked directly at it.” (Arkin, 1 May 1995) In testing,

the C-CLAW could cause the eyes of laboratory animals to explode. Using this on humans, even in war, raised serious ethical questions. Since the Army's LASER would not discriminate between human eyes and optical sensors, the world community, primarily through the United Nations, considered such blinding LASERs horrid. In many ways, blinding LASERs were similar to chemical weapons that could cause blindness, and the UN had already banned such weapons. As a rule, the UN seeks to ban weapons that cause "superfluous injuries and/or unnecessary suffering for little military purpose." (Arkin, 1 May 1995)

By 1995, before their use in combat, the UN established the Protocol on Blinding LASER Weapons, Protocol IV to the 1980 Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons, which prohibited the use of blinding LASERs in warfare and controlled their transfer to any state or non-state actor. The protocol went into force in 1998. (Multilateral-Weapons-Protocol-IV, 2019)

The Protocol on Blinding LASER Weapons has 108 parties (i.e., member states signatories to the treaty), including the United States, Russia, and China. Both China and Russia were early signatories, joining in 1998 and 1999, respectively, while the United States did not become a signatory until 2007. (Multilateral-Weapons-Protocol-IV, 2019) By 2007, other nations likely achieved similar LASER capabilities. With the prospect of a potential adversary using a blinding LASER on American forces, the leadership decided to become a signatory. [4]The Washington Post reported that the US Army's only concern was "over the probable public reaction once the purpose of the weapon becomes known." (Monte, 2021)

In the 1980s, research on directed-energy weapons intensified as Ronald Reagan's administration established the Strategic Defense Initiative (SDI). The Atomic Heritage Foundation, a nonprofit

organization dedicated to the preservation and interpretation of the Manhattan Project and the Atomic Age and its legacy, observed, “Reagan’s interest in anti-ballistic missile technology dated back to 1967 when, as governor of California, he paid a visit to physicist Edward Teller at the Lawrence Livermore National Laboratory. Reagan reportedly was very taken by Teller’s briefing on Directed Energy Weapons (DEWs), such as LASERS and microwaves. Teller argued that DEWs could potentially defend against a nuclear attack.”

When Reagan won the presidency, he wanted a weapon to shoot down enemy missiles from space. He believed that SDI was a path to ridding the world of nuclear weapons. The Soviets were highly vocal opponents to the initiative, arguing that “SDI would pave the way for weaponizing space.” In response, Reagan suggested the United States might eventually share SDI with the Soviet Union, which in an earlier speech, he had described as an “evil empire.” (Monte, 2021) Given Reagan’s characterization of the USSR, the Soviets distrusted his administration and remained entrenched in their opposition to SDI. Other national leaders worried SDI would set off another arms race and make the Cold War even more dangerous.

Nonetheless, despite Soviet protests and shocked officials around the globe, the Reagan administration went forward with the research.

The press dubbed SDI “Star Wars,” based on the LASER-like weapons used in *Star Wars*, a popular science fiction movie. *Much of the program’s development focused on two directed-energy weapons—X-ray LASERS and subatomic particle beams. (Subatomic particle beam weapons use high-energy subatomic particles to damage a target by disrupting its atomic and molecular structure).* Once again, the power needed to supply such weapons proved prohibitive, and SDI floundered. In actuality, this was a good thing. The EMF pulse created by the weapons of SDI would knock out or disable the very electronics needed to track incoming ICBMs. (Monte, 2021)

As evident in the first GULF WAR, the US military eventually

learned to use low-power LASERs to guide missiles to their targets and as range finders on its tanks. By 2006 the US military also used low-power LASERs to “**dazzle**” (i.e., cause temporary blindness) enemy combatants in Iraq. The dazzlers mounted on the American soldiers’ m-4 rifles provided a nonlethal way to stop drivers who attempted to run through checkpoints.

**Figure 10.4: LASER Dazzler for M-4 rifle**



Source: (LASER Sight on M-4, 2022)

**Figure 10.5: LASER Dazzler in operation**



Source: (LASER Sight on M-4, 2022)

The dazzle effect can be defeated with proper goggles blocking the incoming wavelength. High-powered LASERS can be reflected with the use of proper surface coatings. Up to 90% of energy can be redirected. [\[5\]](#)

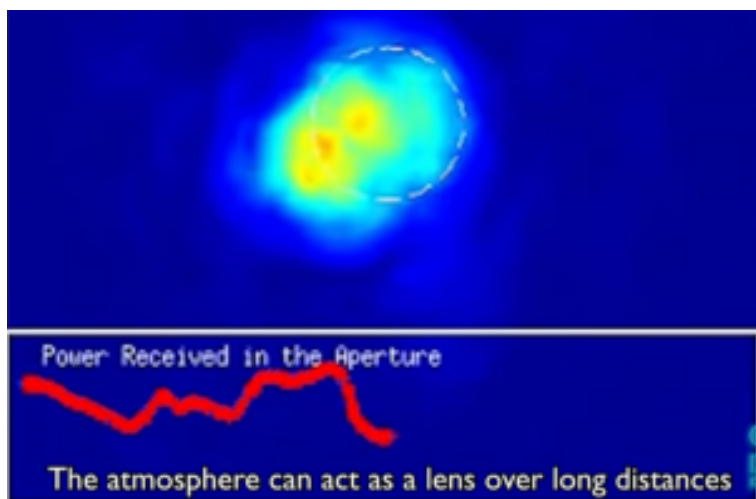
## **WEAPONIZING THE LASER**

Weaponizing the LASER requires an enormous amount of power. Projecting light particles with no mass for all practical purposes must be accelerated to the speed of light and require huge amounts of energy to imply any force upon the desired object to be destroyed. However, technology is progressing. The guidance and control systems, built with integrated circuits, have shrunk in size, becoming more capable, and requiring less power. They follow Moore's law, an observation named after Gordon Moore. (Monte, 2021)

Still, a LASER can have much of its power siphoned off within an atmosphere due to partials and gases that absorb much of the radiation. This can even affect coherence and diminish the ability of the LASER light to stay together, causing a phenomenon called blooming.

### **Figure 10.6: Atmospheric influences**





Source: (Atmospheric influences, 2022)

An atmosphere brings up an important point. Currently, Russia has claimed the successful testing of hypersonic missile systems capable of carrying nuclear weapons that travel thru the earth's atmosphere. Recently, Russia invaded the country of Ukraine and is still engaged as of 04/03/2022. They have created destruction by aerial bombardment and artillery strikes. It has affected the civilian population and is very disturbing to western democracies. Ukrainian leadership has requested NATO impose a no-fly zone over their territory. Russian leadership implied it would consider nuclear weapons if NATO imposed a no-fly zone. Given the tensions in that region, the use of nuclear weapons carried by hypersonic missile systems capable of speeds plus Mach5 pose a unique set of problems for the western allies. The first thought is to have a counter weapons system capable of greater speeds to track and destroy such fast-moving targets. Militarily, the first such system to come to mind is the use of a LASER system. However, the weapons

systems of high-powered LASERs encounter many problems. They are Power source, effective distance, weapons platform, delicate components, and cleanliness.

**Figure 10.7: LASER platform mounted on Boeing 747**



Source: (LASER platform mounted on Boeing 747, 2022)

The platform capable of carrying a LASER that could be used as a weapons system, such as the Boeing 747, would have to *loiter over suspected targeted areas*. An entire fleet would need to be deployed constantly to be effective against incoming hypersonic missiles.

### **MOORE'S LAW IMPLICATIONS**

Moore's law states the speed and capability of computers will double every two years, as the density of transistors doubles on an integrated circuit during the same period. Following Moore's law, the guidance and control circuitry had improved from 1980 to 2007 by more than eight thousand times. Integrated circuit manufacturers of commercial products, such as solid-state memories and microprocessors, had to plan their future products

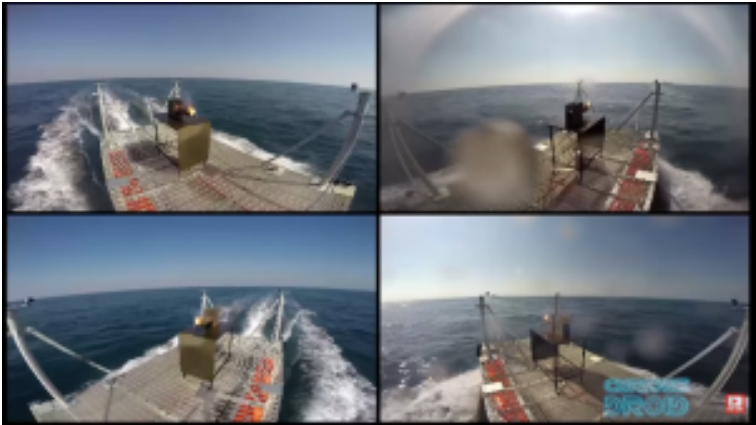
to fit Moore's law. Failing to do so meant they would not be competitive. In a sense, Moore's law became a self-fulfilling prophecy. In the last few years, though, some experts in integrated circuits claim that Moore's law is reaching an end. The size of various features on advanced integrated circuits has shrunk to only a few atoms wide. Experts state that integrated circuits can no longer possibly follow Moore's law. In one sense, they are correct. The ever-shrinking feature size in the integrated circuit industry is how companies could double the circuit density every two years.

However, Moore's observation is a subset of a more encompassing law—namely, the law of accelerating returns. Ray Kurzweil published an essay describing it in 2001, stating, “An analysis of the history of technology shows that technological change is exponential, contrary to the common-sense ‘intuitive linear’ view.” By using the word “exponential,” Kurzweil refers to how technological change increases in a nonlinear fashion, similar to Moore's law and its prediction that the speed and capability of computers will double every two years. That means such change improves 200 percent (relative to its initial ability). If it were linear, it would only grow 100 percent. (Kurzweil, 2020)

Technologists also discovered a crucial element to turn a LASER into a weapon; they pulsed the LASER to fire in discrete blasts timed in fractions of second intervals. This *pulsing* causes the target material's surface to explode with each impact, allowing the plasma the LASER creates to dissipate. This technique requires less energy for the LASER to blast through an object while creating broader craters. In 2014 the US Navy installed the first-ever LASER weapon system (LaWS) on the USS Ponce, an afloat forward staging base, for field testing. After three months of testing in the Arabian Gulf, the navy reported that LaWS worked perfectly against low-end threats, such as small boats and drones. Following the completion of the tests, the navy authorized the commander of the Ponce to use LaWS

as a defensive weapon. (USN, 2022) Until deploying LaWS, most lay public had never heard of the USS Ponce. Then news of its LASER weapon suddenly jolted the Ponce into the public eye. The Ponce, built-in 1966, began to light up the internet as one of the navy's deadliest vessels. (Monte, 2021)

**Figures 10.8 & 10.9: LASER Testing**



Source: (LASER Testing, 2022)

## **NANOTECHNOLOGY**

Nanotechnology is science and engineering conducted at the level of atoms and molecules, typically resulting in feature sizes less than one-thousandth the diameter of a human hair. (Monte, 2021) Although the LASER weapon's technology is secret, numerous articles argue that the rapid development of nanotechnologies over the last decade enabled significant internal component improvements of the solid-state LASER system, making it deployable as a weapon. Currently, the US military leads in developing Nano-weapons, defined as any weapons that exploit nanotechnology. (Monte, 2021)

The US government has been funneling tens of billions of dollars into weaponizing nanotechnology since it established the National Nanotechnology Initiative (NNI) in 2000. The NNI is a research and development initiative involving the nanotechnology-related activities of twenty-five federal agencies. Based on the law of accelerating returns, it is reasonable to conclude that well-funded nanotechnology, combined with well-funded LASER technology, enabled LASERs to evolve from dazzlers in 2007 to directed-energy weapons in 2014. (Monte, 2021) *The navy's new LASER weapon had a dial-in capability. Set to dazzle, it could disable an adversary's drone or boat, allowing its recovery for examination. Alternatively, at full power, it could destroy a drone or boat.* (Monte, 2021)

### **Figure 10.10: LASER weapon Destroying UAV**



Source: (LASER weapon Destroying UAV, 2022)

### **FAIR-WEATHER LASERS**

Are High-Energy LASERs Fair-Weather Weapons? You may have heard the phrase “fair-weather friend,” which refers to a person who will stop being your friend in difficult times. Such a person is not a real friend; the type you can count on when needed. The US military has a name for weapons that only work when weather conditions are right, such as “fair-weather weapons on a sunny day.” The US military does not deploy them because it never knows what weather it will encounter during a conflict. Weapons need to work under a broad spectrum of weather conditions, and the US military needs to know it can count on its armaments to work regardless of the elements. (Monte, 2021)

### **POWER ISSUES**

LASER interacting with matter affects a LASER. Light acts as a

wave; however, it is subject to refraction, diffraction, and all those effects while it propagates, but when it's finally absorbed or scattered from a target, it needs to be treated as a stream of tiny little bullets. How small are the bullets? Quantum theory tells us that light of frequency  $\nu$  is absorbed in units of  $h\nu$ , where  $h$  is a constant (Planck's constant), equal to  $6.63 \times 10^{-34}$  Joule seconds. This means that for a red light with a wavelength of about  $0.7\mu\text{m}$  and a frequency of about  $4 \times 10^{14}$  Hz, the energy of a single bullet is  $h\nu = 3 \times 10^{-19}$  Joules. This is a very small number. (Nielson, 1994) [6]

When compared to the criterion of 10,000 Joules as the zero-order to create damage, we can see how much power a weapons-grade LASER requires. LASER weapons must interact with surface materials. If the LASER cannot interact with a target material, no positive destructive effect will occur. Power is part of the LASER's calculus to be effectively destructive.

The current F-22, F-35, and F-15 are upgraded to increase kW output. This could be used as energy-related weapons are retrofitted to those airframes. Also, as the 6th Generation fighter jet fleet comes online, LASERs will benefit from increased kW outputs.

"[The] peak value of the average intensity [of a LASER beam] can be astonishingly affected by atmospheric turbulence." Therefore, the LASER has the potential to be a fair-weather weapon. If that were the case regarding LaWS, [7] the US military would not deploy it; consequently, we can reasonably assume the US military has worked to mitigate the effects of weather on its LASER weapons. As David Stoudt, writing for Booz Allen Hamilton, observed, "The HEL [high-energy LASER] weapon community has been actively working to mitigate the effects of these conditions for many years, and in the case of atmospheric turbulence, has made significant advances using adaptive optics." Without going into the details, most of which are classified, the US military's LASER can function in multiple atmospheric conditions. As Stoud reports, this capability has enabled the navy to use the LASER in another critical way: "The US

Navy placed a HEL weapon on the USS Ponce, where in addition to its capability as a weapon, it was used almost continuously as a reflecting telescope [a telescope that uses mirrors] that allowed visibility of distances greater than 10 kilometers [about six miles] and penetrating things like smoke, haze, and even light fog.” (USN, 2022) The US Navy is silent on what atmospheric conditions would degrade the effectiveness of the LaWS; however, based on the Booz Allen Hamilton report, it has found solutions to address much of the problem and continues to work on the remainder. In the author’s opinion, LaWS is an all-weather weapon capable of destroying targets in smoke, haze, rain, and fog. (Monte, 2021)

**Figure 10.11: HEL (high energy LASER) USS Ponce**



Source: (HEL High Energy LASER USS Ponce, 2022)



## FOR THE GEEKS

(Nielsen, 1994) Chapter 3 presents 124 pages (pp 81 – 205) of technical details about the propagation of LASER energy in a vacuum and atmosphere on its way to a target. The authors will summarize his main ideas without mathematical derivations: [8]

1. LASERS are intense sources of electromagnetic radiation, with wavelengths from about 10 to 0.4  $\mu\text{m}$  and frequencies from about  $3 \times 10^{13}$  to  $8 \times 10^{14}$  Hz.
2. An index of refraction  $n$  characterizes the materials with which LASERS might interact, and an attenuation coefficient,  $K$ . When light passes regions of different  $n$ , it is bent according to the law of refraction. This can occur deliberately in lenses or inadvertently since fluctuations in  $n$  accompany density fluctuations in the atmosphere. When light propagates a distance  $z$  through a region whose attenuation coefficient is  $K$ , its Intensity is decreased by a factor  $\exp(-Kz)$  [9]
3. A LASER of wavelength  $\lambda$  emerging from the aperture of diameter,  $D$ , can propagate a distance of the order of  $D^2 / \lambda$  as a collimated beam. Beyond this distance, it will diverge at an angle of  $\theta \sim \lambda / D$  through diffraction.
4. Decreases in Intensity resulting from both diffraction and attenuation will reduce the fraction of a beam's energy that can be brought to bear on a target. Beam parameters that may be adjusted to compensate for these effects and deliver damaging intensities to the target include energy, pulse width, wavelength, and the beam's diameter.
5. In the atmosphere,  $K$  is highly wavelength dependent. If a beam becomes too intense, free electrons will multiply, and air will break down, forming an ionized *plasma* that will absorb the beam. They can reverse and detonate the beam. In the atmosphere,  $n$  can vary with turbulence. Other effects are beam expansion ( thermal blooming) or bending.
6. When LASER light encounters a target, a fraction of the light is absorbed in the target surface and appears as heat. The

criterion establishes thresholds for melting and vaporization that energy is deposited so rapidly that it cannot be carried away within the pulse width of the LASER.

7. Targets can be damaged either through erosion which results from melting or vaporization (thermal damage) or through the momentum transferred to the target surface by the evolving vapor jet (mechanical damage) (Nielsen, 1994)[\[10\]](#)

## **NEW THREATS**

The threats the United States now faces are more complex than those during the Cold War were. During that period, the United States had one capable adversary, the Soviet Union. We avoided nuclear war because the American and Soviet Leadership understood the doctrine of mutually assured destruction. Now the United States faces four capable adversaries. With the rise of new weapons (Drones and Hypersonic Missile Systems), radical ideologies, and swarming tactics, the doctrine of MAD (Mutually Assured Destruction) may not deter nuclear war. (Monte, 2021) (countering-the-uas-challenge, 2022) Swarming is a military tactic borrowed from nature. For example, when bees attack, they attack in swarms. In applying this military tactic to sink a US aircraft carrier, an adversary is likely to attempt to overwhelm the carrier group's defenses by attacking it, for example, with large numbers of missiles. The US Navy relies on the Aegis combat system to enable a carrier strike group to combine powerful computer and radar technologies to track and guide weapons and destroy enemy targets, such as incoming missiles. The navy has continued to update the Aegis combat system since its deployment in 1983. In addition, the navies of Australia, Japan, Norway, South Korea, and Spain are using it, with a hundred Aegis-equipped ships now deployed. It also serves as part of NATO's missile defense system. The Aegis combat system is the best missile defense system and can engage medium-range ballistic missiles in flight. Still, the exact

number of ballistic missiles it can intercept is classified. A large number, or swarm, of incoming ballistic missiles fired at an Aegis-equipped carrier may overwhelm the system's defensive capabilities. That would represent a successful swarm attack.

Given the threats previously discussed, the "2019 Missile Defense Review" states, "By the FY 2017 NDAA [National Defense Authorization Act], DoD is preparing a strategic roadmap for the development and fielding of directed-energy weapons and key enabling capabilities. (Monte, 2021) The outlined plan clarifies that high-energy LASER weapons are a strategic element of the US national defense strategy. (Monte, 2021) According to the author, the Pentagon realizes that deploying LASER weapons on navy destroyers, for example, would be critical to defeating swarm attacks against a US aircraft carrier. It does not take much to connect the dots and conclude. According to a Lockheed Martin press release from March 1, 2018, The US Navy awarded Lockheed Martin a \$150 million contract, with options worth up to \$942.8 million, for the development, manufacture, and delivery of two high power LASER weapon systems, [for delivery] by the fiscal year 2020. One unit was delivered for shipboard integration on an Arleigh Burke-class destroyer [the USS Preble], and one unit was used for land testing at White Sands Missile Range [in New Mexico]. The press release does not specify the power of the LASERs, but it is reasonable to judge that they will be as or more potent than the 30-kilowatt LASER the US Navy currently deploys. Numerous articles have speculated on their power, ranging from 60 kilowatts to 150 kilowatts. At 150 kilowatts, the LASER would be five times more potent than the current 30-kilowatt LASER, meaning it can do as much damage as the 30-kilowatt LASER in one-fifth the time. *This increase in power is crucial because it can destroy a target faster and move on to the next threat if necessary.* (Monte, 2021) This factor will be extremely important in defending against swarming sUAV drones and possibly hypersonic missile systems.

**Figure 10.12: Drone being destroyed.**



Source: (Drone being destroyed, 2022)

One thing is clear: The US Navy is serious about deploying LASERs and integrating them into the Aegis combat system. The options mentioned in the Lockheed Martin contract suggest that if the first two LASERs meet the navy's requirements, it will exercise those options and deploy more LASERs onboard its ships. The US Army plans to field an even more powerful LASER weapon in the 250 to 300kilowatt range to protect combat troops against drones, artillery

rockets, helicopters, and attack jets. According to Breaking Defense, “Less than three months after awarding a \$130 million contract [to Lockheed/Dynetics] to build a 100-kilowatt [kW] LASER, the Army has decided to skip the 100-kW weapon and go straight for a much more powerful one in the 250–300 kW range. Unlike the original design, the higher power level could potentially shoot down incoming cruise missiles—plugging a glaring gap in US defenses against a Russia, China or Iran.” This article suggests the navy’s LASER weapon will be in roughly the same range, exceeding previous speculations. (Dynetics, 2019)

### **A SOLUTION WAITING FOR A CONFLICT**

Initially, the scientific community viewed the invention of the LASER as a solution looking for a problem. It is reasonable to imagine it as a solution waiting for a conflict as a weapon. Here are the most compelling reasons why the author thinks the US Navy is eager to deploy LASERs on board ships: LASERs with sufficient power and integrated into the navy’s Aegis combat system have the potential to overcome a broad range of threats, from swarm attacks to carrier-killer missiles. LASERs are cost-effective, with a typical shot to destroy a drone costing less than a dollar in electricity. LASERs allow unlimited shots, requiring only the ship’s generator pump sufficient power. LASERs remove a war vessel’s major vulnerability by replacing conventional weapons that use gun powder, thus eliminating the need to store ammunition within the ship’s magazine. LASERs make it easier to hit a target since there is no need to calculate the trajectory, the windage, or the target’s movement. The LASER’s trajectory is flat, unaffected by windage, and travels at the speed of light, making even a hypersonic missile look as though it is standing still. The US Army’s reason for building an extremely high-power LASER is to address threats from “jet-powered cruise missiles—which fly lower, slower, and with more maneuverability have proliferated worldwide, even to high-end irregular forces like Iran-backed Hezbollah.” In addition, the Army

would also accrue many of the same benefits cited for the navy's LASER system.

### **LASER WEAPONS OF POTENTIAL ADVERSARIES**

Let us examine the LASER weapons of the United States' two most capable potential adversaries, China and Russia. We need to view both as potentially dangerous threats but for different reasons. China has an economy that can support the research and development necessary to develop LASER weapons. Additionally, China supports state-sponsored hacking of US intellectual property, including LASER weapons technology. We must take Russia seriously because it has nuclear parity with the United States. While Russia's economy is weak, it is still modernizing its military. Like China, the Russians appear adept at hacking. (Monte, 2021)

China's LASER weapon closely resembles the US Navy's LaWS. According to Sina.com, China intends to deploy the weapon on land and at sea, including aboard its destroyers, as an alternative to the short-range surface-to-air missile. This last statement implies it has a range of about three miles. Beyond discussing potential applications, China provides no evidence of the LASER's capabilities. Additional information indicates China is working on LASER weapons. In 2017 China released information about a land-mobile LASER weapon that successfully destroyed an unmanned aerial vehicle at a range of about a thousand feet. The Washington Free Beacon also reported, "China's military is expected to deploy a LASER weapon capable of destroying or damaging US military satellites in low earth orbit in the next year [2020], the Pentagon's Defense Intelligence Agency disclosed. In a report on space threats." (Monte, 2021)

The US Defense Intelligence Agency's January 3, 2019, report states, "Chinese leaders characterize China's long-term military modernization program as essential to achieving great power status. Indeed, China is building a robust, lethal force with capabilities spanning the air, maritime, space, and information domains, which

will enable China to impose its will in the region.” The last three words, “in the region,” are particularly significant. (Monte, 2021) A June 26, 2019, article in the New York Times reported, “China is an authoritarian nation that most likely seeks to displace American military dominance of the western Pacific. (NYT, 2019)

China is a nuclear power and may be inclined to use nuclear weapons if its communist-run government thought it might lose such a conflict. (Monte, 2021) In 2018 the United States and China were each other's largest trading partners. According to the Office of the United States Trade Representative's website, “US goods and services trade with China totaled an estimated \$737.1 billion in 2018. Exports were \$179.3 billion; imports were \$557.9 billion. The US goods and services trade deficit with China was \$378.6 billion in 2018.” (Monte, 2021)

These salient facts regarding China's LASER thrusts, its geopolitical goals, and its trade with the United States place its pursuit of LASER weapons in the broader context of its national goal to dominate the Asia-Pacific region. They also delineate the United States' complexities as it attempts to confront China. (Monte, 2021)

Russia's interest in LASER weapons dates to the Soviet Union's construction of a ground-based LASER facility in 1987, a decade ahead of the development of the US ground-based LASER at Lawrence Livermore National Laboratory in 1997. On August 19, 1989, the New York Times reported, “The DoD has pointed in particular to a facility at Sary Shagan in Kazakhstan, which was alleged to contain a LASER weapon that ‘could be used in an anti-satellite role today and possibly a ballistic missile defense role in the future.’” Upon visiting the facility in 1989 as part of the Soviet glasnost policy of openness, the reporters instead found relatively weak LASERS whose “beams were 1,000 times less powerful than those of the Mid-Infrared Chemical LASER at the Strategic Defense Initiative's White Sands [Proving Ground in New Mexico].” (Monte, 2021) If the Soviets had revealed a weapons-grade LASER at the facility, the Times would assuredly have written an article

suggesting that the Soviets could attack US satellites and missiles, information that would have sent shock waves through the Pentagon.

Furthermore, during the same week as the reporters' visit, the Soviets demonstrated "to American experts a high-power gas LASER" at another facility. The demonstration was again part of the Soviet glasnost policy and is proof positive the Soviets had a weapons-grade LASER. These facts raise a question: Were the Soviets being open but misleading simultaneously? During the late 1980s, the US government was deeply concerned regarding the Soviet's LASER capabilities. The New York Times reported in 1987 that "Secretary of Defense Caspar W. Weinberger [under President Reagan] recently has warned of powerful new Soviet LASERs on the horizon. 'We expect them to test ground-based LASERs for defense against ballistic missiles in the next three years.'" Weinberger's statement is clear evidence the US government worried the "balance of terror" would tilt in favor of the Soviets. When the USSR collapsed, Russia inherited its technology. It makes sense that the Russians would continue to develop the LASER technology handed down from the Soviet era. In 2018 Russia tested an anti-ballistic missile interceptor at the site.

The days of glasnost are over. Today, secrecy surrounds the Sary Shagan facility, and news regarding the site is sparse. On March 1, 2018, Russian President Vladimir Putin announced the existence of a new LASER weapon during his State of the Nation address: "We have achieved significant progress in LASER weapons. It is not just a concept or a plan anymore. It is not even in the early production stages. Since last year, our troops have been armed with LASER weapons."

Additionally, Newsweek reported, "Accompanying Putin's March 1 speech, in which he revealed an array of new and advanced weapons, was a short video showing what appeared to be a truck-mounted LASER system. The ministry entitled the clip 'Combat LASER Complex,' but Putin said at the time that he was not ready to



reveal the weapon's name or any other details.” The LASER is similar in appearance to the US Navy’s LASER, which is about all we know. Its capabilities and purpose remain classified. Both China and Russia typically exaggerate their weapons’ capabilities, and both knew the United States was fielding LASER weapons with demonstrated lethality. (Monte, 2021) Their respective leaders were under pressure to show their militaries deployed similar weapons. (Monte, 2021) *They offered no evidence demonstrating their LASERs can down drones, sink small boats, or compensate for atmospheric conditions.* (Monte, 2021) However, we should not discount their military capabilities. Both countries are working on developing LASER weapons. As previously stated, relative momentum is critical in terms of military capability. Short of conflict, we have evidence that our adversaries are using directed-energy weapons, such as microwave weapons, covertly against the United States. (Monte, 2021)

## **OTHER CONSIDERATIONS**

We must look at what will make the most powerful LASER. It may be obvious; however, focusing as much energy in one spot for an appropriate amount of time causing disruption to the material or target will be extremely important. Taking a step back, many of the uses for LASERs require Low power output, mainly due to heat buildup. Heat buildup on computer components is detrimental if not dealt with by some cooling.

Even though LASERs are directional and have coherence, they cannot maintain coherence for an indefinite amount of time and space in an atmosphere. Considering the atmosphere is important because LASER energy interacts with molecules in the atmosphere, thus reducing its effectiveness. The components that make up how long a LASER beam will hang together and what power can be delivered to the targeted material are a function of the Type of LASER, Power, and Design.

The LASER that Maiman initially discovered was a Ruby LASER that used Ruby crystal to develop an oscillation and expel photons of Red LASER light. There are three main types of LASER design in practicality—solid-state LASERs, like Maiman's. Gas LASERs tend to be more uniform and develop less loss in energy, and the resonator can be larger to allow for larger LASER output. However, for weapons-grade, fiber optic LASERs offer the best possible solution.

A fiber optic LASER allows for the greatest amount of LASER output. Regarding design, refraction is how the LASER light will change direction as it transverses from one side of a lens to where it exists. Thin lens coatings are a very involved science based on the chemistry of the coatings applied to the lens. The lens is an important part of the design to establish the coherence of the emitted LASER energy. This is because a lens can affect the Laser's refractive index with lens coatings. A LASER beam begins to hang together at its focal point along its focal length. The focal length is known as the *Raleigh Range*  $Z_r$ . The Raleigh Range is given by:  $Z_r = \pi W^2 / \lambda$ .  $W = D / 3\sqrt{2}$  gives the beam radius.

Conceptually, LASER design is relatively simple and only consists of three components:

1. a medium. This is the source of light within a LASER. It can be composed of a solid, gas, or liquid. The medium is typically confined in a tube.
2. An energy source. The energy source can be an electrical current or another LASER.
3. A feedback element. This component takes the output from the LASER medium and routes it back into the system. (This has the effect of ramping up the energy in the system) The feedback element often consists of two mirrors that confine the LASER light within the LASER medium. In practice, one mirror is partially silvered, meaning the silver coating is less dense and can allow the most powerful LASER light to escape.

These components work together to form a LASER beam.

## CONCLUSION

LASERS represent a potent weapon. LASERS can be attached to drones to attack surface or air targets. On the flip side, LASERS can be used to detect and eradicate drone threats.

## Bibliography

Airforce Technology. (2022, April 7). *usaf-lockheed-athena-laser-weapon/*. Retrieved from [www.airforce-technology.com: https://www.airforce-technology.com/news/usaf-lockheed-athena-laser-weapon/](https://www.airforce-technology.com/news/usaf-lockheed-athena-laser-weapon/)

Arkin, W. M. ( 1 May 1995). *U.S. Blinding Laser Weapons*. London: Human Rights Watch. Retrieved from <https://www.refworld.org/docid/3ae6a7cf10.html>

*Atmospheric influences*. (2022, April 7). Retrieved from [www.youtube.com: Figure 7: Atmospheric influence https://www.youtube.com/watch?v=w6tkL1w27Js&t=35s](https://www.youtube.com/watch?v=w6tkL1w27Js&t=35s)

*Can a LASER pointer bring down a drone?* (2022, April 7). Retrieved from [www.droneblog.com/laser-pointer/: https://www.droneblog.com/laser-pointer/](https://www.droneblog.com/laser-pointer/)

*countering-the-uas-challenge*. (2022, April 7). Retrieved from [www.microwavejournal.com/: https://www.microwavejournal.com/articles/29337-countering-the-uas-challenge](https://www.microwavejournal.com/articles/29337-countering-the-uas-challenge)

*Drone being destroyed*. (2022, April 7). Retrieved from [www.youtube.com: https://www.youtube.com/watch?v=tyUh\\_xSjvXQ](https://www.youtube.com/watch?v=tyUh_xSjvXQ)

Dynetics. (2019, May 15). *team-dynetics-wins-130-million-100kw-class-high-energy-laser-contract-for-us-army*. Retrieved from

www.dynetics.com: <https://www.dynetics.com/newsroom/news/2019/team-dynetics-wins-130-million-100kw-class-high-energy-laser-contract-for-us-army>

HEL High Energy LASER USS Ponce. (2022, April 7). Retrieved from [https://d1ldvf68ux039x.cloudfront.net/thumbs/photos/1707/3622264/1000w\\_q95.jpg](https://d1ldvf68ux039x.cloudfront.net/thumbs/photos/1707/3622264/1000w_q95.jpg): [https://d1ldvf68ux039x.cloudfront.net/thumbs/photos/1707/3622264/1000w\\_q95.jpg](https://d1ldvf68ux039x.cloudfront.net/thumbs/photos/1707/3622264/1000w_q95.jpg)

Kurzweil, R. (2020, July 13). *top-20-predictions-from-kurzweil-future-technologies*. Retrieved from [www.epicheroes.com/](http://www.epicheroes.com/): <https://www.epicheroes.com/2020/07/13/top-20-predictions-from-kurzweil-future-technologies/>

Laser Coherence. (2022, April 7). Retrieved from [images.search.yahoo.com: https://images.search.yahoo.com/yhs/search?p=picture+of+LASER+coherence&fr=yhs-mnet-001&type=type9045647-spa-6246-84501&hspar=mnet&hsim p=yhs-001&imgurl=http%3A%2F%2Fallthingsd.com%2Ffiles%2F2013%2F07%2Fcoherence.jpg#id=3&iurl=http%3A%2F%2Fallthingsd.com%2F](https://images.search.yahoo.com/yhs/search?p=picture+of+LASER+coherence&fr=yhs-mnet-001&type=type9045647-spa-6246-84501&hspar=mnet&hsim p=yhs-001&imgurl=http%3A%2F%2Fallthingsd.com%2Ffiles%2F2013%2F07%2Fcoherence.jpg#id=3&iurl=http%3A%2F%2Fallthingsd.com%2F)

LASER platform mounted on Boeing 747 . (2022, April 7). Retrieved from [www.youtube.com/](http://www.youtube.com/): <https://www.youtube.com/watch?v=w6tkL1w27Js&t=35s>

LASER Sight on M-4. (2022, April 7). Retrieved from <https://ind5.ccio.co/>: <https://ind5.ccio.co/k6/YB/u1/250090585527361016sThElXYBc.jpg>

LASER Testing. (2022, April 7). Retrieved from [www.youtube.com/](http://www.youtube.com/): <https://www.youtube.com/watch?v=w6tkL1w27Js&t=35s>

LASER weapon Destroying UAV. (2022, April 7). Retrieved from [www.youtube.com](http://www.youtube.com/): <https://www.youtube.com/watch?v=w6tkL1w27Js&t=35s>

*laser-pointers-blind-pilots*. (2015, July 7). Retrieved from [paul.is-a-geek.org](http://paul.is-a-geek.org): <https://paul.is-a-geek.org/2015/07/laser-pointers-blind-pilots/>

Monte, L. A. (2021). *War at the speed of light*. (P. E. Central, Ed.) Lincoln, Nebraska, USA: Potomac Books, 2021. Retrieved from

<http://ebookcentral.proquest.com/lib/ksu/detail.action?docID=6460626>

*Multilateral-Weapons-Protocol-IV*. (2019, February 9). Retrieved from <https://www.state.gov/wp-content/uploads/2019/02/09-721.2-Multilateral-Weapons-Protocol-IV.pdf>:  
<https://www.state.gov/wp-content/uploads/2019/02/09-721.2-Multilateral-Weapons-Protocol-IV.pdf>

Nichols, R., & al., e. (2020). *Counter Unmanned Aircraft Systems Technologies and Operations*. Manhattan, KS: new prairie press #31.

Nielsen, P. E. (1994). *Effects of Directed Energy Weapons*. Dayton, OH: USAF.

Nielson, P. E. (1994). Laser Interaction with Matter. In P. E. Nielson, *Effects of Directed Energy Weapons* (pp. 88-89). Coppell.

NYT. (2019, June 26). *united-states-china-conflict.html*. Retrieved from [www.nytimes.com](http://www.nytimes.com): <https://www.nytimes.com/2019/06/26/world/asia/united-states-china-conflict.html>

Rafael Drome Dome - *c-uas-counter-unmanned-aircraft-systems/*. (2022, April 7). Retrieved from [www.rafael.co.il](http://www.rafael.co.il):  
<https://www.rafael.co.il/worlds/air-missile-defense/c-uas-counter-unmanned-aircraft-systems/raytheon-drone-killing-laser>. (2022, April 7). Retrieved from [www.assignmentacer.com](http://www.assignmentacer.com):  
<https://www.assignmentacer.com/raytheon-drone-killing-laser/>

Townes. (2007, June 7). Obituary Theodore H. Maiman. *Nature*, pp. 654-654. doi:<https://doi.org/10.1038/44765a>

Townes, C. H. (2004, November 10). Making Waves. *Nature* 432, p. 153. doi:<https://doi-org.er.lib.k-state.edu/10.1038/432153a>

USN. (2022, April 7). *navy-unveils-next-generation-ddgx-warship-concept-with-hypersonic-missiles-LASERS*. Retrieved from [www.microwavejournal.com/](http://www.microwavejournal.com/):  
<https://www.microwavejournal.com/articles/37513-navy-unveils-next-generation-ddgx-warship-concept-with-hypersonic-missiles-LASERS>

USN. (2022, April 7). *us-navy-successfully-test-fires-high-energy-laser-weapon-system*. Retrieved from [www.foxnews.com](http://www.foxnews.com):

<https://www.foxnews.com/us/us-navy-successfully-test-fires-high-energy-laser-weapon-system>

*Will-a-Laser-Pointer-Bring-Down-a-Drone-Answered.* (2022, January 1). Retrieved from [www.droneblog.com/](http://www.droneblog.com/): <https://www.droneblog.com/wp-content/uploads/2022/01/Will-a-Laser-Pointer-Bring-Down-a-Drone-Answered-735x294.jpg.webp>

## Endnotes

[1] These are just a smattering of the CUAS systems available. The authors do not endorse any product. The CUASS subject is covered in detail in our textbook: (Nichols & al., 2020)

[2] There are many uses for LASERS, both commercially and militarily. The purpose of this chapter is not a history lesson but a look at its potential use as a weapon attached to UAS. Consult any standard textbook for the diversified uses of LASERS.

[3] There has been a vicious legal battle for LASER ownership involving Einstein, Towns, Gordon, Zeiger, Weber, Basov, and Prokhorov. Consult (Monte, 2021) for the historical implications.

[4] If this analysis is correct, it suggests the prospect of having superior conventional weapons trumps ethical concerns.

[5] SME MAI observation 04072022.

[6] Nielson (Nielson 1994) is the expert on using LASERS as DEW. A detailed mathematical and physical analysis may be found in his textbook. Recommended.

[7] LaWS = LASER Weapon System such as the USN advanced LaWS. See: (USN, 2022)

[8] Left to the student for fun.

[9] See Chapter 8 for definitions.

[10] Refer to p 191 of (Nielsen, 1994) for Figures 3-76. "Significant Propagation and Target Interaction Effects, Intensity ( W/cm<sup>2</sup> ) by Pulse (sec). These will bring the seven summary points into focus.

# II. DE Weapons & Microwaves

By **Randall W. Mai, Kansas State University**

## **STUDENT OBJECTIVES**

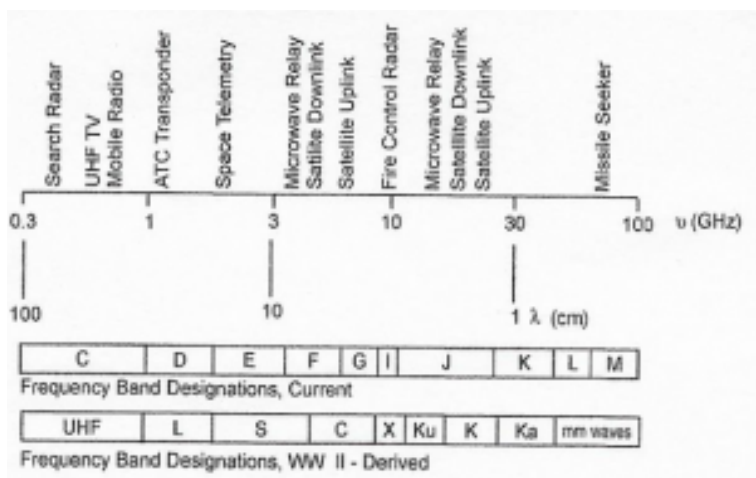
- What are Microwaves?
- How are Microwaves similar and different from Lasers?
- Who uses Microwaves? Civilians / Military?
- Can drones be used for Microwave deployment as a weapon?

Do you like Popcorn? In today's world, you'll most likely have to invoke the assistance of microwaves to enjoy this tasty treat. Like Lasers, Microwaves are another form of electromagnetic radiation. They have a much longer wavelength and a much lower frequency than light. (Nielsen, 2022) Red light has a wavelength of about  $0.7\mu\text{m}$  and a frequency of  $c/\lambda$ , of about  $4 \times 10^{14}$  Hertz. By contrast, Microwave wavelengths of about 1cm and frequencies of 1010 Hertz or 10 Gigahertz(GHz). (Nielsen, 2022)

Most Microwave devices are designed to detect and amplify a weak microwave signal. Figure 11.1 shows a portion of the Electromagnetic Spectrum where Microwaves occur. The majority of the results in the last chapter will also apply here.

**Figure 11.1: Microwave Portion of the Electromagnetic Spectrum**





Source: (Nielsen, 2022) (Nichols & Mumm, 2019)

Higher power Microwave devices are called **LRAD (long-range area denial)**, not to be confused with **LRAD (long-range acoustic devices)**. [1] The first deals with Microwaves, and the second deals with sound waves. The most recognizable device that amplifies Microwaves is the ordinary kitchen Microwave oven that we are all familiar with. It produces much less power than the LRAD.

**Figure 11.2: Kitchen Microwave**



Source: Courtesy of Author (Mai)

**Figure 11.3: Inside of ordinary kitchen microwave oven**



Source: Courtesy of Author (Mai)

**Figure 11.4 Magnetron and set up Transformer**



Source: Courtesy of Author (Mai)

Microwaves interact with water molecules. Electromagnetic Radiation consists of photons and an associated sinusoidal varying electric field. Water molecules are dipolar, meaning that they have oppositely charged ends, making them asymmetric.

When a microwave interacts with water, the energy attempts to flip the water molecule to align with the varying magnetic field. The magnetic field changes or flips at approximately 2.5GHz/sec in a microwave or 2.5 billion times per second. At this rate, the flipping of the water molecule creates friction, causing heat to be transferred to the surrounding nonresponsive material and thus cooking your food. About the microwave oven, an LRAD operates at a much higher energy of 80-100GHz. The microwave oven can penetrate deeper within a material because the number of molecules and the amount of power allows for this to happen. But it would never act well as a weapons system because the waves are dispersed over a relatively short distance.

However, a military, active denial system operating at a much higher power keeps the energy collimated into a beam so it can act upon the surface of an object. Therefore, with smaller energies and larger wavelengths, the energy is deposited deeply into the material, making a Microwave oven-good for cooking compared to a higher power and shorter wavelength that tends to deposit the majority of energy on the surface of a material. This is good for a weapons system where the target is the skin's surface with highly concentrated nerve endings. Also, the shorter wavelength of an LRAD can be better focused and sent further downfield.

**Figure 11.5 ADS (Active Denial System) / LRAD (Long Range Active Denial)**



Source: (ADS / LRAD, 2022)

Frequency is expressed in Hertz, one cycle every second. Microwaves are expressed as having frequencies between 300 million cycles per second (megahertz) and 300 billion cycles per second (gigahertz), making them high-frequency radio waves. Microwaves have numerous useful civil applications. For example, Radar (radio detection and ranging) uses microwaves with higher frequencies and shorter wavelengths. Their shorter wavelengths allow them to transmit them in a specific direction as a beam. They travel in a straight line until reflected by an object they encounter. For example, if directed at a plane, the radar's reflected waves detect its aircraft type, direction, and speed. Using radar allows traffic controllers at airports to direct aircraft traffic. Stealth aircraft have a low radar signature, degrading the radar's ability to detect and track the aircraft, and may appear to resemble a bird more closely on a radar screen. Stealth aircraft achieve a low radar signature by reflecting the radar beam in directions that are not detectable or by absorbing a portion of the radar beam.

## Back to Microwave Ovens

Most kitchens have a microwave oven. Microwave ovens operate at 2,450,000 cycles per second (2,450 megahertz. (Monte, 2021) Microwave ovens work by channeling the microwave beam directly at the food. The molecules composing the food absorb the beam's energy, making the fat and water molecules vibrate. This vibration causes friction, which generates heat and increases the temperature of the food. This increase in temperature cooks the food. You can look inside the microwave because the microwave door contains a plate of glass covered by a metal mesh screen. The screen reflects the microwaves because the mesh holes, too small for microwaves to escape, are large enough to allow visible light to pass through and enable you to see what's cooking inside besides these typical microwave applications, many more, including industrial applications. Let us move on to microwave weapons.

Definition of a **Microwave Weapon**: a device that damages a target by emitting focused microwaves. The critical word in this definition is "damage." (Monte, 2021)

While radar and microwave ovens focus microwaves on a target, their intent is not to damage. A critical attribute of Microwave Weapons, unlike laser weapons, is that they suffer little to no distortion by weather or atmospheric conditions. They can easily penetrate a fog. By contrast, laser weapons find it challenging to penetrate fog. High-energy microwave weapons have a long reach, typically measured tens to hundreds of miles. These weapons can damage humans, electronic systems, and fuel. (Monte, 2021) For example, the Havana Syndrome,[\[2\]](#) [\[3\]](#) Similar to the Moscow Signal, left some victims with permanent brain damage.

### Figure 11.6: US embassy in Havana, Cuba



Source: (US Embassy in Havana, Cuba, 2021)

Electronic systems exposed to a pulse of high-energy microwaves will suffer catastrophic failure, even if the electronics are off or disconnected from a power source. The microwave pulse induces surge currents in the electronic circuits, causing damage. High-energy microwaves can also damage the fuel of a missile, truck, or any other platform. The damage results when the microwaves heat the fuel to the point it explodes. (Monte, 2021) Like lasers weapons, microwave weapons will continue to function as long as they have sufficient power. Another common point is that directed-energy weapons can replace conventional weapons that use gunpowder, thus removing the need to supply and store dangerous ammunition for the replaced armament. (Monte, 2021) For example, if a bomb hits the magazine of a warship, the bomb's explosion will trigger the magazine to explode and may sink the ship. Thus, by replacing conventional weapons, directed-energy weapons can significantly improve safety.<sup>[4]</sup> (Monte, 2021)

### **U.S. Microwave Weapons Antipersonnel Microwave Weapons**

There are two types of antipersonnel microwave weapons, neurological and biological.

### **Neurological Microwave Weapons**

These weapons attack the human nervous system, typically the brain. Projecting low-frequency microwaves at humans is, by definition, a neurological microwave weapon. Although it is nonlethal, it can result in permanent brain damage. (Monte, 2021) The United States is silent about deploying or using this type of weapon; however, DARPA built one to study its effects on a monkey (in the Pandora Program). (L, 2019) Other interesting DARPA projects include the codenames Hello, Goodbye, and Good Night.

### **Hello, Goodbye, and Goodnight**

What are these DARPA projects?

“Development of the system began in the 1990s with the Air Force’s efforts to explore the biological effects of microwaves.

A project code-named **Hello** studied how to modulate the clicking or buzzing sounds produced by microwave heating in the inner ear to produce psychologically devastating ‘voices in the head.’

‘**Goodbye**’ explored the use of microwaves for crowd control. And ‘**Good Night**’ looked at whether they could be used to kill people.” (L, 2019)

### **The PANDORA Project**

“New Research Program in the US — The Pentagon wants to know more about how your body cells use electromagnetic radiations to talk to each other. A new research program will explore:

Whether electromagnetic waves are purposefully transmitted and received within or between cells and, if so, to leverage those insights not just for biosystems but also for communicating in cluttered electromagnetic environments.” (L, 2019)

Many of these ideas about cell-to-cell signaling are not new. Twenty-five years ago, Ross Adey described how cells “can whisper



together across the barrier of cell membranes.” Such messages, he believed, could control complex biological processes. Further, Adey maintained that external EM radiation could also activate, overwhelm, or muddle such processes. These are more commonly known as non-thermal effects. Back in the 1960s, Adey worked on a top-secret DARPA project called Pandora to investigate the effects of low levels of microwave radiation. (L, 2019)

The project was initiated after the U.S. government discovered that the Soviets were beaming microwaves at its embassy in Moscow. (RadioBio: DARPA To Explore Cell-to-Cell Communications, 2017)

### **Biological Microwave Weapons**

These weapons attack the body in various ways, such as causing skin irritation or the sensation of hearing loud sounds or voices. (Monte, 2021)

#### **Skin Irritation**

The U.S. military has developed and deployed a microwave weapon termed the Active Denial System. According to Phys.org, “A sensation of unbearable, sudden heat seems to come out of nowhere; this wave, a strong electromagnetic beam, is the latest non-lethal weapon unveiled by the U.S. military.” (Rabechault, 2012)

The military is intentionally not calling this a microwave weapon because it judges the average person will equate this with using a microwave oven. After conducting interviews with U.S. Marine colonel Tracy Taffola, the director of the Joint Non-Lethal Weapons Directorate, and Stephanie Miller, who measured the system's radio frequency bio-effects at the U.S. Air Force Research Laboratory, Phys.org learned the following information: The system output frequency is 95,000,000,000 cycles per second (95 gigahertz) and is superficially absorbed by the skin, leading to the target's immediate instinct to flee (hence its name, Area Denial System or ADS). Its reach, or range, is a thousand meters (0.6 miles). (Rabechault, 2012)

**Figure 11.6A Two styles of US Marine Corps trucks are seen carrying the Active Denial System, March 9th, 2012, at the US Marine Corps Base Quantico, Virginia. The non-lethal weapon projects a strong electromagnetic beam up to 1000-meters**



Source: (Rabechault, 2012)

The U.S. military considers the system its safest nonlethal capability, having exposed 1,100 people and resulting in only two people suffering injuries that required medical attention to recover fully. The U.S. military deployed it in Afghanistan in 2010 but did not use it in operation. (Monte, 2021)

### **Frey Effect Weapons**

These microwave weapons cause people to perceive they hear a sound. In 2003 WaveBand Corporation received a contract from the U.S. Navy to design a microwave weapon for military crowd control. According to New Scientist, the project transitioned to Sierra Nevada Corporation in 2008. Its product MEDUSA (Mob

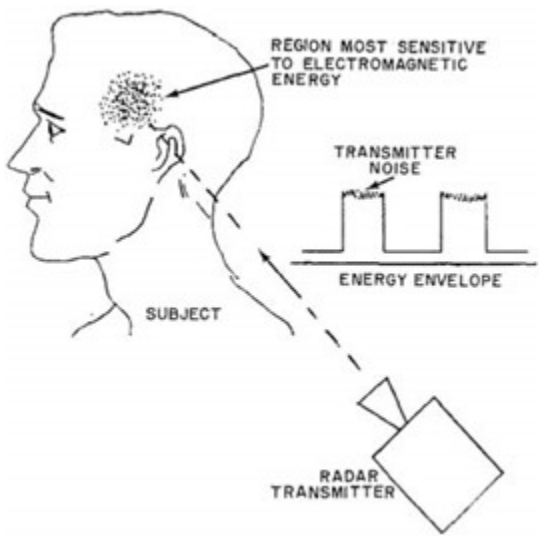
Excess Deterrent Using Silent Audio) is a microwave ray gun that causes people to perceive they hear painfully loud booms. (Hambling, microwave-ray-gun-controls-crowds-with-noise, 2008) The Living Moon reports, “MEDUSA involves a microwave auditory effect ‘loud’ enough to cause discomfort or Microwave Weapons incapacitation.” (Hambling, Microwave ray gun controls crowds with noise, 2008) Unfortunately, much like the Moscow Signal and the Havana Syndrome.

Some experts suggest MEDUSA may also cause “neural damage.” In addition to the victim’s appearing to hear noises and voices, the weapon may disrupt a person’s balance, cause fevers, and trigger epileptic-type seizures. The U.S. Army, and potentially the U.S. Secret Service, use medusa or similar technology and the technology described in another U.S. Patent. In 1996 the U.S. Air Force filed a patent for a “method and device for implementing the radio frequency hearing effect.” (USAF, 1996-12-13 applied) The patent delineated a device that would cause victims to perceive hearing voices. The U.S. Patent and Trade Office granted the patent in 2002. It works fundamentally: The inner ear has sections filled with air and fluid vulnerable to microwaves at specific frequencies. The human head acts as an antenna for microwaves. When the head receives those microwave signals, they slightly heat those inner-ear sections, causing them to expand and shift. The human body does not feel the heat or expansions, but the ear records the shifts. The ear’s design requires it to interpret the variations as sound, which is a function of the microwave frequency. (USAF, 1996-12-13 applied) Modulating the frequencies (i.e., changing the shifts in the inner ear) makes it possible to form words. (Monte, 2021) The volume at which the sound is heard is a function of the power of the microwaves. Unfortunately, a patent has to describe how the technology works sufficiently to guarantee the patentee’s intellectual property rights. This one provides insight into how to build this device. Through the Invention Secrecy Act of 1951, the

U.S. government can prevent a patent's disclosure. (Monte, 2021)

This weapon may induce mental illness or cause a person to act irrationally. Although it is a grim reality, we need to acknowledge these types of microwave weapons exist. Neurological and Frey effect weapons are extremely concerning, given that they have the potential to cause hearing sounds. Typically, hearing odd sounds or voices is a sign of mental illness. However, knowing the Frey effect microwave weapons exist, a person suffering these sensory effects may not be mentally ill but the victim of a microwave attack. (Monte, 2021)

**Figure 11.7: Frey Effect**



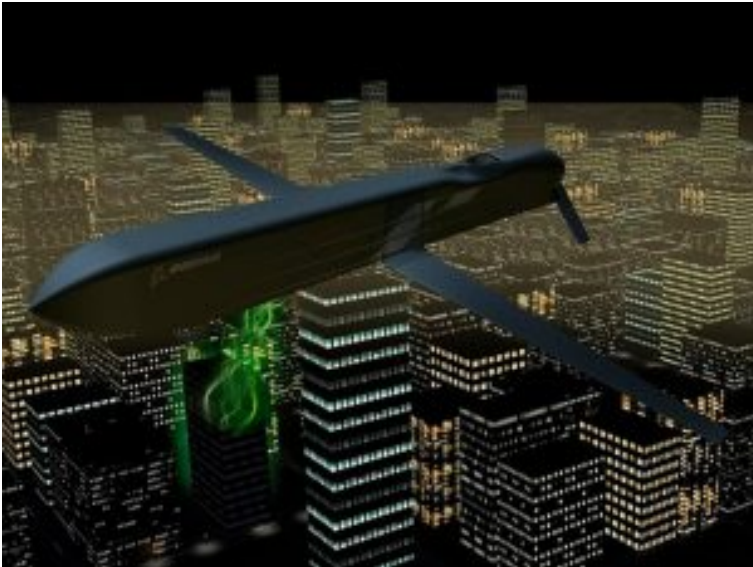
Source: (Frey Effect, 2022)

**CHAMP**

U.S. military personnel responsible for Frey effect weapons likely

also know about it. Currently, no law prohibits their use against enemy combatants or anyone else, including you. Microwaves can damage electrical and electronic systems. (Monte, 2021) On May 19, 2019, the Daily Mail published an article titled “U.S. Air Force Has Deployed 20 Missiles That Could Zap the Military Electronics of North Korea or Iran with Super Powerful Microwaves, Rendering Their Military Capabilities Virtually Useless with no collateral damage.” (U.S. Air Force-deployed-20-missiles-fry-military-electronics-North-Korea-Iran, 2019) According to the article, known as the Counter-Electronics High Power Microwave Advanced Missile Project (CHAMP), the missiles were built by Boeing’s Phantom Works for the U.S. Air Force Research Laboratory. The microwave weapons can be launched into enemy airspace at low altitudes and emit sharp pulses of high-power microwave energy that disable electronic devices targeted. Mary Lou Robinson, the High-Power Microwave Division of the Air Force Research Lab chief, has confirmed to DailyMail.com that the missiles are now operational and ready to take out any target. While North Korea or Iran may attempt to shield their equipment, U.S. officials doubt that would be effective against CHAMP.

**Figure 11.8: CHAMP**



Source: (USAF, 2019)

The project has been advancing secretly ever since the Air Force successfully tested a missile equipped with high-powered microwave energy in 2012. This report would mark a significant milestone in the deployment of microwave weapons, but the Daily Mail is usually considered a questionable source. However, there is some evidence that the report may be valid. [5] Ronald Kessler, a former Washington Post and Wall Street Journal investigative reporter wrote the article. He is also the New York Times best-selling author of *The Trump White House: Changing the Rules of the Game*. (Kessler, 2018)

Boeing's website also lists a 2016 news release describing the same weapon. Here is an excerpt: "During the test, the CHAMP missile navigated a pre-programmed flight plan and emitted bursts of high-powered energy, effectively knocking out the target's data

and electronic subsystems. CHAMP allows for selective high-frequency radio wave strikes against numerous targets during a single mission.” (Fightersweetstaff, 2016) In addition, CNN reported in 2015 that the “Air Force confirms [it has an] electromagnetic pulse weapon.” Boeing has developed a weapon that can target and destroy electronic systems in a specific building.” In the report, CNN used the phrase “Boeing ‘Lights Out’ Weapon,” which Boeing used in a press release that included interviews with Keith Coleman, the champ program manager, and Peter Finlay, the Air Force Research Laboratory’s CHAMP lead test engineer. (CNN, 2015) With CHAMP shrouded in secrecy and the U.S. Air Force silent on its deployment, we must treat the Daily Mail story with a skeptical eye. However, if this advanced missile is deployed, it is a superior electronic warfare weapon because it destroys, rather than jams, electronics. (Monte, 2021)

Jamming only temporarily affects systems, which can recover when the attack ceases. If the U.S. military were deploying CHAMP, it would be a game-changer, as these cruise missiles can be released and attack an adversary without detection. Since CHAMP is a ground-hugging cruise missile, an adversary likely would not detect it via radar. Without the necessary electronic systems to respond, an adversary would only know that its ability to counterattack was inoperable. It also might not be capable of determining the nation responsible for its mysterious power loss. CHAMP’s pulse would render an adversary’s command center useless, with its computers fried, communications salient, and lights out. *Thus, the system’s capability has the potential of rendering the mad doctrine void.*

Drone Defense Microwave Weapon Swarming tactics are a reality, and potential U.S. adversaries use them. On July 22, 2019, Iran seized two merchant vessels, a British oil tanker and an unidentified foreign oil tanker, using swarm tactics. Reuters states, “Instead of trying to match the U.S. military weapon-for-weapon, Iran deploys large numbers of relatively unsophisticated systems on land, at sea, and in the air. The idea is to overwhelm American forces, much

like a single bee is a nuisance to a human being, but a swarm of them could prove lethal.” (Monte, 2021) In 2002, the U.S. military launched the war game Millennium Challenge, the most extensive simulation ever held, involving 13,500 people. It ran from July 24 to August 15 and included live exercises and computer simulations. Its purpose was to simulate a war with Iran set in 2007. According to the New York Times, “The upshot was that the enemy ‘sank’ much of the American fleet as the exercise opened.” Given the might and sophistication of the U.S. Navy, it is reasonable to question how this is possible. The answer is one word, swarming! In the war game, Iranian forces deployed swarms of speedboats armed with cruise missiles, rockets, torpedoes, sea mines, machine guns, and shoulder-fired surface-to-air missiles. (Monte, 2021) In addition, the Iranians deployed shore-based missiles also le of swarming the U.S. fleet. To the surprise of the war game’s participants, the swarming was effective and inflicted significant damage to U.S. Navy warships. The U.S. military uses these war games to test equipment and concepts. (Monte, 2021) The U.S. Navy’s goal is to make these vessels more lethal. In addition to conventional armaments, it appears to be leaning toward directed energy weapons. While the navy is finding lasers are effective against speedboats, Raytheon’s advanced high-power microwave system is proving itself a more effective drone killer. In 2018, according to the company’s website, “Raytheon’s high-power microwave system engaged multiple UAV [unmanned aerial vehicle] swarms, downing 33 drones, two and three at a time.” (Monte, 2021) (Raytheon, 2018). The Microwave beam disrupts the drone’s guidance system and can attack the entire swarm, downing multiple drones at a time. In the same test, Raytheon’s high-energy laser system proved lethal against drones but zapped them simultaneously. Microwave Weapons While the navy is still testing to determine how it will arm its littoral combat ships, directed-energy weapons appear to be in the running. For example, in 2020, the navy stated it would begin testing the effectiveness of laser weapons aboard them. Microwave weapons are far less sensitive to atmospheric disturbances than lasers,



making them a more robust all-weather weapon. Microwave weapons appear better suited than lasers against drone swarm attacks. In combination, they would remove the need for the Phalanx machine gun, the U.S. Navy's close-in weapon system that serves as a last-ditch defense against missiles and uses gunpowder, potential liability a, and the use of short to intermediate-range missiles against drones and missiles. Laser and microwave weapons also provide a low-cost, unlimited, and continual defense against missile, drone, and speedboat swarms; short- to intermediate-range missiles do not. The most crucial phrase in the last sentence is "low cost, unlimited, and continual." As long as the navy supplies power to these directed-energy weapons, they will continue to work, and a typical laser shot costs about a dollar. By contrast, short- to intermediate-range missiles are expensive, typically costing hundreds of thousands of dollars, and a warship can only carry a finite number of them. (Monte, 2021) Let us now examine the microwave weapons of two of the United States' potential adversaries, Russia and China.

### **Russian Microwave Weapons**

Russia has probably developed a low-frequency microwave weapon. It is also likely the Russians used it against U.S. Embassy staff in Moscow (1953), Cuba (2017), and China (2018). They do not claim to have such a weapon, but significant evidence says they do. In 2009 Russia and Cuba signed a strategic partnership alliance to expand cooperation in agriculture, manufacturing, science, and tourism. While there were no public statements regarding their rekindling of Cold War-era military ties, Russia needed military allies, and Cuba needed financial help. Cuba is also conveniently located only about a hundred miles from Florida. These points suggest Russia and Cuba would secretly engage in a military alliance. As noted previously, the Cuban government, armed with a Russian microwave weapon, possibly perpetrated the attack on the U.S. Embassy personnel in Havana. Russia's ties to Cuba and China may have enabled it to trade this microwave weapon for

the secret information about the United States gained through the weapon's use. Russia is aware that the United States is developing microwave weapons. However, the Russian economy and its corrupt government may hamper its indigenous development of high-power microwave weapons through either espionage or its relationship with the Chinese, whose history demonstrates an ability to hack U.S. military secrets. "Russia has just announced their creation of a microwave gun to knock drones and warhead missiles out of the air from 10 kilometers [about six miles] away!"<sup>[6]</sup> In typical Russian fashion, the details of the weapon remain secret. Officials reportedly scheduled a private weapon demonstration during the Russian Defense Ministry's Army-2015 expo. Suppose Russia's claims are valid, according to Military & Aerospace Electronics. It could "complicate U.S. military strategic planning, which has relied heavily on precision-guided munitions, GPS navigation, and tactical battlefield networking for the past quarter-century." While Russia exaggerates its new weapons' capabilities, this report is four years old. Russia could have engineered it to be a potent microwave weapon even with typical development issues. According to a 2010 research report by Robert J. Capozzella, "As for the anti-aircraft systems, Russia is researching and trying to sell the Ranets-E and Rosa-E. The first is a point defense system designed to target the electronics of modern aircraft; the second is a defensive aircraft system that targets enemy aircraft radar. however, these are still in development based on the advertised beam output; [sic] their range is promising against unshielded systems but otherwise limited." (Capozzella, 2010) As part of the sale, Russia requires additional development investment from the buyer, but the Russian military leadership intends to build and sell microwave weapons. Capozzella's report is more than a decade old as of his writing. Meanwhile, the Russians may have secured the necessary development funding and perfected these weapons. Unfortunately, Russia's "iron curtain" still hides secrets from the free world. Its leadership momentum in nuclear weapons lasted only four years

against the Soviet Union, which detonated its first atomic weapon in 1949. (Monte, 2021) (Capozzella, 2010)

### **Chinese Microwave Weapons**

China is actively building microwave weapons that appear identical to the U.S. military's champ and Active Denial System.

Rather than keeping these weapons secret, the Chinese are touting their capabilities. Let us examine these weapons. China's CHAMP, like Microwave Weapon: According to a Popular Science report in 2017, "For over six years, Huasixg Wenhua and his team at the Northwest Institute of Nuclear Technology in Xi'an have been working on a potent microwave weapon. This one, which recently won China's National Science and Technology Progress Award, is small enough to fit on a workbench, making it theoretically portable enough for land vehicles and aircraft." (Singer, 2017) China's leadership believes that directed-energy weapons will dominate warfare by midcentury, fueling this investment level. China's Microwave Active Denial System (CMADS): This system appears identical to the U.S. Active Denial System, even sharing its name. According to the state-run Chinese tabloid Global Times, "China is developing a non-lethal weapon system based on microwave radar technology. (Perwakilan Press, 2019) The project's chief engineer said it improves the country's counter-terrorist and land and maritime border defense capabilities. [It is] officially named Microwave Active Denial System, works by shooting millimeter microwaves at targets, which can cause the pain nerve under the skin to ache in a bid to effectively halt the objective's [a person's] violent actions and disperse targets [crowds]." (Perwakilan Press, 2019)

Radiation-Hardened Electronics and System Shielding Nuclear weapons can create high radiation environments. Those environments give rise to electromagnetic radiation, which can fry electronics. Since U.S. military hardware must work in high radiation environments, such as in outer space or during a nuclear

detonation, the electronics must be hardened, and the cables shielded. The phrase “radiation-hardened systems” typically means the entire system is radiation-resistant. This level of radiation resistance requires the electronics to be radiation tolerant or shielded, and that shielding must also protect the interconnections. If any portion of the system is vulnerable, it may lead to a catastrophic failure. For example, during a microwave or EMP event, even one interconnection without shielding can send high electrical surges throughout the entire system. Radiation-hardened electronics are components whose design and manufacture allow them to withstand high radiation environments, such as those found in outer space or nuclear environments. Again, though, the radiation levels and the duration of exposure to which they were exposed are classified. Honeywell’s Solid-State Electronics Center was one of the few integrated circuit foundries in the United States capable of producing radiation-hardened electronics. These integrated circuits are challenging to design and produce. Their cost reflects that difficulty. Another essential way to protect electronics and interconnections is by shielding, which typically involves using metals to form a Faraday cage or a continuous metal enclosure.

A Faraday cage makes it difficult, but not impossible, for microwave or EMP to penetrate its interior. Therefore, putting your smartphone in a metal can will provide some shielding from an EMP. How militaries shield their systems is, in practice, complex. Various materials can absorb radiation or reflect it. Military system designers also have to balance weight restrictions versus radiation protection. For example, while lead is generally an excellent radiation shield, its weight makes it challenging to use for space applications. Launching heavy satellites into space is extremely difficult. (Monte, 2021)

Unmanned aerial vehicles (UAVs) are integral to how business and people conduct their daily operations and lives. Such things as providing images, deliver and needed medicines to remote areas,

and military support from intelligence gathering and tactical battlefield weapons. They are effective at providing defense systems previously unavailable on the battlefield. Unmanned aircraft, low cost, have become a serious hazard worldwide if used maliciously. Even with strict limitations on the commercial use of unmanned aerial systems, savvy criminals can be a huge threat in protected airspace. They can disrupt air traffic. In U.S. airspace alone, the Federal Aviation Administration receives more than 100 reports of drone incidents each month. (Mayser, 2021)

### **DETECTING AND DISABLING DRONES**

To effectively counter the threat, early warning is critical. Most commercial counter unmanned aerial vehicle (CUAV) systems can block the radio link between the remote-control transmitter and the drone receiver to prevent the aerial vehicle from penetrating a no-fly zone; to do so, they must disable the radio communication. (Nichols & al., 2020) Finding the UAV to protect against is important. Enhanced CUAV technology can detect commercial drone activity and automatically classify the type of drone signal. It can determine the drone's direction and its pilot and, on command, disrupt the radio control link to prevent the drone from reaching its target. (Nichols & al., 2020) (Mayser, 2021)

Drones are controlled with an uplink signal from the remote control to the drone using the frequency hopping spread spectrum (FHSS). WLAN is used as a standard for control also. Signals transmitted to the drone's ground (i.e., the downlink) are typically FHSS, wideband or WLAN signals. (Mayser, 2021) To detect the drone's radio communications (RC) signals, highly sensitive antennas and monitoring receivers are needed. Under ideal conditions, commercial off-the-shelf RCs can be detected up to 7 km and 5 km for drones such as the DJI Phantom 4. (Mayser, 2021)

**Figure 11.9 DJI Phantom 4**



Source: (DJI Phantom 4, 2022)

CUAV systems use radars sensors for detection and require line-of-sight (LOS) to the drone. Other sensors, such as acoustic, are limited by range and environmental factors. Monitoring the RC links is the only method that enables a drone to be detected when switched on. RC activity can be recognized even before a drone takes off, as drones require preflight checks. During this time, the RC is active and can be detected. With this early warning, CUAV systems using RC monitoring provide a key advantage to any multi-sensor CUAV system – more time to react. Also, determining the drone pilot's location from the RC signal enables security personnel to deploy quickly, with a greater chance of finding and apprehending the pilot. (Mayser, 2021) (Nichols & al., 2020)

## **DRONE DETECTION RADAR**

### **Figure 11.10: Analyzing a Radar Pulse Using an R&S Spectrum Analyzer**



Source: (Image Analyzing a Radar Pulse Using an R&S Spectrum Analyzer, 2021)

Because of a drone's small size, low altitude, and slow speed, reliably detecting it is a challenge for radar. Radar sensors must quickly scan large volumes with great sensitivity, eliminate nuisance alarms such as birds and reliably discriminate UAVs from ground targets (see Figure 11.10). When designing a drone detection radar, the key design considerations are:

- Radar operating frequency
- Scan coverage and response time
- Resolution and environmental considerations
- Classification capability.

The operating frequency is determined by considering propagation efficiency, the scanned terrain, environment, desired detection range, and minimum detectable radar cross-section. With many applications requiring 360-degree azimuth coverage, the scanning requirements range from monitoring large spatial volumes with

high refresh rates to illuminating contacts to classify and initiate countermeasures. Further classification using secondary sensors such as optical or audio requires accurate information regarding range, bearing, and height, which often demands complex 3D capabilities. To determine the performance requirements for the component, module, or subsystem, the appropriate solutions should cover all relevant measurements for power output, antenna pattern, spectral emission mask, interface performance, and the phase noise of phased-locked loops in the microwave signal generator. (Mayser, 2021) (Nichols & Mumm, 2019)

### **DETECTING DRONES USING RC**

To detect FHSS-controlled drones using their RC signals, the CUAV system should compare measured signals with a library of drone profiles. With automatic online hopper analysis, the system can identify signal parameters such as hop length, symbol rate, and modulation type, which enables classifying the drone. The CUAV system can force the drone to safely fail by disrupting the control signal with a “smart,” adaptive, low-power countermeasure. (Mayser, 2021) A wideband smart exciter can selectively jam only the detected FHSS signals and disrupt the drone’s uplink. With WLAN-controlled drones, an RC-based CUAV system using sectorial WLAN antennas for directional information can disrupt the WLAN link between the remote control and the drone. (Mayser, 2021) (Nichols & al., 2020) (Nichols & Mumm, 2019)

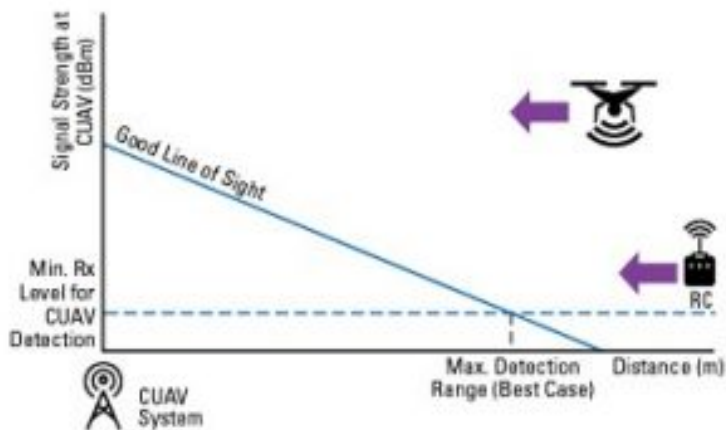
Other CUAV solutions use a barrage jammer, spreading power over the complete frequency band. This requires high output power and disrupts all active transmissions in the frequency band, not only the control signal for the drone.

In addition to detecting and jamming the drone, the CUAV system should provide direction-finding information: the operator’s direction from the direction of the RC uplink signal and the drone’s direction from the telemetry or video downlink signal.

### **DETECTION AND JAMMING RANGES**

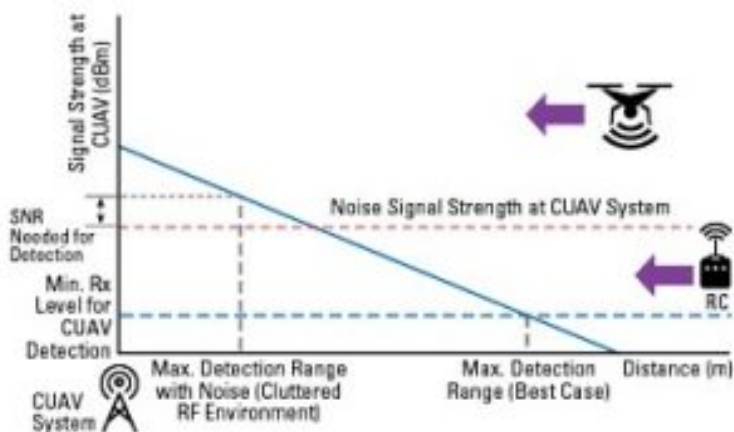
**Figure 11.11: Theoretical Detection Range Without Noise**





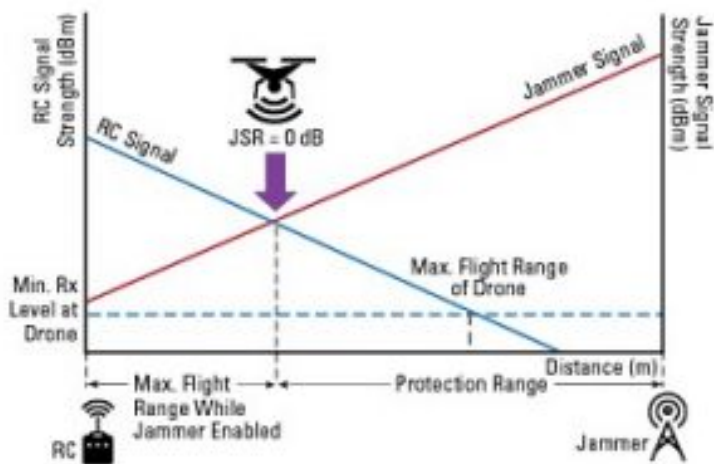
Source: (Image- Theoretical Detection Range Without Noise, 2021)

**Figure 11.12: Theoretical Detection Range With Noise, e.g., In An Urban Environment**



Source: (Image -Theoretical Detection Range With Noise, e.g., In An Urban Environment., 2021)

**Figure 11.13: Theoretical jamming range**

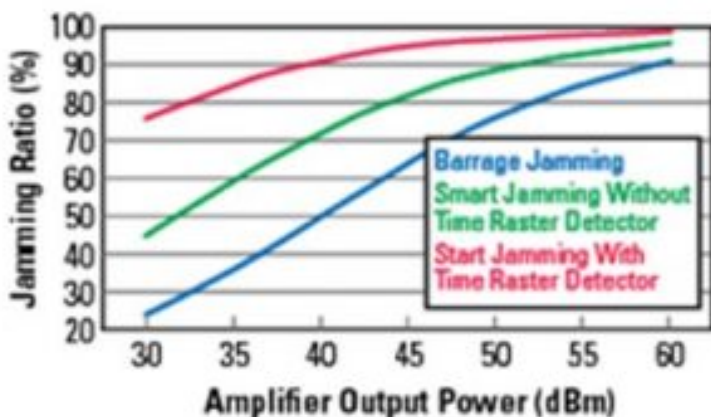


Source: (Image – Theoretical Jamming Range, 2021)

For drone detection, the received RC signal strength at the CUAV receiver must be equal to or greater than the receiver (Rx) sensitivity or minimum signal-to-noise ratio (SNR), i.e., the minimum level. The SNR depends on the actual RF environment and changes continuously. A cluttered RF environment, for example, will reduce the detection range. To classify the drone type, a minimum Rx level must be received by the CUAV receiver. This minimum level is specific to the type of drone and depends on the FHSS modulation of the RC signal and the overall noise perceived by the detector. Figure 11.11 illustrates the maximum detection range in an environment with minimal noise. The detection range is substantially reduced in an electromagnetically noisy environment like a city (see Figure 11.12). (Mayser, 2021)

A drone is controllable when the RC signal strength at the drone receiver is greater than the minimum Rx level. If a jamming signal is also present and greater than the RC signal power at the drone – when the jamming-to-signal ratio (JSR) is  $\geq 0$  dB – the drone is typically no longer controllable by the pilot. However, this depends on the coding scheme of the remote control (see Figure 11.13). The greater the JSR, the higher the probability the CUAV can disable the drone.

**Figure 11.14: Jamming ratio for CE-compliant remote control operating in the 2.4GHz ISM band**



Source: (Image -Jamming ratio for CE-compliant remote control operating in the 2.4GHz ISM band, 2021)

Figure 11.14 illustrates a jamming test using a CE-compliant remote-controlled drone with the uplink in the 2.4 GHz band. The jammer uses a power amplifier connected to a Rohde & Schwarz UHF omnidirectional antenna with a 10 m cable. Three types of jamming signals were evaluated: barrage jamming, smart jamming without a time raster detector, and smart jamming with a time raster detector. The plot shows the jamming ratio versus amplifier output power for the three scenarios, showing smart jamming is more effective than barrage jamming. (Mayser, 2021)

CUAV manufacturers often claim long ranges and precise jamming distances; however, these figures are not precise. The jamming range will depend on the ratio of the jammer signal strength to the RC uplink signal strength at the drone, i.e., the JSR. (Nichols & al., 2020) Under realistic conditions, field trials have repeatedly shown the range claims of CUAV system suppliers are often not verifiable. Ironically, the performance of systems claiming relatively short ranges, such as 2 km, is often similar to systems claiming

longer ranges, such as 15 km. What is a realistic detection range? In some scenarios, systems will achieve very long detection ranges, usually the values shown in the technical specifications of CUAV systems. Yet these “best case” circumstances do not represent the performance in typical rural or urban deployments. Environmental conditions, such as RF noise or the relative permittivity of the ground, influence detection and jamming ranges. The environment changes constantly, and the measured detection and jamming ranges will often vary with every measurement. (Nichols & al., 2020) (Mayser, 2021)

To achieve exceptionally long detection ranges, the Rx antenna of the CUAV system should be elevated, and the terrain between the CUAV Rx antenna and the RC Tx antenna should have low relative permittivity, such as a freshwater lake at 0°C water temperature. The first, second, and third Fresnel zones should be free of obstacles, and the RF environment should have low noise – thermal and other transmitters. The RC signal frequency should be in a low-frequency band, the signal should have high output power, and the antenna cables should be short. Choosing antennas with higher directionality will increase the antenna gain. (Mayser, 2021)

## **DEPLOYING CUAV SYSTEMS**

As CUAV systems depend on the application environment, they must be adapted to each scenario to achieve the optimum detection and jamming ranges. The distance ranges published by manufacturers only indicate how to optimize the CUAV system for the application. (Mayser, 2021) (Nichols & Mumm, 2019)

Under optimized conditions, the R&S ARDRONIS CUAV system can detect an RC signal 7 km. Detection ranges measured in urban or rural environments are shorter because of lower SNR, non-optimized antenna sites, and other factors. Table 11.1 shows several environments and the typical ranges in the ARDRONIS system that can detect a CE-compliant RC output signal at 2.4 GHz, comparing urban, rural, and low noise environments with LOS and non-LOS between the drone and CUAV. The R&S ARDRONIS system uses

a wideband smart exciter to jam remote-controlled transmission, using an FHSS signal matching the detected type of drone signal. Its jamming range will depend on the remote control's output power and the system's detection range (see Table 11.2). (Mayser, 2021)

**Table 11.1 Shows Several Environments and the Typical Ranges  
In The ARDRONIS System**

| <b>TABLE 1</b><br><b>TYPICAL DETECTION RANGES</b><br><b>(CE-COMPLIANT OUTPUT POWER AT 2.4 GHz)</b> |                   |
|--|-------------------|
| <i>Environment</i>   | <i>Range (km)</i> |
| Urban, LOS   | 0.2–0.8           |
| Urban, NLOS  | ≤ 0.1             |
| Rural, LOS   | 1.0–1.5           |
| Rural, NLOS  | ≤ 0.4             |
| Low Radio Noise, LOS   | 4–7               |
| Low Radio Noise, NLOS  | ≤ 0.5             |

Source: {Table 1} Courtesy of (Mayser, 2021)

**Table 11.2 Typical Jamming Ranges**

| <b>TABLE 2</b><br><b>TYPICAL JAMMING RANGE</b> |                       |                                      |   |
|--|-----------------------|--------------------------------------|---|
| <i>Remote Control Compliance</i>               | <i>Frequency Band</i> | <i>Max Remote Control EIRP (dBm)</i> | <i>Jamming Range (% of Detection Range)</i> |
| CE (Europe)                                    | 2.4                   | 20                                   | 67  |
|  | 5.8                   | 14                                   | 84  |
| FCC (U.S.)                                     | 2.4                   | 26                                   | 50  |
|  | 5.8                   | 26                                   | 50  |
| SRCC (China)                                   | 2.4                   | 20                                   | 67  |
|  | 5.8                   | 26                                   | 50  |

Source: {Table 2 } Courtesy of (Mayser, 2021)

Determining what detection and jamming ranges are acceptable for a specific application depends on the following considerations:

- What time is needed from detection to reaction? The earlier a drone is detected, the more time for reaction.
- After detecting a drone, what action is required? Activating a jammer is very fast. However, finding and apprehending the pilot with security personnel will take more time.

The longer the required early warning time, the more important short detection and jamming become. (Mayser, 2021)

**CONCLUSIONS**

From popcorn to crowd control, from aircraft detection to CUAVs,

Microwaves play an important part in each of these areas of modern society in their function and protection or its destruction. All CUAV systems are subject to the laws of physics. The detection range is determined by the relative location of the RC and CUAV system, the Tx power of the RC, and the physical and RF environments. The jamming range is determined by the relative location of the drone and CUAV system, the Tx power of the jammer, and, again, the environment. The required detection and jamming ranges depend on the application scenario for the CUAV system. Proper planning for each scenario is necessary before the CUAV system can be defined and deployed. (Mayser, 2021)

### **Managing Editor's OPINION**

It is clear that sUAS – moderate UAS may not be useful to deliver Microwave based weapon systems. Limitations on weight, speed, cost, power, and maneuverability are negatives. Our discussion of the USA, Russian, and previous Chinese PUBLIC / OPEN research suggests that large UAS capable of extended distances, heavy payloads, and survivability with stealth-based protections may be feasible to deploy Microwave weapons. Effective Microwave defenses against SWARMS exist from ground-based systems. (Nichols & al., 2020) However, much of the research on UAS and the ability to deliver Microwave weaponry is CLASSIFIED and not available for OPEN / Public publication. For the time being, Microwave UAS weapons delivered by small or moderate-sized drones remain in the land of conjecture and popular science fiction.

[7]

### **Bibliography**

ADS / LRAD. (2022, April 17). Retrieved from <http://terasense.com>: <http://terasense.com/wp-content/uploads/2019/05/ADS-1.jpg>

Capozzella, L. R. (2010, Feb 17). HIGH POWER MICROWAVES ON



THE FUTURE BATTLEFIELD: IMPLICATIONS FOR U.S. DEFENSE.  
Retrieved from [www.airuniversity.af.edu:  
https://www.airuniversity.af.edu/Portals/10/CSAT/documents/  
researchpapers/2010/bh2010\\_capozzella.pdf](http://www.airuniversity.af.edu:https://www.airuniversity.af.edu/Portals/10/CSAT/documents/researchpapers/2010/bh2010_capozzella.pdf)

CNN. (2015, May 25). *boeing-electromagnetic-pulse-weapon*.  
Retrieved from [www.cnn.com/videos/](http://www.cnn.com/videos/): [https://www.cnn.com/  
videos/us/2015/05/25/orig-boeing-electromagnetic-pulse-  
weapon.cnn](https://www.cnn.com/videos/us/2015/05/25/orig-boeing-electromagnetic-pulse-weapon.cnn)

DJI Phantom 4 . (2022, April 18). Retrieved from  
[https://images.unsplash.com/  
photo-1599336599646-2889f61b2349?ixlib=rb-1.2.1&ixid=MnwxMjA  
3fDB8MHxwaG90by1wYWdlfHx8fGVufDB8fHx8&auto=format&fit=  
crop&w=1170&q=80: https://images.unsplash.com/  
photo-1599336599646-2889f61b2349?ixlib=rb-1.2.1&ixid=MnwxMjA  
3fDB8MHxwaG90by1wYWdlfHx8fGVufDB8fHx8&auto=format&fit=  
crop&w=1170&q=80](https://images.unsplash.com/photo-1599336599646-2889f61b2349?ixlib=rb-1.2.1&ixid=MnwxMjA3fDB8MHxwaG90by1wYWdlfHx8fGVufDB8fHx8&auto=format&fit=crop&w=1170&q=80:https://images.unsplash.com/photo-1599336599646-2889f61b2349?ixlib=rb-1.2.1&ixid=MnwxMjA3fDB8MHxwaG90by1wYWdlfHx8fGVufDB8fHx8&auto=format&fit=crop&w=1170&q=80)

Fightersweetstaff. (2016, December 22). *boeings-champ-missile-literally-knocks-lights/*. Retrieved from [sofrep.com:  
https://sofrep.com/fightersweep/boeings-champ-missile-  
literally-knocks-lights/](http://sofrep.com:https://sofrep.com/fightersweep/boeings-champ-missile-literally-knocks-lights/)

Frey Effect. (2022, April 18). Retrieved from [samim.io:  
https://samim.io/static/upload/akwjdawd.jpeg](http://samim.io:https://samim.io/static/upload/akwjdawd.jpeg)

Hambling, D. (2008, July). *Microwave ray gun controls crowds with noise*. Retrieved from [thelivingmoon.com:  
http://thelivingmoon.com/45jack\\_files/03files/  
MEDUSA\\_Ray\\_Gun\\_.html](http://thelivingmoon.com:theivingmoon.com:https://thelivingmoon.com/45jack_files/03files/MEDUSA_Ray_Gun_.html)

Hambling, D. (2008, July 3). *microwave-ray-gun-controls-crowds-with-noise*. Retrieved from [www.newscientist.com:  
https://www.newscientist.com/article/dn14250-microwave-ray-  
gun-controls-crowds-with-noise/](http://www.newscientist.com:https://www.newscientist.com/article/dn14250-microwave-ray-gun-controls-crowds-with-noise/)

*Image – Theoretical Jamming Range*. (2021, June 6). Retrieved from [www.microwavejournal.com: https://www.microwavejournal.com/  
ext/resources/images/Figures/2021/Jun/6M29S/f4.jpg](http://www.microwavejournal.com:https://www.microwavejournal.com/ext/resources/images/Figures/2021/Jun/6M29S/f4.jpg)

*Image Analyzing a Radar Pulse Using an R&S Spectrum Analyzer*.  
(2021, Jun 6). Retrieved from [www.microwavejournal.com:](http://www.microwavejournal.com:)

<https://www.microwavejournal.com/ext/resources/images/Figures/2021/Jun/6M29S/f1.jpg>

Image -Jamming ration for CE-compliant remote control operating in the 2.4GHz ISM band. (2021, June 6). Retrieved from [www.microwavejournal.com/](https://www.microwavejournal.com/):

<https://www.microwavejournal.com/ext/resources/images/Figures/2021/Jun/6M29S/f5.jpg>

Image -Theoretical Detection Range With Noise, e.g., In An Urban Environment. (2021, June 6). Retrieved from [www.microwavejournal.com](https://www.microwavejournal.com/): <https://www.microwavejournal.com/ext/resources/images/Figures/2021/Jun/6M29S/f3.jpg>

Image- Theoretical Detection Range Without Noise. (2021, June 6). Retrieved from [www.microwavejournal.com](https://www.microwavejournal.com/): <https://www.microwavejournal.com/ext/resources/images/Figures/2021/Jun/6M29S/f2.jpg>

Kessler, R. (2018). *Changing the Rules of the Game*. Washington: Random House.

1. (2019, Feb 22). *two-years-ago-darpa-to-resurrect-top-secret-pandora-project*. Retrieved from [inteltoday.org](https://inteltoday.org/): <https://inteltoday.org/2019/02/22/two-years-ago-darpa-to-resurrect-top-secret-pandora-project/>

Mai, R. (n.d.). *Images. CBRNECy Weapons Deployed from Drones*. KSU, Manhattan, KS.

Mayser, T. W. (2021). *Adapting Counter-UAV Systems to the Environment*. *Microwave Journal*, 1. Retrieved from <https://www.microwavejournal.com/articles/36134-adapting-counter-uav-systems-to-the-environment>

Monte, L. A. (2021). *War at the Speed of Light*. Lincoln: Potomac Books. Retrieved from ProQuest Ebook Central, <http://ebookcentral.proquest.com/lib/ksu/detail.action?docID=6460626>

Nichols, R. K., & Mumm, H. C. (2019). *Unmanned Aircraft Systems*

in the Cyber Domain, 2nd Edition. Manhattan, KS: [www.newprairiepress.org/ebooks/27](http://www.newprairiepress.org/ebooks/27).

Nichols, R., & al., e. (2020). *Counter Unmanned Aircraft Systems Technologies and Operations*. Manhattan, KS: new prairie press #31.

Nielsen, P. E. (2022). *Effects of Directed Energy Weapons*. The USA. Perwakilan Press. (2019, Feb 22). *china-develops-non-lethal-microwave-radar-weapon-global-times*. Retrieved from [perwakilan.co.uk](https://perwakilan.co.uk): <https://perwakilan.co.uk/2019/02/china-develops-non-lethal-microwave-radar-weapon-global-times>

Rabechault, M. (2012, March 11). *military-unveils-non-lethal-ray-weapon*. Retrieved from [phys.org/news/](https://phys.org/news/): <https://phys.org/news/2012-03-military-unveils-non-lethal-ray-weapon.html>

RadioBio: DARPA To Explore Cell-to-Cell Communications. (2017, Feb 16). Retrieved from <https://microwavenews.com/news-center/darpa-radiobio>: <https://microwavenews.com/news-center/darpa-radiobio>

Raytheon. (2018, March 20). *High-power-microwaves-and-lasers-defeat-multiple-drones-during-US-Army-exercise*. Retrieved from [raytheon.mediaroom.com](https://raytheon.mediaroom.com): <https://raytheon.mediaroom.com/2018-03-20-High-power-microwaves-and-lasers-defeat-multiple-drones-during-US-Army-exercise>

Singer, J. L. (2017, Jan 27). *China's new microwave weapon can disable missiles and paralyze tanks*. Retrieved from [www.popsci.com](http://www.popsci.com): <https://www.popsci.com/china-microwave-weapon-electronic-warfare/>

U.S. Air Force-deployed-20-missiles-fry-military-electronics-North-Korea-Iran. (2019, May 16). Retrieved from [www.dailymail.co.uk/news](http://www.dailymail.co.uk/news): <https://www.dailymail.co.uk/news/article-7037549/Air-Force-deployed-20-missiles-fry-military-electronics-North-Korea-Iran.html>

US Embassy in Havana, Cuba. (2021, November). Retrieved from [www.aljazeera.com](http://www.aljazeera.com): Source: <https://www.aljazeera.com/wp-content/uploads/2021/11/>

[GettyImages-855674196-1.jpg?resize=770%2C513](https://www.gettyimages.com/detail/photo/usa-12-13-applied-2016-12-13-expired-method-and-device-855674196-1.jpg?resize=770%2C513)

USAF. (1996-12-13 applied, 2016-12-13 expired). *Method and device*

*for implementing the radio frequency hearing effect.* Retrieved from [patents.google.com/patent/US6470214B1/en](https://patents.google.com/patent/US6470214B1/en):

<https://patents.google.com/patent/US6470214B1/en>

USAF. (2019, May). USA\_high-power\_microwaves\_missiles\_that\_destroys\_electronics\_not\_buildings. Retrieved from [www.airrecognition.com:https://www.airrecognition.com/images/stories/news/2019/may/USA\\_high-power\\_microwaves\\_missiles\\_that\\_destroys\\_electronics\\_not\\_buildings.jpg](https://www.airrecognition.com/images/stories/news/2019/may/USA_high-power_microwaves_missiles_that_destroys_electronics_not_buildings.jpg)

## Endnotes

[1] LRAD long-range acoustic devices are covered in Chapter 13.

[2] The Havana Syndrome is also covered under Chapter 13 as an acoustic phenomenon. The mechanisms behind the Syndrome are not fully understood but caused severe damage to US diplomats at the embassy. “Quick Analysis — If the facts are confirmed, and if a physical device indeed causes the effects, I find the microwave explanation far more likely than a sonic attack; for many reasons.” If this is indeed the case, I expect to hear nothing further in the future because the truth would send a wave of panic in the Telecom sector.”

[3] For the record — The expression “Havana Syndrome” was coined by Dr. Ludwig De Braeckeleer and appeared for the first time in a story published by the Intel Today blog on October 3, 2017. (L, 2019)

[4] This is a military argument. Terrorists have a completely different view. Safety and finances are not a concern. Expedient Damage is. “ (L, 2019)

[5] Author opinion

[6] The source is INSTAGRAM and considered unreliable/unverifiable – almost as bad as TWITTER for disinformation. (Capozzella, 2010) report pdf is verified.

[7] The Last paragraph is the opinion of the Managing Editor- ONLY.

# 12. Hypersonic Drone Missiles

**By William Slofer, JR, Wilmington University**

## **Student Objectives**

- Understand the differences between subsonic, supersonic, and hypersonic
- Further understanding of differences in population systems and the need for Scramjet technology to achieve and maintain hypersonic speeds.
- Obtain appreciation for the relationship between speed and distance and why hypersonic devices are a military concern
- Gain an appreciation of the technical considerations to create such weapons how such weapons require changes to existing strategies

## **The Speed Spectrum**

Since the time of flight, humans have strived to travel faster and further. With the development of stronger and lighter materials and more powerful engines, humans can now travel into space and beyond the reaches of the solar system at speeds never before imagined. This age has seen the coming of flight from non-powered to propeller-driven flight, oxygen-consuming turbines, to rocket engines hurling spacecraft across the expanse of space. In addition to allowing man-made objects to travel past the bounds of the solar system, this increase in speed has ushered in a new era of super-fast missiles and devices known as hypersonic weapons. This evolution of weaponry is changing the paradigm of how such devices are created, launched, controlled, detected, and defended against. This

technology will alter how technicians, strategists, and diplomats will view their existing doctrines, policies, and strategies and the need to revise offensive and defensive approaches to address this disruptive technology.

To appreciate the concept of hypersonic speed, it is necessary to understand various parts of the speed spectrum and how they relate to the speed of sound. Two fairly common examples of speed notated speed are:

- 1) The speed of light or light-speed, indicated by light-years or approximately 670,616,629 miles per hour in a vacuum (NASA, 2019)
- 2) The speed of sound, which is denoted Mach speed.

These are short-hand notations to identify an object between any two points. The speed of sound, or Mach 1, will be the baseline for the speed of sound calculated by the formula.

$$V_s = 643.855 \times (T/273.15)^{0.5}$$

**Equation 12.1**

where:

$V_s$  = Velocity of Sound (Knots)

$T$  = temperature (Kelvin)

643.855 = Calculated speed of sound (N.O.A.A., (n.d.))

In general terms, “On Earth, the speed of sound at sea level — assuming an air temperature of 59 degrees Fahrenheit (15 degrees Celsius) — is 761.2 mph (1,225 km/h).” (Science Daily, 2021)

The generally accepted speed spectrums for aeronautics are categorized into three major groupings: Subsonic, Supersonic, and Hypersonic. These categories are all relative to the speed of sound,

also known as Mach 1 or approximately 761.2 mph, depending on temperature and pressure. To provide additional perspective, the table below identifies the types of aircraft that operate within the various parts of the sound spectrum and the approximate speeds ranges:

**Table 12.1**  
**Comparison of the various aircraft & speed ranges in the sound spectrum**

|                                    |                    |
|------------------------------------|--------------------|
| <b><u>Subsonic</u></b>             |                    |
| Helicopters                        | 550 – 580 mph      |
| General Aviation                   | 550 – 580 mph      |
| Commercial A/C                     | 550 – 580 mph      |
| <b><u>Supersonic</u></b>           |                    |
| Fighter jets<br>(Mach 2.5+)        | 1,453 – 2,500 mph  |
| <b><u>Hypersonic</u></b>           |                    |
| X-15, Space Shuttle                | 3,806 mph (Mach 5) |
| – 17,500+ Mach 25+                 |                    |
| Manned space capsules (on reentry) | 3,806 mph (Mach 5) |
| – 17,500+ Mach 25+                 |                    |

Sources: (Aero Corner, 2021) (Smithsonian National Air and Space Museum, 2022)

**Subsonic**  
They are aircraft types most people are familiar with and are used for general recreation and commercial transportation. This would include small aircraft such as Piper, Cessna, Beechcraft, Boeing, Airbus, and Embraer. These aircraft travel at speeds under Mach 1.

**Supersonic**  
Most aircraft are military or research types, other than a few commercial airliners, such as the Concorde and Tupolev TU-144. These aircraft typically fly at speeds up to and including 2,500 mph. And have serious physical demands on pilots when performing extreme maneuvers. At these speeds, usually in excess of Mach 2, human physiology becomes the weak link in the system.

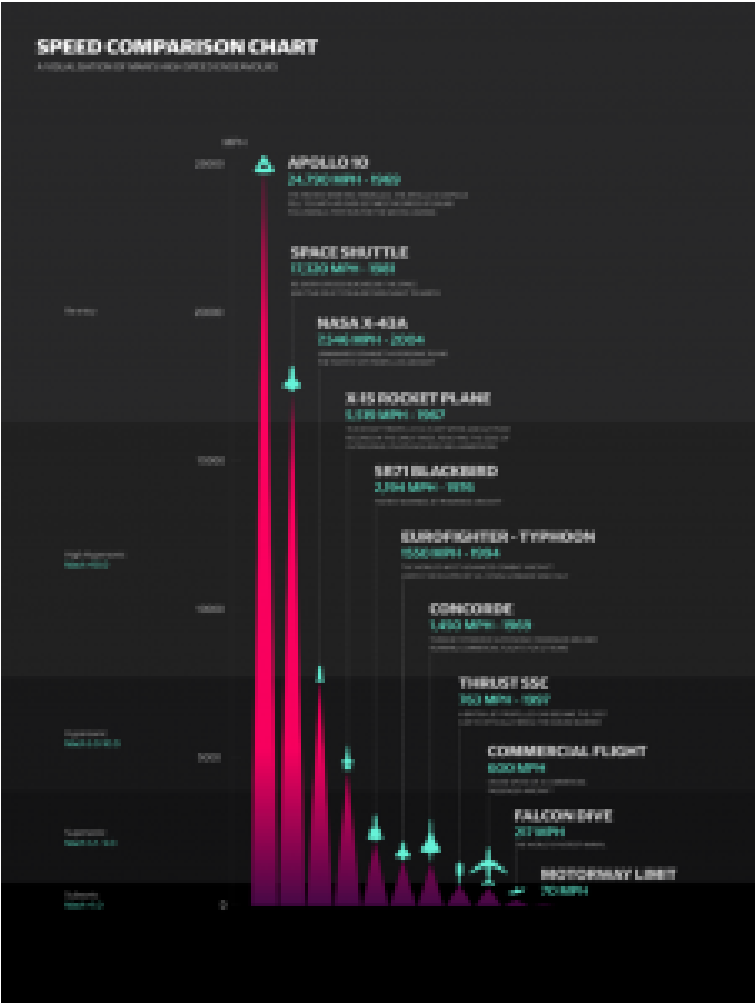


## **Hypersonic**

To obtain the hypersonic region, an aircraft must reach or surpass speeds of Mach 5 (>3,806 mph) and generally altitudes below 90km or 295,276 feet. Most of these aircraft are missiles, spacecraft, or experimental/research-based. At such speeds, extraordinary strain is placed on the physical structure and the human body so that astronauts re-entering the atmosphere pass out due to the extreme forces. Some of the Apollo Command Module reentries obtained speeds of Mach 20+ (Smithsonian National Air and Space Museum, 2022)

**Figure 12.1**

**Comparison of speeds for various aircraft and vehicles**



Note. The chart outlines relative speeds from automobiles through a line of flying vehicles with a timeline of speed advancements.

Source: (Kynvin, J., & Guardian Digital Agency, 2011)

**Speed and distance**

Once there is a realization of how fast these vehicles can fly, it is important to conceptualize the distance they can travel in a short period. A simple formula not accounting for changes in acceleration and other factors will assist with this visualization.

d=s\*t

Equation 12.2

where:

d = the distance traveled over a given speed and time

s = the constant speed the object is moving

t = the time the object has been in motion for a given speed.

Based on this formula, objects traveling at Mach speeds can transverse a great distance in a relatively short period. To appreciate national security concerns surrounding hypersonic weapons, it is essential to have a good perspective of the speed these vehicles can travel and how that compares to relative distances covered and the associated time. The following table provides some measurements to illustrate the relationship.

Table 12.2

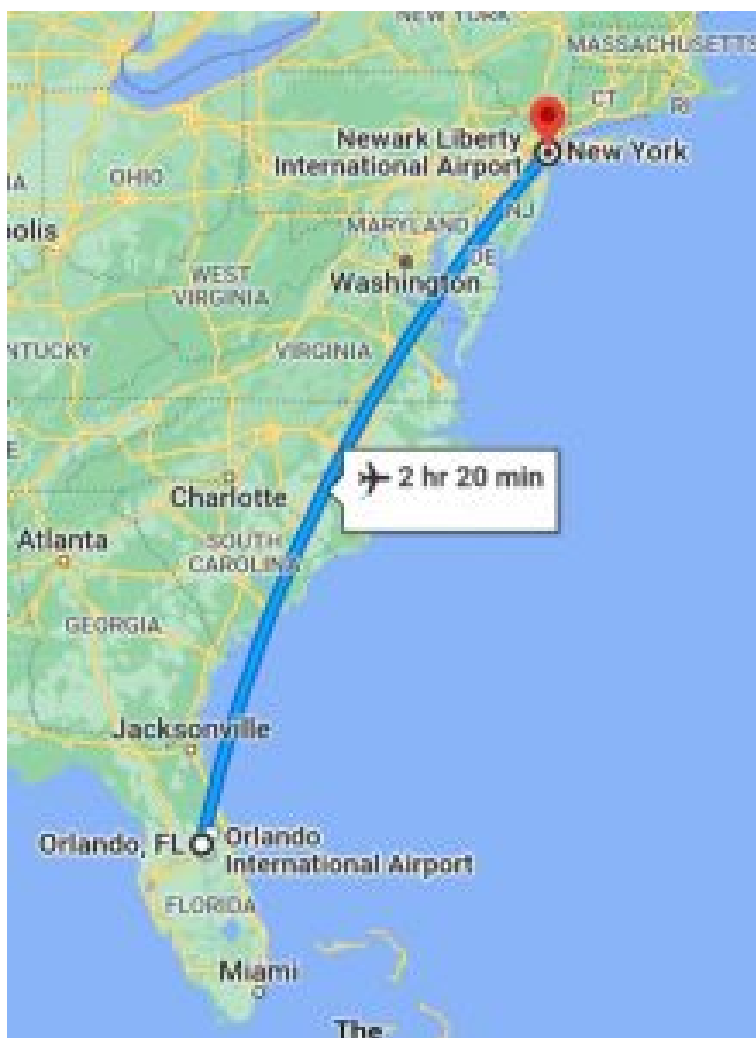
Speed, time, and distance comparisons at various Mach speeds  
from 1-30 and times to cover 1000 miles

| Mach<br>Speed | Miles/hr. | km/hr.    | Miles<br>/ sec. | Travel time<br>1000 miles<br>(mins.) | Mach | Miles/hr. | km/hr.    | Miles<br>/ sec. | Travel time<br>1000 miles<br>(mins.) |
|---------------|-----------|-----------|-----------------|--------------------------------------|------|-----------|-----------|-----------------|--------------------------------------|
| 1             | 761.20    | 1,224.77  | 0.21            | 78.62                                | 16   | 12,179.20 | 19,596.33 | 3.38            | 4.93                                 |
| 2             | 1,522.40  | 2,449.54  | 0.42            | 39.41                                | 17   | 12,940.40 | 20,821.30 | 3.58            | 4.64                                 |
| 3             | 2,283.60  | 3,674.31  | 0.63            | 26.27                                | 18   | 13,701.60 | 22,045.87 | 3.81            | 4.38                                 |
| 4             | 3,044.80  | 4,899.08  | 0.85            | 19.71                                | 19   | 14,462.80 | 23,270.65 | 4.02            | 4.15                                 |
| 5             | 3,806.00  | 6,123.85  | 1.06            | 15.76                                | 20   | 15,224.00 | 24,495.42 | 4.23            | 3.95                                 |
| 6             | 4,567.20  | 7,348.62  | 1.27            | 13.14                                | 21   | 15,985.20 | 25,720.19 | 4.44            | 3.82                                 |
| 7             | 5,328.40  | 8,573.40  | 1.48            | 11.26                                | 22   | 16,746.40 | 26,944.96 | 4.65            | 3.68                                 |
| 8             | 6,089.60  | 9,798.17  | 1.69            | 9.88                                 | 23   | 17,507.60 | 28,169.73 | 4.86            | 3.59                                 |
| 9             | 6,850.80  | 11,022.94 | 1.90            | 8.76                                 | 24   | 18,268.80 | 29,394.50 | 5.07            | 3.50                                 |
| 10            | 7,612.00  | 12,247.71 | 2.11            | 7.88                                 | 25   | 19,030.00 | 30,619.27 | 5.29            | 3.42                                 |
| 11            | 8,373.20  | 13,472.48 | 2.33            | 7.17                                 | 26   | 19,791.20 | 31,844.04 | 5.50            | 3.33                                 |
| 12            | 9,134.40  | 14,697.25 | 2.54            | 6.57                                 | 27   | 20,552.40 | 33,068.81 | 5.71            | 3.24                                 |
| 13            | 9,895.60  | 15,922.02 | 2.75            | 6.06                                 | 28   | 21,313.60 | 34,293.58 | 5.92            | 3.16                                 |
| 14            | 10,656.80 | 17,146.79 | 2.96            | 5.63                                 | 29   | 22,074.80 | 35,518.35 | 6.13            | 3.07                                 |
| 15            | 11,418.00 | 18,371.56 | 3.17            | 5.25                                 | 30   | 22,836.00 | 36,743.12 | 6.34            | 3.02                                 |

Source: (Kynvin, J., & Guardian Digital Agency , 2011) Photo conversion by author to meet PB specifications

Based on the above chart, if we were to use an object traveling at Mach 7, we would observe that the object is traveling at 5,328.4 miles per hour or 1.48 miles per second and will travel 1,000 miles at this speed of 11.26 minutes. By comparison, a car would take approximately 16 hours and a commercial flight approximately 2 hrs. And 20 min.

**Figure 12.2**  
**Commercial flight time from New York City to Orlando Florida**



Source: (Google Maps, 2022)

The extreme speeds of hypersonic weapons bring challenges for any country trying to perform threat analysis and make launch intercept decisions. Such weapons can reduce the available time to make such decisions from hours to minutes or less. This will be discussed later in the chapter.

### Types of hypersonic missiles

There are two categories of hypersonic devices currently under various stages of research and development, although some countries have claimed to have deployed them into active service. The two categories are the Hypersonic Cruise Missile (HCM) and the Hypersonic Glide Vehicle (HGV).

**Figure 12.3**  
**Categories of Hypersonic missiles**



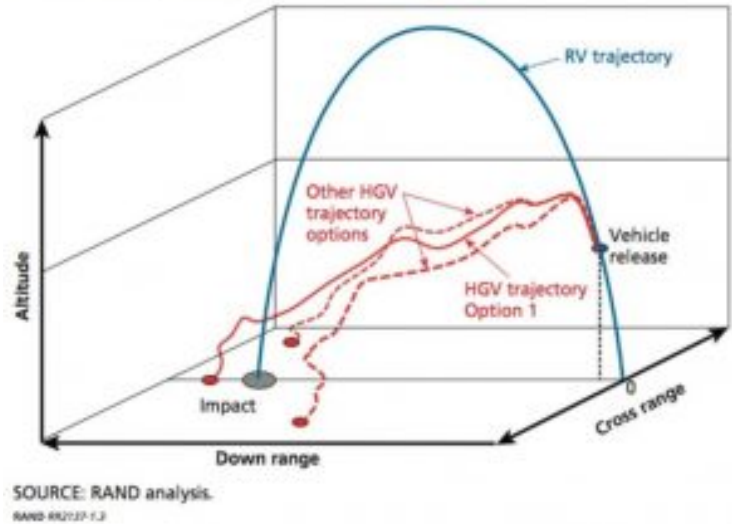
Note: Examples of a Hypersonic Cruise Missile and Hypersonic Glide Vehicle.

Source: (Brimelow B., 2018)

The HCMs are extremely fast Cruise Missiles powered by a SCRAM jet engine and can be launched from various platforms. They are self-propelled, which allows them to acquire alternate targets within their travel range, usually extended beyond gravitational pull. The X-43A (an experimental NASA vehicle) claims to have reached a speed of Mach 9.6 or approximately 6,800 mph or close to 2 miles per second (NASA, 2016) and, at this speed, will travel 1,000 miles in almost 8 minutes.

In contrast to the HCMs, the HGVs are not self-propelled and are solely dependent on gravity. These are also called Boost Glide Vehicles and are placed at a high altitude via an ICBM (Inter-Continental Ballistic Missile) type booster or space platform. The HGV becomes the booster's payload, which replaces the typical re-entry vehicles, previously known as Multiple Re-entry Vehicles or MRVs. Once released from a platform in space or their ICBM transport, they are propelled via the pull of gravity and use their hull design.

**Figure 12.4**  
**HGV trajectories compared to a Ballistic Reentry Vehicle**  
**Ballistic Reentry Vehicle (RV) Versus HGV Trajectories**

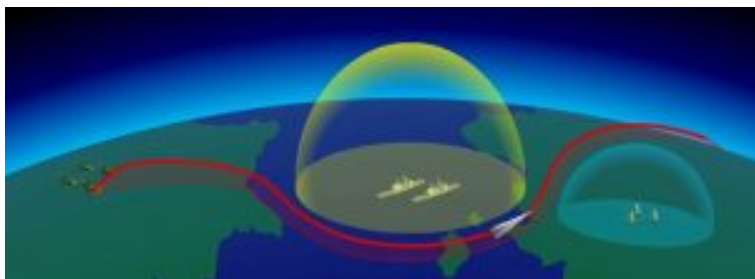


Note. Due to their type and design, the HGV can take a glide path that does not follow the same characteristics as a conventional Re-entry Vehicle (RV).

Source: (Speier, 2017)

The design of the HGV will allow it to glide to its target at hypersonic speed and generate lift via a process known as hypersonic aerodynamic lift. This would allow it to skip and glide across the atmosphere as it travels toward its target. However, unlike the ballistic missile, the path does not need to follow a linear trajectory and can maneuver in all spatial plains for roll, pitch, and yaw. This level of control can be accomplished with very small control surfaces that can make tracking the vehicle difficult and enhance its capability to avoid a midair interception or even to avoid detection areas.

**Figure 12.5**  
**Detection avoidance**



Source: (Brimelow B., 2018)

### **Types of Launch Platforms**

Deployment platforms for the technology can vary greatly depending on the mission profile, type of missile, and theater of operation, as outlined in the following examples:

**Stationary Land-Based** launch platforms are typically launched from silos. They are typically used for booster rockets to lift heavy payloads and place an object into a high orbit, allowing it to take advantage of gravity to increase its speed.



**Figure 12.6**  
**Russia's land-based silo launch**



Note. Topol-M launch

Source: (Russian Defense Ministry/TASS, 2020)

**Land-based mobile platforms** permit launches to be achieved by transporting the missiles and can be moved from location to location. This can make it difficult to determine a precise launch location until after the device has been mobilized and or launched. Multiple types of these platforms are often used to launch multiple rockets batteries and cruise missiles.

**Figure 12.7**  
**India Mobil launcher**



Note. Image courtesy: India TV. (India TV, 2020)

**Sea/ocean-based** launches can be performed from surface vessels, or submarines are currently equipped with subsonic cruise missiles. These provide a logistical advantage in positioning themselves closer to a target and providing ready capability. It also can spread out the launch area for optimal targeting. In the case of submarines, there is the ability to perform hit-and-run operations in that a vessel can surface and release, or it can provide a below surface launch and reduce its surface exposure.

**Figure 12.8**  
**Zircon Hypersonic missile ship launch**



Note. Image courtesy: Russian Defense Ministry. (Russian Defense Ministry, 2020)

**Airdrop** launches can be performed from two sub-launch platforms. The first is an aircraft that will ferry the missile to a high altitude and release it. This provides the altitude and speed to allow the missile to optimize fuel and provide sufficient speed to force air through its engines. Additional details on engine technology will be discussed later in the chapter.

In addition to aerial drops, there is the possibility to perform a space platform drop from a low or medium orbiting space platform. This has an advantage in which minimal fuel needs for the vehicle.

**Figure 12.9**  
**Aircraft launched a hypersonic missile.**



*Source: (Industry tap into news, n.d.)*

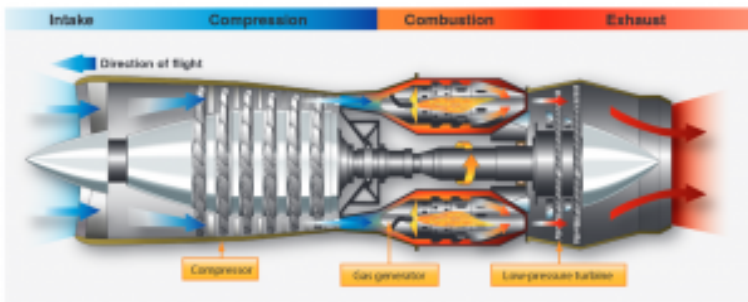
### **Power Plants / Propulsion systems**

Hypersonic aircraft have two distinct characteristics which overcome obstacles for traditional jet engines. First, they fly extremely fast, and secondly, they cruise at very high altitudes. This requires an engine that will intake air at near hypersonic speeds and operate at an altitude where the air is extremely thin. This need has led to the development of the Scramjet, short for Supersonic Combustion Ramjet. This engine is the successor to the turbine and ramjet engines. The Scram and Ramjets operate differently from the jet turbine currently used on most commercial aircraft. The following illustrates the two different engines (focus will be on the turbine and Scram) and their characteristics.

**Turbines or turbojets** are designed to intake air via a set of high-speed rotating turbine blades and compress the air into what is

known as a diffuser (which affords some cooling of the compressed air) which is then pushed into a combustion chamber. The compressed air is mixed with fuel and ignited in the combustion chamber. The resulting blast pushes the air out of the exhaust, which will spin exhaust fan blades connected to the intake blades, again intaking additional air. This process is referred to as the Suck, Squeeze, Burn, Blow principle.

**Figure 12.10**  
**Cutaway diagram of a basic jet engine**



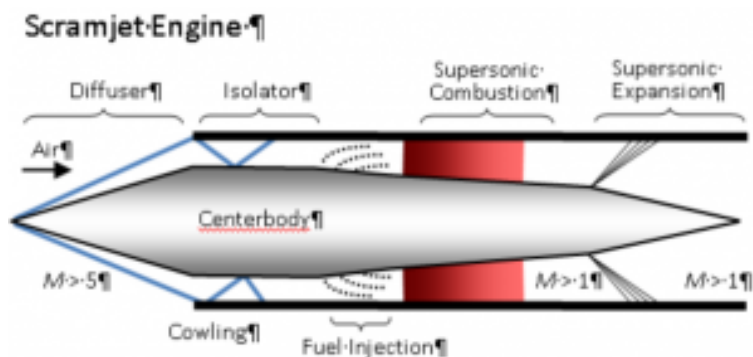
Source: (FAA, 2022)

These engines are extremely efficient at higher altitudes and generally cruise between 20,000-40,000 feet to obtain the best efficiencies of flight and fuel. The modern turbojet engines found in a fighter jet can reach 50,000-65,000 feet service ceilings. However, altitudes reach a little over 100,000 feet and a speed of approximately Mach 2.5 (Boeing, n.d.) The turbine engine loses efficiency in this general altitudes and speed range and will usually flame out due to oxygen deprivation.

**Supersonic-combustion ramjet, aka Scramjet**, unlike its

predecessor, the turbine, does not have a complex component structure composed of numerous moving parts; it has none. The turbine engine requires a complex set of rotary compressors to suck in and compress the air, containing the oxygen necessary to sustain fuel burning. On the other hand, the scramjet obtains its compression by ramming air into its intake by traveling at a high-speed velocity.

**Figure 12.11**  
Cutaway diagram of scram engine.

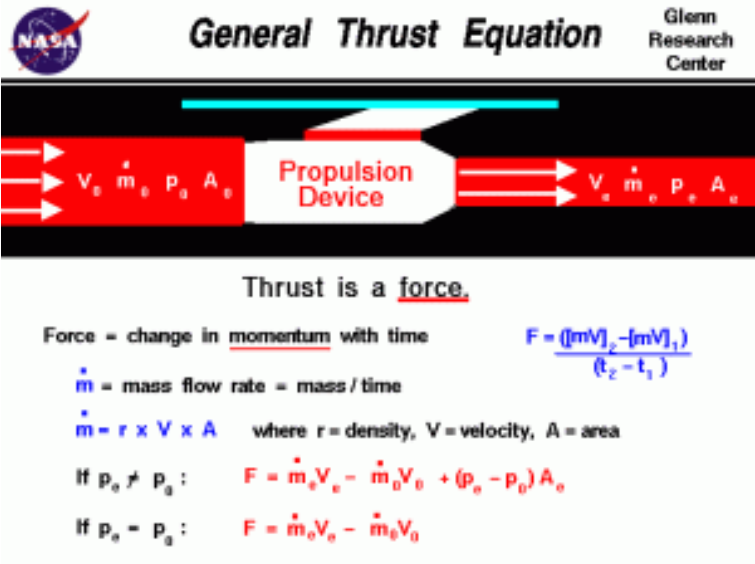


Sourced : (University of Washington, 2015)

This lack of a compressor requires a high speed which requires a launch from a rocket or aerial drop. A speed in the Mach 3+ range is needed for proper compression. This need typically requires a wide or long intake to channel the air being forced into the engine. Other changes in the pressure can be managed via the inlet and diffuser design leading into the combustion chamber. However, to increase the amount of thrust generated, it is essential not to decrease the speed at which airflow is passing through the system. Unlike a ramjet, the scramjet design ensures that the airspeed maintains a supersonic velocity as it passes from intake through combustion

to an even higher exhaust acceleration to obtain very high Mach speeds. Therefore, if we were to follow through on Newton's Second Law of motion applying to force and object mass:

Figure 12.12  
General thrust equation



Source: (NASA, 2021)

we could derive the general thrust equation

$$F = (\dot{m} * V)e - (\dot{m} * V)0 + (pe - p0) * Ae$$

Equation 12.3

Where:

$A_e$  = exit area

$\dot{\phantom{x}}$  = indicates the variable changes in time

$e$  = exit station

$F$  = force

$m$  = mass of the object

$O$  = freestream

$P$  = pressure

$V$  = velocity

The equation makes some profound implications related to the production of thrust. "...make the exit velocity much greater than the incoming velocity...A moderate amount of flow is accelerated to a high velocity" (NASA, 2021). This principle allows the scramjet to obtain and maintain a high supersonic/hypersonic airflow and generate high thrust. The engine design can surpass the speeds of Mach 10, which have already been achieved. However, other aerodynamic and physical processes must be addressed with such increases in speed. These will be discussed later in the chapter.

### **Technology Considerations for Hypersonic**

Although many of the countries mentioned are making claims of missiles achieving extremely high-end Mach speeds, some of the claims may be unlikely at the present point in time due to inefficiencies in existing and associated technologies. In 2018, Russia claimed it had developed and tested a Mach 20 capable weapon, and "Recently Russia claimed to have developed a weapon that could travel at Mach 20. As stated by Putin, "The Avangard is invulnerable to intercept by any existing and prospective missile defense means of the potential adversary," and they continued to add that the weapon was expected to enter into Russian service the following year (Shalini, 2018). However, this has not been proven, and any research attempts to obtain such a speed, with what would be considered a hypersonic weapon at Mach 5 and greater speeds, have disintegrated the vehicle, highlighting numerous challenges that must be addressed to achieve such a feat. Besides achieving



and maintaining such a super hyper-speed, it will be necessary to overcome some of the following obstacles:

**Aerodynamic heating and airframe construction** are two such concerns that must be accounted for when traveling at speeds of Mach 5 and greater through the atmosphere. These extreme environmental concerns result from heat generation and transference, which must be adequately managed to keep the vehicle from heat damage and drag management associated with the airframe design (Deloitte, 2020). To manage heat transference, current vehicles moving at speeds close to Mach 20 or above have only been documented by space vehicles upon reentry, for example, the Space Shuttle and the Apollo capsules. One other has been HTV-1 and HTV-2 (there were two tests with HTV-1 type vehicles) destroyed by the heat during their research flights. According to NASA, as outlined in their Orbiter Thermal Protection fact sheet, the space shuttle travels more than 17,00 mph, roughly Mach 20, and uses the atmosphere as a friction brake to slow down. During the deceleration process, the outside surface can reach temperatures up to 3,000 oF or 1,648 oC.

The following provides a comparison of common metals that will melt at or below these temperatures:

**Table 12.3**  
**Melting temperatures of 10 common metals.**

| Atomic # | Element                   | Melting Point (°C) | Melting Point (°F) |
|----------|---------------------------|--------------------|--------------------|
| 26       | <a href="#">Iron</a>      | 1538 °C            | 2800 °F            |
| 28       | <a href="#">Nickel</a>    | 1453 °C            | 2651 °F            |
| 29       | <a href="#">Copper</a>    | 1084.62 °C         | 1984.32 °F         |
| 79       | <a href="#">Gold</a>      | 1064.18°C          | 1947.52°F          |
| 47       | <a href="#">Silver</a>    | 961.78°C           | 1763.2°F           |
| 13       | <a href="#">Aluminum</a>  | 660.32 °C          | 1220.58 °F         |
| 12       | <a href="#">Magnesium</a> | 650 °C             | 1202 °F            |
| 30       | <a href="#">Zinc</a>      | 419.53 °C          | 787.15 °F          |
| 82       | <a href="#">Lead</a>      | 327.46°C           | 621.43°F           |
| 50       | <a href="#">Tin</a>       | 231.93°C           | 449.47°F           |

Source: (AE Toolbox, 2022)

The NASA fact sheet highlights the need to keep any internal components and structures below a certain temperature range because of damage to the airframe and internal systems. “Although the orbiters were built using highly advanced construction methods and materials, the airframe is formed primarily from aluminum and can only withstand 350 F without the material annealing or softening. The purpose of the thermal protection system is to ensure that the aluminum airframe does not exceed this 350-degree limit.” (NASA, n.d.).

It should be noted that the information previously provided from the NASA fact sheet is regarding the Space Shuttle (Orbiter), which is a very large piece of machinery as opposed to a cruise-type missile. Because of its size, it can carry additional thermal protection and has a larger protective plume. With that said, its protection systems have the following weight profile based on the type of tiles used in the various areas:

**Figure 12.13**

**Tile weights per cubic foot for the Thermal Protection System  
tiles used on the STS Orbiter**

|  |        |   |      |
|--|--------|---|------|
| <b>High-Temperature Reusable Surface Insulation (HRSI) tiles</b> |        | <b>Low-Temperature Reusable Surface Insulation (LRSI) tiles</b> |      |
| 22-pound-per-cubic-foot =  | 525    | 9-pound-per-cubic-foot =  | 725  |
| 9-pound-per-cubic-foot =   | 20,000 | 12-pound-per-cubic-foot =                                       | 77** |
| <b>Fibrous Refractory Composite Insulation (FRCI) tiles*</b>     |        | <b>Flexible Insulation Blankets (FIBs) =</b>                    |      |
| 12-pound-per-cubic-foot =  |        | 2,300   |      |
|  |        | <b>Felt Reusable Surface Insulation (FRSI) =</b>                |      |
|  |        | 975***  |      |

\* Not shown is FRCI. The tiles are limited to isolated areas.

\*\* There is a slight variation in the number of tiles per vehicle. Some orbiters also have no 12-pound-per-cubic-foot LRSI tiles.

\*\*\* The FRSI sheets will vary slightly in number for each orbiter. An average of 1,860 square feet of FRSI sheets are used on an orbiter.

Source: (NASA, n.d.)

Smaller devices traveling at high speeds will still need to contend with the concern of heat displacement and protection of critical electronic components as-well-as structural integrity of the reentry vehicle. An object traveling at Mach 5 can incur temperatures of 1800°C (3,272°F) on its leading edges. Likewise, the same object traveling at Mach 15 could expect approximately 6000°C (10,832°F) on the same surfaces. This poses a severe engineering challenge with existing materials:

**Table 12.4**  
**Common Critical Electronic materials**

| Atomic # | Element           | Melting Point (°C) | Melting Point (°F) |
|----------|-------------------|--------------------|--------------------|
| 6        | Carbon (graphite) | >3527 °C           | >6381 °F           |
| 74       | Tungsten          | 3422°C             | 6192°F             |
| 75       | Rhenium           | 3186°C             | 5767°F             |
| 76       | Osmium            | 3033°C             | 5491°F             |
| 73       | Tantalum          | 3017°C             | 5463°F             |
| 42       | Molybdenum        | 2623°C             | 4753°F             |
| 41       | Niobium           | 2477°C             | 4491°F             |
| 77       | Iridium           | 2466°C             | 4471°F             |

Source: (AE Toolbox, 2022)

Since any projectile or vehicle traveling at such speeds would need to overcome the melting temperatures of composites such as Hafnium Carbide, which have melting points of approximately 3958°C (Precision Ceramics EU, 2021), as well as Carbon Graphite. Because of these limitations, a projectile or missile traveling at such speeds in the atmosphere would likely disintegrate as it accelerates towards a speed of Mach 20. An example of such a breakdown at the extreme speed of Mach 20 and temperatures of >1900°C (3500°F) is the DARPA Hypersonic Test Vehicle (HTV-2). There were two flights lasting approximately 9 minutes. The reporting of lost signals in both flights and the vehicles crashing into the ocean (Plummer, 2011); ironically, communications interruption was experienced at the same in-flight time for both test flights. Some reports indicate that “A DARPA engineering review board found” most probable cause of the HTV-2 Flight 2 premature flight termination was unexpected aero-shell degradation, creating multiple upsets of increasing severity that ultimately activated the Flight Safety System.” (Malik, 2012).

This illustrates concerns related to the technology associated with heat management based on existing surface materials. There are alternate technologies associated with hull designs that will act as heat sinks, along with cryogenic cooling of the missile with a

circulation of the liquid fuel through the hull. Such designs cooling designs beg additional considerations and investigation since a decrease in cooling efficiency will occur as there is a reduction in fuel and cooling based on fuel depletion. This could potentially expose the remaining fuel to an increasingly hotter hull. This also does not account for any potential shifts in weight, which would be a critical factor to include in any compensating calculations.

**Navigation, guidance, and control systems** are also areas of concern. Almost every aspect of modern warfare is based on electronic components, all of which have operational ranges associated with environmental such as heat, humidity, voltage fluctuation, ionization, etc. Based on decades of knowledge derived from satellite instrumentation, it is known that “The maximum structure temperature is still far higher than the temperatures that would cause degradation and failure to electronic components...Components can be subjected to temperatures as low as  $-55^{\circ}\text{C}$  ( $-67^{\circ}\text{F}$ ) and as high as  $125^{\circ}\text{C}$  ( $257^{\circ}\text{F}$ )... These thermal conditions can induce several failure modes, including package and die cracking, bond-wire breakage, moisture ingress, die delamination, tin whisker growth, and solder-joint failure.” (Electronic Products, 2019). Any internal temperature that would far exceed such numbers would bring a failure to the systems that maintain communications and flight control of the vehicle or weapon. To control a hypersonic missile or projectile, it will be necessary to provide signaling to control surfaces. That is typically performed via fly-by-wire technology controlled by internal electronics. The electronic transmissions to the control surfaces will come from the electronic components that must be protected from the extreme environments created by hypersonic travel.

A major part of any navigation system will be communications. Upon any high-speed vehicle's re-entry into the atmosphere, a couple of phenomena occur. First, there is the heating of the air due to friction of the air molecules rushing over the craft's hull. A shockwave follows this once the sound barrier is broken at Mach 1. In the hypersonic, above Mach 5, and the high-Hypersonic, Mach 10

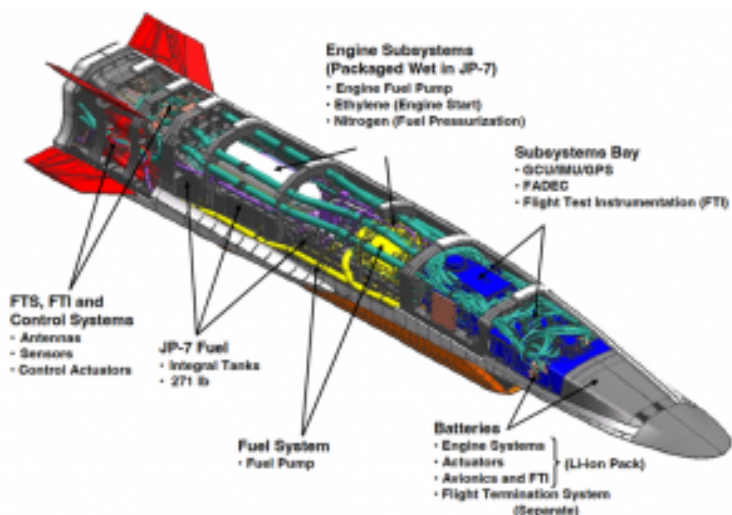
and above, the shockwave adds to the temperature and atmospheric friction. The extreme heat, as previously discussed, changes the chemical make-up of the oxygen and nitrogen in the air and causes the release of electrons which ionizes the air creating a plasma field surrounding the moving object (Nelson, 2020). In the case of the Orbiter or other spacecraft performing atmospheric re-entry, this ionization causes a communication blackout. In the case of the Mars Pathfinder, communications were lost with Earth for approximately 30 seconds (Morabito, 2002). A hypersonic projectile traveling at Mach 10 could travel over 63 miles in that short period with potentially only autonomous control. However, this would potentially exclude any communications with GPS systems barring new communications technology such as advanced X-ray technology or a large enough vehicle that the plume left an opening to allow a communications hole. The lack of technology would limit the ability to perform course corrections from external sources.

**Other considerations** would be the immaturity of the Scramjet engines and accessory design. For example, a critical component of the engine is the intake. There have only been a few very effective techniques to maintain the massive airflow and minimize any reductions in pressure. One is the development of a long intake, as presented by the Bussmann intake, and another is the management of shockwaves to manage the flow to avoid unstart conditions (Krishnan et al., 2009). However, the latter is very dependent on boundary layer flow which is very difficult to calculate at higher Mach speeds. The highest-rated wind tunnel in the U.S. is the LENS II Hypervelocity Tunnel, rated at Mach 15 (Holden, 2002). It is also reported that China is currently working on one that will be rated at Mach 30. Therefore, other than actual flights and data collection from sensors, the location of the hypersonic boundary layer is based on simulation and mathematical models, which may not be actual. This does not account for other factors such as proper fuel mixing and ignition within the combustion chamber, which is all timing and must be continuous for sustained powered flight. This does not

account for the materials within the engine that must sustain high stress and temperatures for the flight's duration.

An additional noteworthy discussion point is that there is a direct contrast between stability and performance in aviation. Pilots do not start out flying high-performance aircraft. They will begin with a more stable and forgiving form of a trainer. As they progress, they work their way up to high-performance aircraft that are inherently less stable because there is a trade-off between performance and stability. In addition, to the typical aircraft systems of propulsion, airframe, wings, and aerodynamic control surfaces, the more complex or high-performance aircraft have numerous subsystems to monitor and provide correction to the critical engine, environmental, and sensor components that assist the pilot with critical maneuvers that could not be performed without their aid. In addition, to these mentioned subsystems, others support communications and navigations and play a critical role in any in-flight vehicle, especially one traveling at hypersonic speed. Although an HGV would not need systems for monitoring population systems, some of the other systems illustrated in the diagram below would still apply (Brockmann, 2022).

**Figure 12.14**  
**Cutaway diagram of the X-51A HCM with subsystems.**



Source: J. Hank, J. M., Murphy, J. S. and Mutzman, R. C., 'The X-51A Scramjet Engine Flight

Demonstration Program', 15th AIAA International Space Planes and Hypersonic Systems and

Technologies Conference, May 2008, p. 7., (J. Hank, 2008)

"As the wedge-shaped vehicle rips the air apart at such high speeds, controlling the capsule at such speed is another challenge, requiring precise sensing and near-simultaneous response to flight path disturbances, requiring hybrid controls combining Reaction Control System (RCS) and aerodynamic effects." (Eshel, 2011). This would require systems and monitors that provide flight data such as altimeter and pressure and airspeed and stability information, especially concerning the horizon. There would also be guidance, navigation, hydraulic and control systems that determine distance measuring and magnetic orientation along with gyroscopes or angular velocity measuring equipment, not to mention systems to manage electrical power distribution. In the case of most complex



aircraft, these subsystems are very tightly coupled (NASA, 2006) and would need to be more so for the management of such a vehicle.

Enhanced computer technology associated with the hypersonic platforms will need the ability to provide computational power for areas similar to, but not limited to: ”

- mission computing, focused on responding to commands, adjusting to changing conditions, and ensuring that all subsystems work in concert to accomplish a platform’s mission.
- flight computing, controlling the platform’s path, monitoring the outputs of sensors, and controlling the operational employment of sensors.
- real-time signal processing for radar, electro-optical sensors, and electronic warfare (EW);
- and flawless and secure communications with command-and-control networks.” (Wilson, 2020)

It is important to note that there will be a need to realize the distinction between flight and mission computing as a weaponized device that must be performing real-time computing activities requiring massive computing resources and preemptive logic calculations to maintain flight control signaling. The transmissions to the control surfaces will come from the computer(s) and electronic components that must be protected from the extreme conditions previously discussed and maintain constant and consistent communications between themselves, which is a major technological challenge.

### **Military Application and Threats**

The types of vehicles and weapons known to travel at hypersonic speeds, the type of powerplants that can produce thrust at Mach 5+ speeds, and the various deployment methods such weapons can be dispensed from are all important. Some of the technological challenges associated with hypersonic technology were highlighted,

begging to question what parts fact vs. fiction are and what is an immediate threat vs. posturing of all sides.

With the previously mentioned knowledge, we can determine that the speed alone of these devices can make for a formable weapon. This, coupled with maneuverability and the ability to evade current defensive countermeasures, potentially makes the technology a force to be addressed from an offense and defensive perspective.

The technology needed to create a hypersonic weapon is not trivial. Numerous technological hurdles must be overcome to create a reliable weapon system. These hurdles would require a country with access to the most modern materials science, populations, computer, and engineering technology. It would also require a massive financial investment to perform the needed Research and Development, even testing a prototype of such a device, consuming large sums of the country's budget. However, there are many countries currently working to achieve such.

**Figure 12.15**  
**Countries pursuing hypersonic weapon technology**



Source: (VOA Graphics, 2022)

Of these countries, China, India, North Korea, Russia, and the United States have alleged to have created test vehicles and performed flights using the technology. The vehicles that have been reported to be tested for each nation are:

**Table 12.5**  
**Listing of countries with their hypersonic devices and associated speeds and distances**

| Country     | Reported Vehicle    | Claimed Mach Speed | Claimed range mi / km | Citations                            |
|-------------|---------------------|--------------------|-----------------------|--------------------------------------|
| Brazil      | X-14                | 06.0               | 120 / 200             | (Força Aérea Brasileira, 2021)       |
| China       | DF-17               | 10.0               | 1,553 / 2,500         | (CSIS Missile Defense Project, 2021) |
| India       | Shukra              | 07.5               | 733 / 1,180           | (Military-Today, n.d.)               |
|             | Brahmos II          | 05.0               | 310 / 500             | (CSIS Missile Defense Project, 2021) |
| North Korea | Hwasong 8           | 05.0               | 1,988 / 3,200         | (Military-Today, n.d.)               |
| Russia      | Avangard (BGV)      | 20.0               | 3,728 / 6,000         | (Nilent, 2021)                       |
|             | 3M22 Zircon/Zayrkon | 07.0               | 621 / 1,000           | (Military-Today, n.d.)               |
| USA         | X-51A Waverider     | 05.0               | 480 / 724             | (USAF, n.d.)                         |

Source: (USAF, n.d.) Photo conversion by author to meet PB specifications

Note. The information presented is based on claims and may not be actual speeds and distances. This also does not include sustained speeds or time at speed information. There may also be variations based on booster assistance.

Since it has been established there is a likelihood of technological and manufacturing, misinformation, exaggeration, and posturing, it is difficult to compare the claimed technology that each country may have. To provide some relative context of the weapon platform's potential, the averages of the Mach speeds and ranges have been used based on the above table and are as follows:

Mach 8: Average estimated speed

1189 miles: Average estimated range

9.84 minutes: Average estimated time to travel 1000 miles

**Note:** These times appear to be on the higher end but are based on the averages of the available information.

For context, a few scenarios may provide additional perspective on the distances that can be covered in a short period and why a missile or any other fast-moving weapon, time becomes the critical factor.

The following figure depicts a hypersonic attack on NATO countries (shaded in gray) from a seaport in Kaliningrad or possibly a missile cruiser in the Baltic Sea, with hypersonic weapons trained on London and Berlin, and Warsaw.

**Figure 12.16**

**Attack scenario against 3 NATO countries from a Baltic based launch**



Source: (NATO, n.d.)

In the case of a launch towards London, which is approximately a distance of 880 miles, the scenario missile traveling at Mach

8 would cover that distance in approximately 8 minutes and 40 seconds. This is more than twice as long as the flight to Poland, which has a distance of approximately 330 miles and will receive its delivery in an estimated 3 minutes, 15 seconds. Warsaw, Poland, is approximately 180 miles distance and could expect a strike in approximately 1 minute and 46 seconds. Although these are raw numbers and don't account for launch and initial acceleration, they paint a fairly good picture of how fast these weapons can arrive at a target before the opposing force can react.

Another scenario may be that of China and its ability to launch from multiple locations against numerous targets in the Pacific and South China Sea.

**Figure 12.17**  
**Distances between possible Chinese launch sites and targets in Korea, Japan, and Taiwan**



*Source: (Google Maps, 2022)*

With the short distance on the coast of China, for instance, a base near Qingdao could send a Mach 8 missile to Osaka, Japan, in approximately 8 minutes and Sole Korea in approximately 3 minutes 46 seconds. Continuing to use Mach 8 and a launch from Quanzhou, China, a missile would reach Taichung City, Taiwan, in approximately 1 minute and 32 seconds. In the situation of Taiwan, there would be no time to react or alert or for the population to seek shelter. From a more strategic perspective, China could quickly deliver a hypersonic weapon to almost any point in the South Pacific in less than 10 minutes. Based on the anticipated ranges of the

deployable weapons, this would include the Philippines and nations that border China.

**Figure 12.18**  
**Various ranges for ballistic coverage from eastern Chinese missile launch facilities cover the south Pacific.**



Source: (Lockie, 2019)

With these times and based on the existing ballistic missile technology, it is difficult to defend against hypersonic weapons. According to Richard Speier, an adjunct staff member with Rand, “We don’t currently have effective defenses against hypersonic weapons because of the way they fly, i.e., they’re maneuverable and fly at an altitude our current defense systems are not designed to operate at, ... Our whole defensive system assumes that you’re going to intercept a ballistic object.” (Macias, 2018)

Based on the previously defined assumptions related to weapon speed and distance and a non-ballistic trajectory, it is feasible that China could launch an attack against the US and the interest of other countries that would use the shipping lanes of the South China Sea connecting East Asia and India, Western Asia, Taiwan, and the Luzon Straits. An attack on a vessel at sea would have a very little warning or time to react to a hypersonic weapon assault. In short, the first one to strike would have an advantage since the reaction time for the other side has been dramatically reduced.

**Figure 12.19**  
**Illustration of China's hypersonic tests**



Source: (Pileggi, 2019)

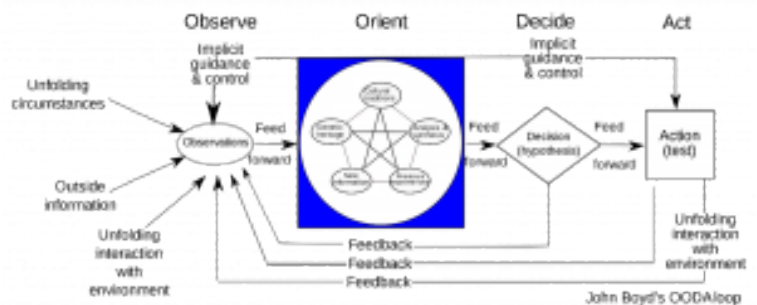
Time is everything, and as a result, “...the adversaries have increasingly focused on systems that dramatically compress the timelines and the timescale of a tactical battlefield. These systems – including ballistic missiles, ballistic missiles with maneuvering reentry vehicles, and vehicles increasingly hypersonic in nature –



give adversaries the ability to hold our forces at risk from hundreds, even thousands, of miles away, with flight times that are measured in minutes.” (Cronk, 2021)

One of the existing decision strategies is the OODA-loop, created by Air Force Colonel John Boyd; it is an acronym for Observe, Orient, Decide, and; it is an iterative strategy that will allow one to make decisions and act on them quicker than their opponent, therefore, disrupting the opponent’s loop and giving an advantage. In the case of an incoming missile, this loop is the time to observe the incoming bogie, orient by determining where it is heading and if it is hostile, determine to intercept and or retaliate then t finally act on that action (Wikipedia, 2003)

**Figure 12.20**  
**The Observe. Orient. Decide. Act-Loop**



*Sourced from: (Wikipedia, 2003)*

Executing the loop takes time, beginning from the point of observation, which is a key distinction and important point. Hypersonic weapons are a disruptive technology that has required

the need for technology to perform early detection, which will increase the time available for orientation and determination, time to decide then act. However, even with early detection, the other areas of the loop may not have sufficient time to react due to the lighting speed of the hypersonic weapon. The new technology has taken the OODA-Loop from minutes to seconds, making orientation, decisions, and acting so fast that humans may no longer be able to do such. The following table provides some approximate time estimates that currently exist for making a launch determination using ICBMs.

**Table 12.6**  
**Steps and times from observation to launch decision for**  
**incoming ballistic missile**

---

|                            |   |
|----------------------------|---|
| H<br>Missile<br>launch     |   |
| H+1<br>min                 | U.S. infra-red satellite detects hot plumes from Russian ballistic missiles during the 4-7-minute-long boost phase of flight. Satellites instantly transmit the detection data to early warning teams at NORAD, STRATCOM, NMCC, ANMCC, and other facilities. Russian stealthy cruise missiles launched from stealthy submarines patrolling off the U.S. coasts likely elude detection throughout their flight to targets. |
| H+4<br>min                 | NORAD and STRATCOM early-warning teams must report initial confidence (no, medium, or high) of nuclear missile threat to North America. NORAD and STRATCOM Commanders are notified and briefed on the apparent threat.  |
| H+4<br>to+9<br>min         | If confidence is medium or high, POTUS is notified, and reachable advisors are dialed into teleconference or video conference.  |
| H+9 to<br>+10<br>min       | STRATCOM Commander briefs POTUS on the threat and response options along with their consequences (mainly civilian casualties in Russia) and makes a recommendation.   |
| H+10<br>to +15<br>min      | BMEWS ground radars detect missiles in mid-flight. Early warning teams confirm an attack underway, and computers update predictions of impact areas and targets.  |
| H+10<br>to +17<br>min      | POTUS is updated by briefers, deliberates, and may confer with other advisors.  |
| H+17<br>to<br>+17.5<br>min | POTUS informs Pentagon War Room (the emergency actions center of the NMCC, which has been monitoring the conference since its beginning) of the response option to be executed. NMCC challenges POTUS to authenticate their identity using "Gold Codes." <sup>4</sup>   |
| H+18<br>to +20             | min War Room (NMCC or alternate) formats and transmits launch order (1/2 length of a Tweet!) directly to SSBNs, ICBMs, and bombers (as well as the entire chain of nuclear command). Order contains the time of launch, option to execute, unlock codes, and special authentication codes. <sup>5</sup>   |
| H+20<br>to +22<br>min      | ICBM, SSBN, and bomber crews authenticate messages using special authentication codes in their possession. ICBM crews target missiles by chosen war plan, unlock (enable) missiles selected for launch, and transmit launch signals   |
| H+22<br>to +27<br>min      | ICBMs instantly fire out of silos over pre-programmed 5-minute fly-out salvo.   |

|                               |  |
|-------------------------------|--|
| H+27<br>to +30<br>min         | Incoming Russian warheads begin to detonate on CONUS.                    |
| H+35<br>to +40<br>min         | U.S. SLBM launches begin; 1 every 15 seconds for each SSBN.              |
| H+50<br>to +60<br>min         | U.S. ICBM and SLBM warheads strike Russian targets.                      |
| H+8<br>hrs. to<br>+12<br>hrs. | CONUS-based U.S. bombers begin firing cruise missiles or dropping bombs. |

---

Note. The above provides time estimates based on a U.S. decision to launch a nuclear missile upon warning of an enemy attack. Source: (Blair, 2019)

The difference in time for a hypersonic missile to be launched and delivered to its target 1000 miles away at a speed of Mach 8 could be under 10 minutes. Likewise, a closer target, such as an aircraft carrier at 100 miles, would have less than 1 minute to observe, orient, decide and act. In the case of an aircraft carrier, it is most likely the vessel will be lost. In the case of a larger target, such as a city within the 1000-mile range, there will be little chance of any occupants being able to obtain reasonable shelter in the available time.

### **Doctrines, Policies, and Strategies in an era of hypersonic weapons**

To continue with the topic of offensive and defensive strategies, as they relate to hypersonic weapons, it is important to have a brief understanding of how they interact because they will determine how investments are made, what systems are deployed, and where, along with how a country may use such technology to react/not react to an actual or perceived threat. To have this conversation, we need to start with the concept of doctrine, which is the highest level of the three. This is the concept, belief, or ideology from

which policies and strategies are developed. For example, general emphasis or at least espoused doctrines of the US, Russia, and China are along the lines of:

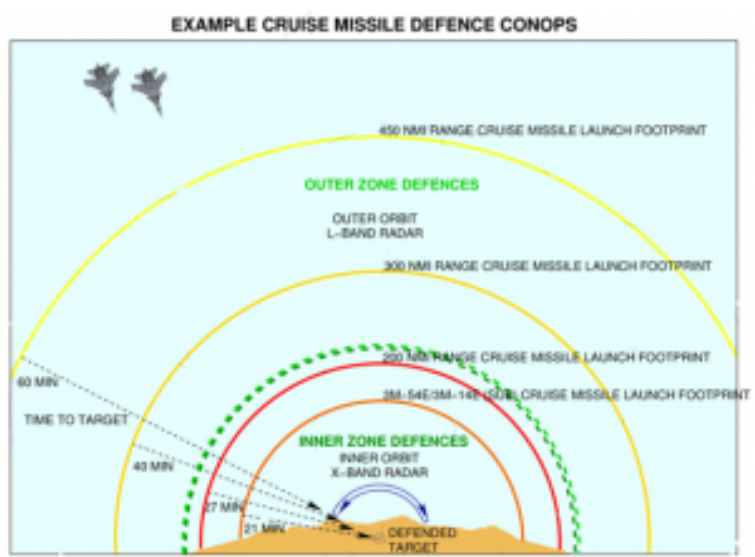
- the United States has the US Constitution, which advocates separation of powers, church, and state with concern for the rights and freedoms of the individual. It also is built on the concept of publicly elected officials by national vote and a “principle” of a peaceful transfer of power.
- Russian Federation, as stated in part of a policy concept, “To ensure reliable security of the country, to preserve and strengthen its sovereignty and territorial integrity, to achieve firm and prestigious positions in the world community, most fully consistent with the interests of the Russian Federation as a great power, as one of the most influential centers of the modern world, and which are necessary for the growth of its political, economic, intellectual and spiritual potential.” (Russian Federation, 2000)
- the People’s Republic of China, under the Xi Jinping doctrine, focuses on “the mission of the Chinese Communist Party”...” national rejuvenation,”...” global community,” and “Chinese contribution. Xi says, “Chinese people will never allow any foreign force to bully, oppress, or subjugate us...” (Xinhua, 2021)

From their doctrine(s), a country will develop various policies supporting those doctrines, leading to strategies and tactics that will enforce or bring those policies to fruition. In the case of some countries, there may be the doctrine to expand or warmonger and, as such, may have little apprehension to taking advantage of a preemptive assault if there is a reasonable presumption they could do so and avoid any repercussions of a retaliatory strike.

As previously discussed, the speed at which hypersonic weapons travel, any country that has a command of this technology could use it for retaliatory or preemptive actions and do so before the opposition could react, therefore providing those with the

technology with additional strategic and tactical options compared to those from previous generations of warfare. When working with aircraft and ballistic missiles, the OODA loop was an effective strategy because it would provide an iterative process of what would be considered a, by today's standards, an elongated time to decide and react therefore disrupting the OODA loop of the opponent there is no longer sufficient time for humans to react effectively with the incredibly short periods.

**Figure 12.21**  
**Cruise missiles launch footprints and travel times to target**



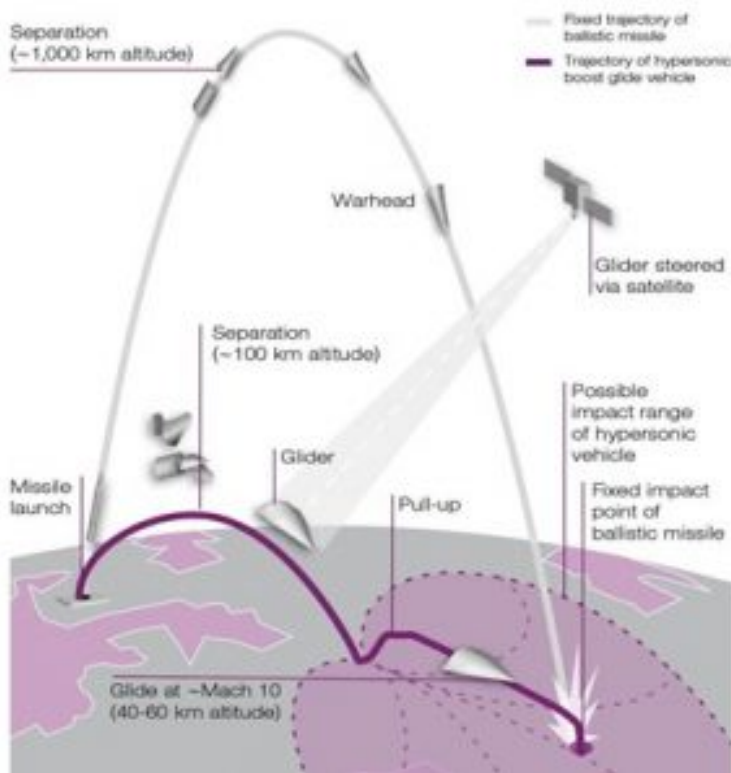
Sourced: (Kopp, 2014)

Using the above Cruise missile footprint diagram. Launching a Cruise missile airdrop of 200 miles would require approximately 27 minutes to target. In the same scenarios, deploying a Mach 8

missile at an aircraft carrier or other target 200 miles away would provide the ship's captain approximately 2 minutes to react. In the event of an airdrop or ship launch, it is very foreseeable that multiple missiles could target and overcome multiple aircraft carriers in a fleet.

In addition to speed, there is a high degree of mobility. A guided weapon can perform deceptive target acquisition by altering its flight path and redirecting to another possible target within its acquisition range. Again, this would provide another degree of uncertainty about what assets to protect. The possible coverage of such a missile is outlined in the diagram below.

**Figure 12.22**  
**Possible target coverage ranges of a Hypersonic Glide Vehicle**



Source: (Delcker, 2019)

In selecting a strategy, it is essential to understand the strengths and weaknesses of one's defenses and those of the Opposing Force. It is also important to understand that the element of surprise can benefit the initiator of a preemptive strike. Therefore, it is important to realize there may be multiple short- and long-term strategies for various theaters of operation. For example, there could be a separate strategy for an offensive posture such as preemptive or even retaliatory strike doctrines, such as Mutually Assured Destruction/Deterrence, ensuring the destruction of all opposing sides, or an initiative to develop defense systems based



on advanced technology. This would all depend on the doctrines, policies, and determining strategies of the countries involved.

As an example, there are currently parties in the Department of Defense that believe the Peoples Republic of China (PRC) may have some level of credibility in their stated deployment of hypersonic technology and realize their aggressive activities to develop such technology via their 2025 plan, as well as creating fortifications in the East and South China Seas, from which numerous weapon platforms can be launched. China's People's Liberation Army (PLA), according to the Office of the Secretary of Defense, has stated that "The PLA is developing capabilities to provide options for the PRC to dissuade, deter, or, if ordered, defeat third-party intervention during a large-scale, theater campaign such as a Taiwan contingency." (DoD, 2020). Depending on where weapons are launched from China, a Mach 8 hypersonic missile could hit Taiwan in under 2 minutes and vice versa. Chinese defense strategy has already considered these possibilities, and "The PLA argues that the implementation of "intelligentized" capabilities will increase the speed of future combat, necessitating more rapid processing and fusing of information to support quick and efficient command decision making. According to PLA strategists, victory in future warfare will depend upon which side can more quickly and effectively observe, orient, decide, and act in an increasingly dynamic operating environment." (DoD, 2020) . In the US, there has already been an acceptance that some ". "S. defense officials have stated that both terrestrial- and current space-based sensor architectures are insufficient to detect and track hypersonic weapons, with former USD(R&E) Griffin noting that "hypersonic targets are 10 to 20 times dimmer than what the U.S. normally tracks by satellites in geostationary orbit." (DoD, 2020)

As the weapon delivery systems become quicker, reducing the OODA-loop times, and the self-awareness that no one country may have the technical capabilities to defend against this emerging technology, strategies will change to a more reactive posture. The

existing policies and tactics based on arcane ICBM strategies may change from a DEFCON type system with various levels of readiness working up to a “Launch On Warning” that may not become a “Launch On Detection.” This may further be exacerbated by the deployment and integration of such technologies as low-altitude satellites as dedicated tracking sensors across the globe, providing a Wide Field Of View (WFOV) for launch detections. This is currently underway with US government contractors (DoD, 2020) and the possibility of space-based countermeasures. In any event, a current US strategy is to invest in technology to not only develop hypersonic technologies but to also defend against them with the US, “Hypersonic weapon-related and technology development is widespread across DOD and includes supporting efforts by DOE and NASA, such as basic hypersonic research and reimbursable testing. Reported received and planned future funding substantially increased from 2015 through 2024 and is currently estimated to total almost \$15 billion.” (GOA, 2008) China is also making a major investment in technology and advanced weapons as part of its goal to be self-sufficient by 2025.

### **Summary**

Aviation and its associated technology have evolved from the first flights of the Wright Brothers to supersonic jets to devices in the high-hypersonic range. They can transition the planet in approximately 90 minutes or less. This same technology has advanced to the state where warring countries can deliver weapon systems to targets in under 10 minutes for what once took over 30 minutes or even hours. These advancements will require nations to reconsider their military and Civil Defense policies. Because of the speed at which technology can move, the time allotted to Observe, Orient, Decide, and Act has been vastly decreased. These short intervals may no longer provide the time necessary for humans to collect the needed information and make a launch/no launch decision. Going forward, such decisions may be made by complex systems employing Artificial Intelligence to collect, analyze, and decide the fate of the moment and the retaliatory actions that will

occur after that. This should leave us to wonder if we are on the cusps of Colossus: The Forbin Project.

## **Bibliography**

AE Toolbox. (2022, Mar 31). *Melting Points for 10 Common Metals*. Retrieved from [www.americanelements.com: https://www.americanelements.com/meltingpoint.html](https://www.americanelements.com/meltingpoint.html)

Aero Corner. (2021, June 15). *Thirteen fastest fighter Jets globally (+ 4 fastest jet aircraft)*. Retrieved from <https://aerocorner.com/blog/fastest-fighter-jets/>: <https://aerocorner.com/blog/fastest-fighter-jets/>

Blair, B. G. (2019, Oct). *The U.S. Nuclear Launch Decision Process (on warning of incoming Russian missile)*. Retrieved from [www.globalzero.org/](https://www.globalzero.org/wp-content/uploads/2020/11/Full-LOWTimeline.pdf): <https://www.globalzero.org/wp-content/uploads/2020/11/Full-LOWTimeline.pdf>

Boeing. (n.d.). *Boeing: Historical Snapshot: F-15 eagle tactical fighter*. Retrieved from [www.boeing.com: https://www.boeing.com/history/products/f-15-eagle.page](https://www.boeing.com/history/products/f-15-eagle.page)

Brimelow, B. &. (2018, March 4). *Hypersonic weapons can make virtually all missile defenses useless – and destabilize the world order*. Retrieved from [www.businessinsider.com: https://www.businessinsider.com/hypersonic-weapons-could-nullify-missile-defenses-2](https://www.businessinsider.com/hypersonic-weapons-could-nullify-missile-defenses-2)

Brimelow, B. (2018, April 30). *Russia, China, and the US are in a hypersonic weapons arms race – and officials warn the US could be falling behind*. Retrieved from [www.businessinsider.com: https://www.businessinsider.com/hypersonic-weapons-us-china-russia-arms-race-2018-4](https://www.businessinsider.com/hypersonic-weapons-us-china-russia-arms-race-2018-4)

Brockmann, K. &. (2022, Feb 4). *A matter of speed? Understanding hypersonic missile systems*. Retrieved from [sipri.org: https://sipri.org/commentary/topical-backgrounder/2022/matter-speed-understanding-hypersonic-missile-systems](https://sipri.org/commentary/topical-backgrounder/2022/matter-speed-understanding-hypersonic-missile-systems)

Cronk, T. M. (2021, May 3). *Defense official says hypersonics are vital to modernization strategy, battlefield Dominance*. Retrieved

from [www.defense.gov/](https://www.defense.gov/News/News-Stories/Article/Article/2593029/defense-official-says-hypersonics-are-v): <https://www.defense.gov/News/News-Stories/Article/Article/2593029/defense-official-says-hypersonics-are-v>

CSIS. (2021, July 31). CSIS Missile Defense Project. Retrieved from [missilethreat.csis.org](https://missilethreat.csis.org/missile/avangard/): <https://missilethreat.csis.org/missile/avangard/>

CSIS. (2021, Aug 2). CSIS Missile Defense Project. Retrieved from [missilethreat.csis.org/missile/](https://missilethreat.csis.org/missile/missile/df-17/#:~:text=Specifications%20The%20DF-17%20is%20solid-fueled%2C%20measures%20around%2011,as%20that%20used%20for%20China%E2%80%99): <https://missilethreat.csis.org/missile/missile/df-17/#:~:text=Specifications%20The%20DF-17%20is%20solid-fueled%2C%20measures%20around%2011,as%20that%20used%20for%20China%E2%80%99>

Delcker, J. (2019, Feb 8). *China leads research into hypersonic technology*: Report. Retrieved from [defense.pk/](https://defence.pk/pdf/threads/china-leads-research-into-hypersonic-technology-report.600978/): <https://defence.pk/pdf/threads/china-leads-research-into-hypersonic-technology-report.600978/>

Deloitte. (2020, April 9). *The rise of hypersonics*. Retrieved from [www2.deloitte.com](https://www2.deloitte.com/us/en/pages/energy-and-resources/articles/rise-of-hypersonics.html): <https://www2.deloitte.com/us/en/pages/energy-and-resources/articles/rise-of-hypersonics.html>

DoD. (2020). *Military and security developments involving the People's Republic Of China*. Retrieved from [media.defense.gov/](https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF): <https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF>

Electronic Products. (2019, April 11). *A brief history of electronic reliability in space – including today's risks and how to mitigate them*. Retrieved from [www.electronicproducts.com](https://www.electronicproducts.com/a-brief-history-of-electronic-reliability-in-space-including-to): Electronic Products. (2019, April 11). *A brief history of electronic reliability in space – including today's risks and how to mitigate them*. Retrieved from <https://www.electronicproducts.com/a-brief-history-of-electronic-reliability-in-space-including-to>

Eshel, T. (2011, April 11). *DARPA's HTV-2 fails to complete the second hypersonic flight test*. Retrieved from [defense-update.com/](https://defense-update.com/20110811_htv-2_falcon_second_test.html): [https://defense-update.com/20110811\\_htv-2\\_falcon\\_second\\_test.html](https://defense-update.com/20110811_htv-2_falcon_second_test.html)

FAA. (2022). Ch. 16. *Airplane flying handbook*. Retrieved from

www.faa.gov/: [https://www.faa.gov/regulations\\_policies/handbooks\\_manuals/aviation/airplane\\_handbook/media/17\\_afh\\_ch16.pdf](https://www.faa.gov/regulations_policies/handbooks_manuals/aviation/airplane_handbook/media/17_afh_ch16.pdf)

Força Aerea Brasileira. (2021, Dec 16). *FAB realiza primeiro teste de voo do motor aeronáutico hipersônico 14-X*. Retrieved from [fab-mil-br.translate.google.com/noticias/mostra/38395/](https://fab-mil-br.translate.google.com/noticias/mostra/38395/): <https://fab-mil-br.translate.google.com/noticias/mostra/38395/OPERA%C3%A7%C3%A3O%20CRUZEIRO%20-%20FAB%20realiza%20primeiro%20tes>

GOA. (2008, July). *Ballistic missile defense Actions are needed to improve the process of identifying and addressing combatant command priorities*. Retrieved from [www.gao.gov/](https://www.gao.gov/): <https://www.gao.gov/assets/gao-08-740.pdf>

Google Maps. (2022, Mar 20). *China to Japan, Korea, and Taiwan*. Retrieved from [www.google.com](https://www.google.com): <https://www.google.com>

Google Maps. (2022, March 20). *NYC to Orlando*. Retrieved from [www.google.com/maps/](https://www.google.com/maps/): <https://www.google.com/maps/dir/Orlando,+Florida/New+York,+NY/@34.5433045,-82.1817811,6z/data=!3m1!4b1!4m14!4m13!1m5!1m1!1s0x88e773d8fecdbc77:0xac3b2063ca5bf9e!2m2!1d-81.3789269!2d28.5383832!1m>

Holden, M. S.-U. (2002). *LENS Hypervelocity Tunnels and Application to Vehicle Testing at Duplicated Flight Conditions*. Retrieved from [arc.aiaa.org](https://arc.aiaa.org): <https://arc.aiaa.org/doi/10.2514/5.9781600866678.0073.0110>

India TV. (2020, Sept 18). *Global military spending in 2019 was the largest in a decade; China and India are in top 3: SIPRI*. Retrieved from [www.newsclick.in](https://www.newsclick.in): <https://www.newsclick.in/global-military-spending-2019-largest-decade-china-india-top-3-SIPRI>

Industry tap into news. (n.d.). *x51 Waverider Hypersonic Missile*. Retrieved from [www.industrytap.com](https://www.industrytap.com): <https://www.industrytap.com/hypersonic-missiles-make-us-defense-systems-obsolete/36491/x-51-waverider-hypersonic-attached-b-52-bomber>

1. Hank, J. M. (2008). *The X-51A Scramjet Engine Flight*

Demonstration Program. 15th AIAA International Space Planes and Hypersonic Systems and Technologies Conference (p. 7). AIAA.

Kopp, D. C. (2014, Jan 27). *Defeating cruise missiles*. Retrieved from [www.ausairpower.net](http://www.ausairpower.net): <http://www.ausairpower.net/Analysis-Cruise-Missiles.html>

Kynvin, J., & Guardian Digital Agency. (2011, November 25). *Speed comparison chart*. Retrieved from [visual.ly/](https://visual.ly/): <https://visual.ly/community/Infographics/transportation/speed-comparison-chart>

Lockie, A. (2019, April 2). *China's missiles could dust the US military in minutes – here's what would happen if they tried*. Retrieved from [www.businessinsider.co.za/](https://www.businessinsider.co.za/): <https://www.businessinsider.co.za/chinese-missiles-could-hit-us-jets-ships-in-pacific-but-at-great-risk-2019-3>

Macias, A. (2018, Mar 21). *Russia and China are 'aggressively developing' hypersonic weapons – here's what they are and why the US can't defend against them*. Retrieved from [www.cnbc.com](https://www.cnbc.com/): <https://www.cnbc.com/2018/03/21/hypersonic-weapons-what-they-are-and-why-us-cant>

Malik, T. (2012, April 23). *Death of DARPA's superfast hypersonic glider explained*. Retrieved from [www.space.com/](https://www.space.com/): <https://www.space.com/15388-darpa-hypersonic-glider-demise-explained.html>

Military-Today. (n.d.). *Hwasong 8 ballistic missile with a hypersonic glide vehicle*. Retrieved from [www.military-today.com/missiles/hwasong\\_8.htm](https://www.military-today.com/missiles/hwasong_8.htm): [https://www.military-today.com/missiles/hwasong\\_8.htm](https://www.military-today.com/missiles/hwasong_8.htm)

Military-Today. (n.d.). *Shaurya short- and medium-range ballistic missile*. Retrieved from [www.military-today.com/missiles/shaurya.htm](https://www.military-today.com/missiles/shaurya.htm): <https://www.military-today.com/missiles/shaurya.htm>

Military-Today. (n.d.). *Tsyron anti-ship cruise missile*. Retrieved

from [www.military-today.com/missiles/tsyrkon.htm](http://www.military-today.com/missiles/tsyrkon.htm):  
<https://www.military-today.com/missiles/tsyrkon.htm>

Morabito, D. D. (2002, Aug 15). *The Spacecraft Communications Blackout Problem Encountered during Passage or Entry of Planetary Atmospheres*. Retrieved from [ipnpr.jpl.nasa.gov/https://ipnpr.jpl.nasa.gov/progress\\_report/42-150/150C.pdf](https://ipnpr.jpl.nasa.gov/progress_report/42-150/150C.pdf)

N.O.A.A. ((n.d.)). *Speed of sound*. Retrieved from [www.weather.gov/https://www.weather.gov/media/epz/wxcalc/speedOfSound.pdf](https://www.weather.gov/media/epz/wxcalc/speedOfSound.pdf)

NASA. (2006, Jan 1). *Integrated system health management (ISHM) technology demonstration project final report*. Retrieved from [www.researchgate.net/https://www.researchgate.net/publication/246487548\\_Integrated\\_System\\_Health\\_Management\\_ISHM\\_Technology\\_Demonstration\\_Project\\_](https://www.researchgate.net/publication/246487548_Integrated_System_Health_Management_ISHM_Technology_Demonstration_Project_)

NASA. (2019). *Hypersonic tunnel facility*. Retrieved from [www1.grc.nasa.gov/https://www1.grc.nasa.gov/facilities/htf/](https://www1.grc.nasa.gov/facilities/htf/)

NASA. (2021, May 13). *General thrust equation*. Retrieved from [www.grc.nasa.gov/https://www.grc.nasa.gov/WWW/k-12/airplane/thrsteq.html](https://www.grc.nasa.gov/WWW/k-12/airplane/thrsteq.html)

NASA. (2022, dec 25). *abc.com*. Retrieved from [Nasa.gov: nasa.gov](https://nasa.gov)

NASA. (n.d.). *Orbiter Thermal Protection System*. Retrieved from [www.nasa.gov/https://www.nasa.gov/centers/kennedy/pdf/167473main\\_TPS-06rev.pdf](https://www.nasa.gov/centers/kennedy/pdf/167473main_TPS-06rev.pdf)

NATO. (n.d.). *NATO on the map*. Retrieved from [www.nato.int/nato-on-the-map/](https://www.nato.int/nato-on-the-map/): NATO. (n.d.). *NATO on the map*. Retrieved from <https://www.nato.int/nato-on-the-map/#lat=53.06502518704667&lon=10.138445588401366&zoom=0&layer=1>

Nelson, D. (2020, Mar 14). *Mach speed: From Mach 1 to Mach 3 speed and beyond*. Retrieved from [sciencetrends.com/https://sciencetrends.com/mach-speed-breakdown-examples-mach-1-2-3-beyond/#:~:text=The%20range%20of%20speed%20that%20exists%20from%20Mach,molecules%20of%20oxyg](https://sciencetrends.com/mach-speed-breakdown-examples-mach-1-2-3-beyond/#:~:text=The%20range%20of%20speed%20that%20exists%20from%20Mach,molecules%20of%20oxyg)

Nilsen, T. (2021, July 19). *Northern fleet frigate test fires Tsirkon*

hypersonic missile. Retrieved from thebarentsobserver.com/: <https://thebarentsobserver.com/en/security/2021/07/northern-fleet-frigate-test-fires-tsirkon-hypersonic-missile>

Pileggi, V. (2019, Jan 12). *Pekin anuncia el despliegue de UN misil "asesino de portaaviones" después de Que UN buque de guerra estadounidense navegue cerca de los islotes del mar de China meridional*. Retrieved from desarrollodefensaytecnologi: <https://desarrollodefensaytecnologi>

Plummer, M. &. (2011, August 11). *Falcon HTV-2 hypersonic plane loses control in Mach 20 test*. Retrieved from abcnews.go.com/: <https://abcnews.go.com/Technology/hypersonic-flight-darpa-launches-htv-plane-test-loses-contact/story?id=14280849>

Precision Ceramics EU. (2021, Nov 23). *Hypersonic speed & ultra-high temperature ceramics*. Retrieved from Precision Ceramics EU. (2021, November 23). [Hypeprecision-ceramics.com/EU/high-temperature-ceramics/](https://precision-ceramics.com/EU/high-temperature-ceramics/): <https://precision-ceramics.com/eu/high-temperature-ceramics/>

Russian Defense Ministry. (2020, Oct 7). *Watch successful launch of Russia's zircon hypersonic cruise missile*. . Retrieved from sputniknews.com/: <https://sputniknews.com/20201007/watch-successful-launch-of-russias-zircon-hypersonic-cruise-missile-1080691630.html>

Russian Defense Ministry/TASS. (2020, January 16). *A closer look at rearmament of Russian strategic nuclear forces*. Retrieved from southfront.org: <https://southfront.org/closer-look-at-rearmament-of-russian-nuclear-forces/>

Russian Federation. (2000, June 28). *The foreign policy concept of the Russian Federation*. Retrieved from nuke.fas.org/: <https://nuke.fas.org/guide/russia/doctrine/econcept.htm#:~:text=The%20Russian%20Federation%20is%20pursuing%20an%20independent%20and,states%20and%20i>

Science Daily. (2021, September 19). *Speed of sound*. Retrieved from www.sciencedaily.com/: [https://www.sciencedaily.com/terms/speed\\_of\\_sound.htm](https://www.sciencedaily.com/terms/speed_of_sound.htm)

Shalini, S. (2018, Dec 17). *Russia tests nuclear-capable Mach 20*



*hypersonic missile successfully, overtaking US capability.* Retrieved from [www.ibtimes.com/](http://www.ibtimes.com/): <https://www.ibtimes.com/russia-tests-nuclear-capable-mach-20-hypersonic-missile-successfully-overtaking-us-2746>

Smithsonian National Air and Space Museum. (2022). *Hypersonic flight.* Retrieved from [airandspace.si.edu/](http://airandspace.si.edu/): <https://airandspace.si.edu/stories/editorial/hypersonic-flight>

Speier, R. H. (2017). *Hypersonic missile nonproliferation.* Retrieved from [www.rand.org/](http://www.rand.org/): [https://www.rand.org/content/dam/rand/pubs/research\\_reports/RR2100/RR2137/RAND\\_RR2137.pdf](https://www.rand.org/content/dam/rand/pubs/research_reports/RR2100/RR2137/RAND_RR2137.pdf)

University of Washington. (2015, Oct 9). *General features.* Retrieved from [www.aawashington.edu/](http://www.aawashington.edu/): <https://www.aawashington.edu/research/ramaccel/features>

USAF. (n.d.). *X-51A Waverider.* Retrieved from [www.af.mil](http://www.af.mil/): <https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104467/x-51a-waverider/>

VOA Graphics. (2022, Feb 2). *Graphic: Which countries are working on hypersonic weapons?* Retrieved from [www.voanews.com](http://www.voanews.com/): <https://www.voanews.com/a/graphic-which-countries-are-working-on-hypersonic-weapons-/6423803.html>

Wikipedia. (2003, Nov 28). *OODA loop.* Retrieved from [en.wikipedia.org/wiki/OODA\\_loop](http://en.wikipedia.org/wiki/OODA_loop): [https://en.wikipedia.org/wiki/OODA\\_loop](https://en.wikipedia.org/wiki/OODA_loop)

Wilson, J. (2020, May 22). *The electronics design challenges of hypersonic flight.* Retrieved from [www.militaryaerospace.com](http://www.militaryaerospace.com/): <https://www.militaryaerospace.com/sensors/article/14176531/the-electronics-design-challenges-of-hypersonic-flight>

Xinhua. (2021, July 1). *Xi says Chinese people will never allow foreign bullying, oppressing, or subjugation.* Retrieved from [www.xinhuanet.com](http://www.xinhuanet.com/): [https://www.xinhuanet.com/english/special/2021-07/01/c\\_1310037372.htm](https://www.xinhuanet.com/english/special/2021-07/01/c_1310037372.htm)

# 13. Acoustic Weapons

**By Professor Randall K. Nichols, Professor Candice M. Carter, Dr. Robert McCreight**

## **Student Learning Objectives**

- The student will take a brief sojourn into the science of audiology to understand why acoustic countermeasures work.
- The student will explore acoustic countermeasures against hostile UAS (especially Swarms) and their dual use as Identify Friend or Foe (IFF) vectors for UAS characterization.
- The student will learn about Havana Syndrome.
- The student will be re-introduced to the *problem* of countering hostile use of UAS, UV / Unmanned boats / UUV against US national defense interests. This chapter focuses on the Spratlys, a tiny set of islands in the South China Seas. The Spratlys are at the forefront of China's military expansion and control program (Corr, 2018). In this tiny island sanctuary, drones and unmanned boats are the intelligence weapons of choice. Intrusions on US capital ships have already begun and could escalate to become the flashpoint for WW III. [\[1\]](#) The focus will be on the use of acoustic weapons at short range
- The student will be updated on suspicious drone use by China for ISR missions in the South China Seas in light of the Russian invasion of Ukraine and China's signals that Taiwan might suffer the same fate.
- The concept of the *Screamer* will be postulated.

## **Disclaimer**

This chapter represents a review of material in Chapter 19 of our ***Unmanned Aircraft Systems in the Cyber Domain, 2nd Edition***. (Nichols & Mumm, *Unmanned Aircraft Systems in the Cyber*

Domain, 2nd Edition., 2019). It also updates original research into drone use by China in the South China Seas (SCS) by the authors, which became the basis for Chapters 9, 12, & 14 in our recent textbook **Unmanned Vehicle Systems & Operations on Air, Sea & Land**. (Nichols & Ryan, Unmanned Vehicle Systems & Operations on Air, Sea & Land, 2020).

In addition, the authors will cover the relation of sound to the *Havana Syndrome* and, finally, detail an update in the SCS of suspicious drone incidents. (Neo, Aerial, and UUV suspicious drone incidents in the SCS, 2019-2022) Chapter 15 in this textbook will cover Cyber Weapons and CBRN critical infrastructure facilities. Permissions of the Wildcat writing team, managing editor, and copyright holders have been received.

### **Detection Signatures Review**

Recall from **Chapter 8 Stealth**, in the author's textbook **Unmanned Aircraft Systems in the Cyber Domain, 2nd Edition**, (Nichols & Mumm, Unmanned Aircraft Systems in the Cyber Domain, 2nd Edition., 2019) that **their signatures detect UAS / UAVs**: noise (acoustic), optical (visible), infrared (thermal) and radar (radio). "These acoustic or electromagnetic emissions occur at the following wavelengths: (Austin, 2010)

1. A) Noise (acoustic) [16 m-2 cm, or 20 – 16000 Hz]
2. B) Optical (visible) [0.4 – 0.7 um]
3. C) Infrared (thermal) [0.75 um – 1 mm]
4. D) RADAR (radio) [3 mm – 3 cm]" (Austin, 2010)

In the discussion on stealth, it was presented that "If the designer is to reduce the vehicle detectability to an acceptable risk level, it is necessary to reduce the received emissions or reflection of the above wavelengths (expressed as frequencies) below the threshold *signature* value. A good portion of the UAS signatures is a function

of the operating height of air vehicle.” (Austin, 2010) The concept of frequency as a fifth realm was elucidated in terms of targets, battlespace, and wavelengths. One of the parameters, range, was a serious limitation on performance. The range has a significant impact on radio transmission. Depending on the environment, the strength of a received signal,  $T$ , is a function of the square or fourth power of a distance,  $d$ , from the transmitter. (Adamy D. -0., 2015) The EMS was presented with emphasis on sound frequencies, many out of human hearing range. The UAS designer’s upper end of noise – Stealth acceptability is 17,150 Hz. **The full Stealth range is 20 Hz – 17,150 Hz.**

**Essentials of Audiology**

*Why would a UAS going at 100 mph or more be susceptible to a loud noise hitting the MEMS under the UAS rotors or the rotors themselves? Additionally, why would this same noise or variation thereof be capable of characterization the UASs as a hostile or friendly power? It is not something we can just take for granted without understanding the essentials of audiology underlying the process.*

**Audiology Fundamentals**

The science of sound is called *acoustics*, a branch of physics. Table 13.1 displays the principal physical quantities in MKS, cgs, and English units. Table 13.1 can be found in most engineering, physics, or medical textbooks. (Entokey, 2019) It is the starting point of a trip uphill to resonance frequencies.

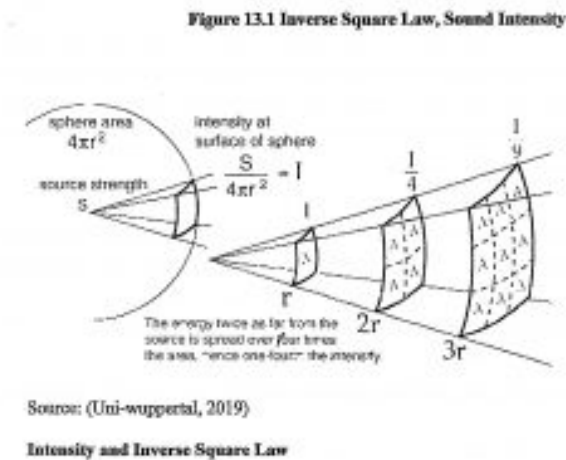
**Table 13.1: Principal Physical Properties** (Entokey, 2019)  
and (Gelfand S. A., 2009)

| Quantity            | Formula          | MKS<br>(SI.)Units         | Cgs Units                 | Comments   | English<br>Units   |
|---------------------|------------------|---------------------------|---------------------------|--|--|
| Mass (M)            | M                | kilogram<br>(kg)          | gram (g)                  | 1kg = 103 g<br>1kg =<br>2.2046 lbs   | pounds<br>(lbs)  |
| Time (t)            | t                | seconds,<br>(s)           | s                         |  | s  |
| Area (A)            | A                | m <sup>2</sup>            | cm <sup>2</sup>           | 1 m <sup>2</sup> = 104<br>cm <sup>2</sup>  | ft <sup>2</sup>  |
| Displacement<br>(d) | d                | meter<br>(m)              | centimeter<br>(cm)        | 1m = 102<br>cm   | ft   |
| Velocity (v)        | v = d/t          | m/s                       | cm/s                      | 1 m/s =<br>102 cm/s  | ft/s   |
| Acceleration<br>(a) | A = v/t          | m/s <sup>2</sup>          | cm/s <sup>2</sup>         | 1 m/s <sup>2</sup> =<br>102 cm/s <sup>2</sup>  | ft/s <sup>2</sup>  |
| Force (F)           | F = MA =<br>Mv/t | kg x m/<br>s <sup>2</sup> | g x cm <sup>2</sup>       | 1N = 105<br>dynes  | 1lbf = 1 lb<br>x<br>32.174049<br>ft -lbs<br>/s <sup>2</sup> =<br>9.80665<br>m/s <sup>2</sup> |
|                     | Mv =<br>Momentum | newton<br>(N)             | dyne                      |  |  |
| Pressure (p)        | p = F/ A         | N /m <sup>2</sup>         | dynes<br>/cm <sup>2</sup> | 20 μPa = 2<br>x 10 <sup>-5</sup> N/<br>m <sup>2</sup>  | Psi = lbf<br>/in <sup>2</sup>  |
|                     |                  | Pascal<br>(Pa)            | microbar<br>(μbar)        | reference<br>value   | 1 N/m <sup>2</sup> =<br>0.000145<br>psi  |
| Work (W)            | W =Fd            | N x m                     | dyne x cm                 | 1 j = 107<br>erg/s   | BTU  |
|                     |                  | Joule                     | erg                       | Energy<br>-capability<br>to do<br>Work.<br>Potential<br>energy for<br>a body at<br>rest and<br>kinetic<br>energy for<br>a body in<br>motion. | [British<br>Thermal<br>Unit]<br>1BTU =<br>1055.056<br>joules                                 |

|               |                        |                  |                   |                                    |                    |
|---------------|------------------------|------------------|-------------------|------------------------------------|--------------------|
| Power (P)     | $P = W/t =$            | Joules/s         | erg/s             | $1 \text{ w} = 1 \text{ J/s}$      | $1 \text{ watt} =$ |
|               | $Fd/t = Fv$            | watt (w)         | watt (w)          | $= 10^7$                           | 3.412              |
|               | $I = P/A$              |                  |                   | erg/s                              | BTU/hr             |
| Intensity (I) | $I = P / 4\pi r^2$     |                  |                   |                                    |                    |
|               | Based on sphere radius | w/m <sup>2</sup> | w/cm <sup>2</sup> |                                    |                    |
|               |                        |                  |                   | 10 <sup>-12</sup> w/m <sup>2</sup> | reference value    |

Sources: (Entokey, 2019) and (Studios, 2017)

Figure 13.1: Inverse Square Law, Sound Intensity



Source: (Uni-wuppertal, 2019)

**The intensity and Inverse Square Law**

“Sound radiates outward in every direction from its source. This constitutes a sphere that gets larger and larger with increasing

distance from the source.” (Entokey, 2019) Figure 13.1 shows the relationship between Intensity and the Inverse Square Law. (Uniwuppertal, 2019) Intensity (I) (power divided by area) decreases with distance from the original source because a finite amount of power is spread over increasing surface area. (Entokey, 2019) Proportionately less power falls on the same unit of area with increasing distance from the source. (Gelfand, 2004)

“Four important and understandable relationships to note are that power is equal to pressure squared,  $P = p^2$ , pressure is equal to the square root of power,  $p = \sqrt{P}$ , intensity is proportional to pressured squared,  $I \approx p^2$ , and pressure is proportional to intensity,  $p \approx \sqrt{I}$ . This makes it easy to convert between sound intensity and sound pressure.” (Entokey, 2019) These relations yield a few more to relate sound pressure, sound intensity, and distance  $r$ . Given to pressures  $p_1$  and  $p_2$  at distance  $r_1$  and  $r_2$ , they are proportional:  $p_2 / p_1 = r_1 / r_2$ ; and factoring in intensities at  $I_1$  and  $I_2$ , gives  $I_2 / I_1 = (r_1 / r_2)^2$ .

Finally,  $r_2 / r_1 = p_2 / p_1 = \sqrt{I_2 / I_1}$ . (TRS, 2018)

### **Decibels** (Adamy D. , 2001) (Gelfand S. A., 2009)

Sound magnitudes, intensities, and pressures vary over an enormous range. We use decibels (dB) to express sound values. Decibels takes advantage of ratios and logarithms. Ratios are used so that physical magnitudes can be stated in relation to a reference value that has meaning to us. The reference point chosen is the softest sound that normal people can hear. The reference value has an intensity of  $10^{-12}$  w/m<sup>2</sup> ( $10^{-16}$  w/cm<sup>2</sup>). In terms of sound pressure, the reference value is:  $2 \times 10^{-5}$  N/m<sup>2</sup> or 20  $\mu$ Pa ( $2 \times 10^{-4}$  dynes/cm<sup>2</sup>). An interesting Geek bar bet is what is the logarithm of all 2:1 ratios, 8:4, 20, 20:10, 100:50, etc.? Even though the distance between absolute numbers gets wider, 1,4,10, 50..., the logarithms of the 2:1 ratios are the same at 0.3. Another interesting factoid about ratios is that the units generally cancel out.

The general decibel formula in terms of power level (PL) is as follows (Gelfand, 2004):

$$\text{PL} = 10 \log P / P_o \quad \text{Equation 13.1}$$

Where P = power of the sound measured, and  $P_o$  is the reference power to be compared.

The general decibel formula in terms of power level (IL) is as follows (Gelfand, 2004):

$$\text{IL} = 10 \log I / I_o \quad \text{Equation 13.2}$$

Where I = intensity of the sound measured, and  $I_o$  is the reference intensity to be compared.  $I_o$  is given as  $10^{-12} \text{ W/m}^2$ .

The general decibel formula for sound pressure level (SPL) is obtained by replacing all of the intensity values with the corresponding values of pressure squared because ( $I \approx p^2$ ).

$$\text{SPL} = 10 \log p^2 / p_o^2 \quad \text{Equation 13.3}$$

Where p is the measured sound pressure (in  $\text{N/m}^2$ ) and  $p_o$  is the reference sound pressure of

$2 \times 10^{-5} \text{ N/m}^2$ . A more convenient form of this equation recognizes that  $\log x^2 = 2 \log x$ . (Gelfand, 2004)

$$\text{SPL} = 20 \log p / p_o \quad \text{Equation 13.4}$$

Equation 13.4 is the common formula for SPL. A positive decibel value means that the sound pressure level is greater than the reference. The decibel value of the reference is 0 because reference value / reference value = 1 and  $10 \log 1 = 0$ . This does not mean any sound; it means the sound measured equals the reference point. A negative value of decibels means that the sound magnitude is lower than the reference. (Gelfand S. A., 2009)

Figure 13.2 shows common decibel and Intensity levels within the hearing range. This does not consider the environment, frequency differences, or noise (discussed presently). It does show the ease with which decibels may be used to rank the sound intensity levels, which vary greatly in magnitude. [2]Hearing aids are effective from about 6 – 90 decibels. Above 90 dB, they can dampen but not



eliminate the very loud sounds unless there is a complete loss of hearing.

**Figure 13.2 shows common decibel and Intensity levels within the hearing range**

Approximate sound levels and intensities within human hearing range

| Source of sound      | Intensity level (dB) | Intensity ( $\text{W m}^{-2}$ ) | Perception   |
|----------------------|----------------------|---------------------------------|--------------|
| jet plane at 30 m    | 140                  | 100                             | extreme pain |
| threshold of pain    | 125                  | 3                               | pain         |
| pneumatic drill      | 110                  | $10^{-1}$                       | very loud    |
| siren at 30 m        | 100                  | $10^{-2}$                       |              |
| loud car horn        | 90                   | $10^{-3}$                       | loud         |
| door slamming        | 80                   | $10^{-4}$                       |              |
| busy street traffic  | 70                   | $10^{-5}$                       | noisy        |
| normal conversation  | 60                   | $10^{-6}$                       | moderate     |
| quiet radio          | 40                   | $10^{-8}$                       | quiet        |
| quiet room           | 20                   | $10^{-10}$                      | very quiet   |
| rustle of leaves     | 10                   | $10^{-11}$                      |              |
| threshold of hearing | 0                    | $10^{-12}$                      |              |

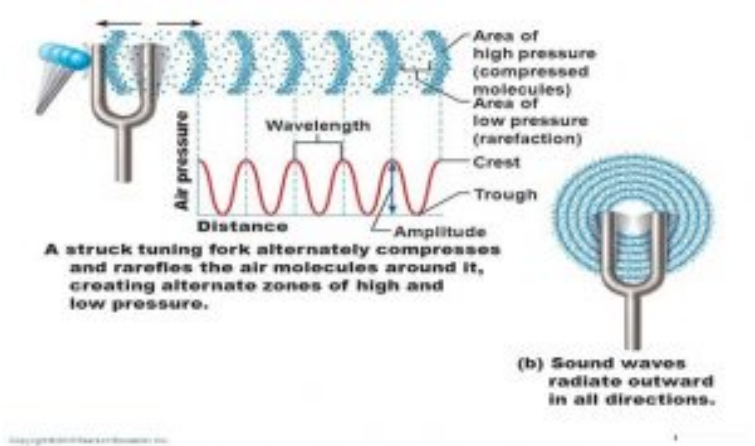
Source: (slideshare.net, 2019)

**The Nature of Sound**

“Sound is defined as a form of vibration that propagates through the air in the form of a wave. Vibration is the to-and-fro motion (aka oscillation) of an object. Examples are playground swings, tuning fork prongs, air molecules, and UAS rotor blades [circular motion]. The vibration is called *sound* when it is transferred from air molecule to air molecule. This transfer may be simple, like a tuning fork, or a complex pattern like the din in a school cafeteria. Naturally occurring sounds are very complex.” (Entokey, 2019) UAS sounds are not natural and are supported by machinery, hardware, and

software. Three weaknesses of the UAS are the MEMS, gimbal assembly, and rotors. Although stealth mechanisms may be employed to reduce noise emissions, the former parts are exposed. They do produce discernable signatures.

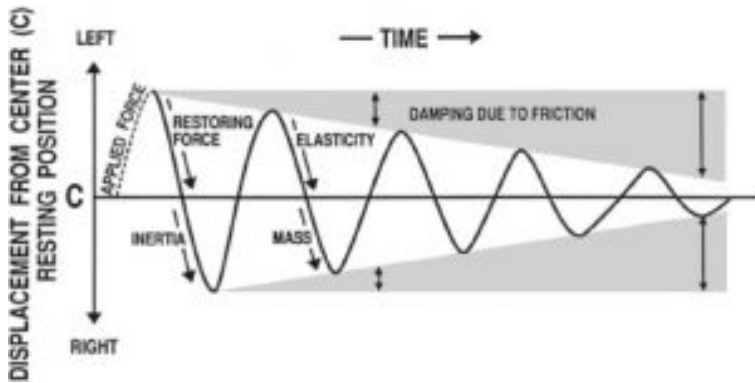
**Figure 13.3: Tuning for Oscillations** (Pierson, 2019)



Source: (Pierson, 2019)

A tuning fork illustrates the oscillations of sound. After being struck, the tuning fork vibrates with a simple pattern that repeats itself over time. (Entokey, 2019) Figure 13.3 shows that the tuning fork, when struck, exerts a force on the air molecules which alternatively exerts a high pressure (compression) and a low pressure (rarefaction) zones. The zones exhibit wave amplitude and wavelength as a function of air pressure and distance. The sound wave is distributed 360 degrees through the air.

**Figure 13.4: Tuning fork oscillations over time** (Entokey, 2019)



Source: (Entokey, 2019)

Figure 13.4 diagrams a tuning fork's oscillations over time. Sounds that are associated with simple harmonic motion are called pure-tones. Vertical displacement amount of the tuning fork prong displacement around its resting position. Distance from left to right represents the progression of time. One complete round-trip or replication of an oscillating motion is called a cycle. The number of cycles occurring in one second is the *frequency*. The duration of one cycle is called it's *period*. This form of motion occurs when a force is applied to an object having properties of elasticity and inertia. Simple harmonic motion (SHM) shows the same course of oscillations as in Figure 13.4 because they repeat themselves at the same rate until friction causes dampening of the waveform. (Entokey, 2019) and (Gelfand S. A., 2009)

### Other Parameters of Sound waves

Probably the most useful SHM waveform is the sinusoidal wave or sign wave.[\[3\]](#)

The number of times a waveform repeats itself in one second is known as the frequency or cycles per second (CPS). (Gelfand S. A., 2009)Two useful relationships are:  $f = 1/ t$  or  $t = 1/f$ ; where  $f$

is the frequency in cps and  $t$  is the period in seconds. *Amplitude* denotes the magnitude of the wave. The *peak-to-peak* amplitude is the total vertical distance between negative and positive peaks. The peak amplitude is the distance from the baseline to one peak. The magnitude of sound at any instant is the *instantaneous amplitude*. Wavelength ( $\lambda$ ) is the distance traveled between one peak and the next. (Gelfand, 2004)

The wavelength formula is:  $\lambda = c / f$ , where  $c$  is the speed of sound in air (344 m/s.  $f$  is the frequency of sound in Hz. Similarly, frequency is inversely proportional to wavelength or  $f = c / \lambda$ . (Gelfand S. A., 2009) Another interesting sound parameter is *Pitch*. Pitch is the quality of sound and especially a musical tone, governed by the rate of vibrations producing it. It is the degree of highness or lowness of sound. (Merriam-Webster, 2019)

### **Complex waves**

When two or more pure-tone waves are combined, the result is a *complex wave*. (Gelfand, 2004) They may contain any number of frequencies. Complex periodic waves have waveforms that repeat themselves. If they don't, they are *aperiodic*. Combining waves may reinforce themselves or cancel themselves whether they are in phase or out. The lowest frequency component of a complex periodic wave (like a combination of sign waves) is called its *fundamental frequency*. (Gelfand, 2004)

*Harmonics* are a whole number or integral multiples of the fundamental frequency. Waveforms show how amplitude changes with time. (Gelfand, 2004) Fourier's Theorem shows that complex sound waves can be mathematically dissected into pure tones.

Of more interest to UAS designers are aperiodic sounds made up of components that are not harmonically related and do not repeat themselves over time. The extreme cases of aperiodic sounds are transients and random noise. A *transient* is an abrupt sound that is very brief in duration. *Random noise* has a completely random waveform, so it contains all possible frequencies in the same average amplitude over the long run. *Random noise* is also called

white noise, like white light, because all possible frequencies are represented.

### **Standing Waves and Resonance**

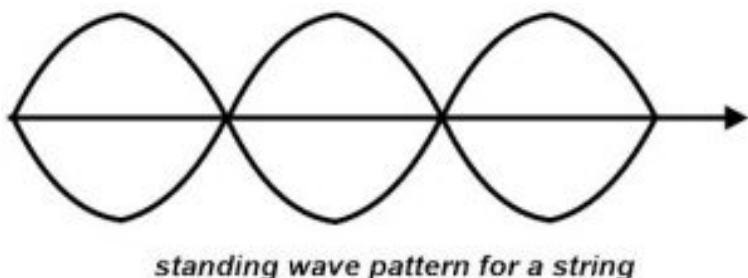
We have arrived at the crux of the acoustic countermeasures discussion, the natural or resonating frequency, which is defined as:

“The frequency(ies) at which a body or medium vibrates most readily is called its natural or resonant frequency(ies).” (Gelfand S. A., 2009) Differences in resonance frequency ranges enable different devices to act as filters by transmitting energy more readily for certain high, low, or band-pass frequencies. UAS with multiple rotors circulates the rotors to gain lift and/or hold steady / or descend in altitude. Four, six, eight – rotor UAS maintains control via internal SCADA systems and sends critical information through a MEMS component located at the bottom of rotors. Rotor frequencies are coordinated, monitored, and position-controlled through the MEMS and in-board computers. Even though the rotor(s) motions are spinning circularly, the sound wave generation is not curvilinear or aperiodic but transferred up through the Y-axis and back again to its base as it ascends in altitude. There is a tendency to maintain equilibrium in terms of the position of the UAS.

The author contends that the UAS rotor systems act like vibrating strings, and this approach can approximate resonance frequency information. An example of a vibrating spring is when you “pluck” a guitar. The waves initiated move outward toward the two tied ends of the string. The waves are then reflected, and they propagate in opposite directions. The result is a set of waves moving toward each other, resulting in a perturbation sustained by continuing reflections from the two ends. The superimposed waves interact and propagate and appear as a pattern that is standing still. Peaks (maximum displacement) and no displacement (baseline crossings) occur at fixed points along the string. Places along the spring where zero displacement in the standing wave pattern are called nodes.

(Gelfand, 2004) Locations where the maximum displacement occurs are called antinodes.

**Figure 13.5: Standing wave** (Administrator, 2015)



Source: (Administrator, 2015)

“The *fundamental frequency* is defined as the lowest frequency of a periodic waveform. It is generally denoted as ‘f’. The lowest resonating frequency of a vibrating object is called the fundamental frequency.” (Administrator, 2015)

“*Harmonic is a frequency, which is an integer multiple of the fundamental frequency.* The forced resonance vibrations of an object are caused to produce standing waves. At the natural frequency, it forms a standing wave pattern. These patterns are created at specific frequencies; they are called Harmonic Frequencies of Harmonics.” (Administrator, 2015)

“The sound produced by a waveform at its harmonic frequency is very clear, and at other frequencies, we get noise and cannot hear the clear sound of waves. Harmonics may occur in any shaped waveforms, but mostly they occur in sine waves only. Non – sinusoidal waveforms, like triangular and sawtooth waveforms, are constructed by adding together the harmonic frequencies. The word harmonic is generally used to describe the distortions caused

by different un- desirable frequencies called noise, of a sine wave.” (Administrator, 2015)

“Node and antinodes occur in a waveform. So, the waves have a harmonic frequency in them. The fundamental frequency is the smallest frequency in a harmonic. Hence there is only a single antinode occurs between them. This antinode is in the middle of the two nodes. So, from this, we can say that the guitar string produces the longest wavelength and the lowest frequency.” (Administrator, 2015)

“The lowest frequency produced by any instrument is called the *fundamental frequency*. This is also known as the first harmonic of the wave. In words of the fundamental frequency, harmonics are the integer multiples of the fundamental frequency.” (Ex:  $f, 2f, 3f, 4f$ , etc.... are harmonics.) (Administrator, 2015)

“Because of multiple integers of the fundamental frequency, we will have n number of harmonics like 1st harmonic, 2nd harmonic, 3rd harmonic, and so forth.” (Administrator, 2015). “The fundamental frequency is also called as *First harmonic*. In the first harmonic, we have two nodes and one antinode. The numbers of antinodes are equal to the integer multiples of specific harmonics. i.e., for 1st harmonic we have 1 antinode, for 2nd harmonic, we have 2 antinodes, etc.” (Administrator, 2015)

The formula for the string’s resonant frequency  $F_0$  is:

$$F_0 = \frac{1}{2L} \times \sqrt{T/M} \quad \text{Equation 13.5}$$

$F_0$  is resonance frequency in Hz,  $T$  is Tension,  $M$  is Mass,  $L = \lambda / 2$  and  $f = c / \lambda$ , and  $c$  = speed of sound.  $L$  = length of the string. (Gelfand, 2004) The string’s lowest resonant frequency is  $f = c / 2L$ , but Eq. 13.5 considers that the speed of sound is different for a vibrating string than air.

### **In terms of UAS. Countermeasures, why are Acoustics so important?**

They are important because:

- Offensive systems use ultrasonic frequency resonance
- It cannot be heard by humans when used to intercept a drone
- Passive systems are difficult, if not impossible, to detect
- Able to identify and track drones based on acoustic and visual signature
- Acoustic detection systems are limited in range ~ 350 ft. to 500+ ft. due to environmental variables. Still, commercial companies like LRAD Corporation have developed long-range acoustic devices that can detect a UAS up to a mile away at altitude. (LRAD, 2019)
- It can be a cost-effective way to defend a small area –especially against Swarm Attacks. (Nichols R. K., 2019) (Nichols & al., Counter Unmanned Aircraft Systems Technologies, and Operations, 2020)

### **What are the Acoustic Detection Issues?**

Detection relies on the uniqueness of the UAS and hearing capabilities at low frequencies:

- Detects drones by recognizing the unique sounds produced by their motors
- Rely on a library of sounds produced by known drones, then matched to sounds detected in the operating environment.
- The human ear is a problem for the designer.
- It is most sensitive to frequencies around 3500 Hz and can hear sound down to a practical threshold of 10 dB
- For a given sound pressure level, attenuation of sound with distance in the air and insulating material varies as the square of the sound frequency.
- Low-frequency sound presents a greater problem for UAS stealth design.
- The greater noise problem is posed by smaller UAS using piston engines.
- Sound comes from their internal combustion and exhaust systems.



- Sound emission can be reduced with sound-absorptive materials, silencers, and mufflers and by directing the intake and exhaust manifolds upward.
- The level of sound detected depends on the level of background noise for sound contrast.
- Limited range to 500 feet (experimental and research – not commercial or military)
- Noisy backgrounds (airports, city downtown) limit detection & interdiction
- Drone tuning (changing the stock propellers) limits detection / Interdiction. (Nichols & al., Counter Unmanned Aircraft Systems Technologies, and Operations, 2020) (Nichols R. K., 2019)

### **Can UAS acoustic signatures be reduced?**

Yes because:

- Aircraft noise may be the first warning of its presence
- However, it may not immediately be directionally/locatable for detection
- UAS noise emanates predominantly from vortices, tips of wings, rotors, or propellers
- Lowering wingspan or blade span enhances acoustical stealth
- Conventional propulsion systems are a concern because of the noise of combustion
- Electric motors develop virtually no noise
- Reducing the mass and aerodynamic drag of the UAS reduces noise generation (Nichols & al., Counter Unmanned Aircraft Systems Technologies, and Operations, 2020)(Nichols R. K., 2019)

### **Is Acoustic Quieting possible?**

“Yes, under certain conditions:

- Disguise sounds from sensors to eliminate their noise and passive echoes
- The Navy used “Acoustic superiority” to mask the detection of US submarines
- Acoustic technology is “passive,” meaning it is engineered to receive pings and “listen” without sending out a signal which might reveal its location to an enemy.
- Increased use of lower frequency active sonar and non-acoustic methods of detecting.”(Nichols R. K., 2019) (Austin, 2010) (Nichols & al., Counter Unmanned Aircraft Systems Technologies, and Operations, 2020)

### **What is an Acoustical attack on the UAS's Gyroscope?**

There are two possibilities: compromising the sound source or drone on drone attack:

#### *Compromising the Sound Source*

- UAM with speakers (consider police and military operations or search-and-rescue operations)(Usenix.org, 2019)
- Counter the source of the sound from the speaker with a different frequency sound
- A jamming attack aims to generate ultrasonic noises and cause continuous membrane vibration on the sensor, making the measurements impossible.
- The level of noise causes performance degradation.

#### *Drone on Drone Attack*

- Taking a picture of a moving object from UAM,
- An adversary drone equipped with a speaker could steer itself toward a victim drone and generate a sound with the resonant frequency of the victim's gyroscope to drag it down(Usenix.org, 2019) [\[4\]](#)

## **How has the Long-Range Acoustic Device (LRAD) been used as a sonic weapon?**

It has been used primarily for denying GPS navigation: [\[5\]](#)

### ***GPS Denied Navigation***

- GPS navigation relies on measuring the distance or delay to several known transmitters to triangulate the mobile receiver's position
- The GPS-denied environment presents navigation challenges for UAVs and UAMs.
- These areas include urban canyons, forest canopy, etc.
- Strike Resonance frequency – which disrupts balance (vehicles tilt, orientation & rotation) (LRAD, 2019)

### **LRAD**

LRAD stands for Long-Range Acoustic Devices. They have been used to address protestors, knock pirates off their attacking boats, disable soldiers in the field, and knock out UAS in the air. (English, 2022) The LRAD is a device that can put out a highly directional “beam” of incredibly loud sound, up to 160 decibels (dB). (English, 2022)

To understand how loud 160dB is, it's important to understand that volume, or “sound pressure level” (SPL), is not a linear measure: an increase of 10dB corresponds to a tenfold increase in SPL. A 20dB increase would be a 100-fold increase in SPL. As a rough reference, standing directly behind a jet engine as it takes off is between 130 and 140dB, and nearby gunshot rates are approximately 150db. Anything over 140dB will cause pain for most people, but even sounds over 120dB can cause permanent hearing damage from even short periods of exposure. (English, 2022) See

[https://youtu.be/QSMY3\\_dmrM](https://youtu.be/QSMY3_dmrM) for a demonstration of LRAD G20 by police at a Pittsburgh protest. (English, 2022)

**Figure 13.6 LRAD**



Source: (LRAD , 2022)

### **NATO Autonomous Mine Sweepers (ATM)**

Research is ongoing to detect underwater mines and submarines. Underwater mines don't necessarily need to detonate on contact with a ship. Many explode when they sense the *acoustic sounds* that ships give off when passing through a waterway or by detecting the magnetic signatures of the metals used to construct ships. (NATP OTAN, 2014)

**Figure 13.7 NATO OTAM ATM**



Source: (NATP OTAN, 2014)

Figure 13.7 shows NATO's MANEX experiment. Mines are an inevitable consequence of an unstable world. The legitimate use of mines includes protecting sovereign waters from covert operations that might be illegal in international law. In times of war, supply routes may be mined to cripple an enemy's war efforts. The above method of deploying mine is crude and potentially still risky to the human operators. It has been used as a ship defense.

**Figure 13.8 LRAD Ship Defense on USS ESSEX**



Source: (USS Essex conducts a Straits Transit exercise in the Pacific Ocean by #PACOM, 2015)

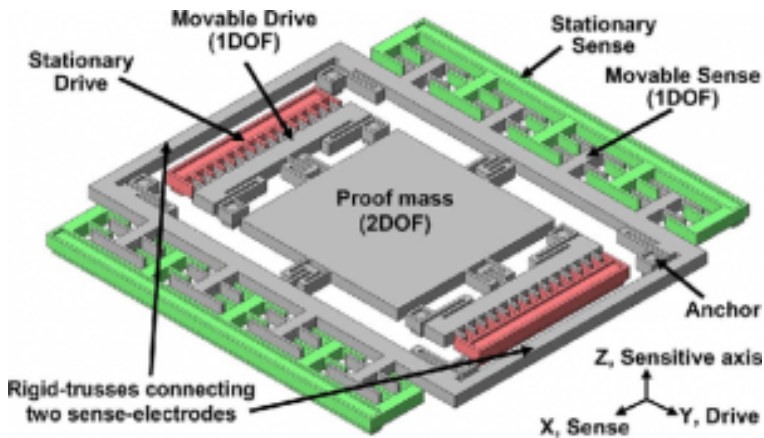
## **MEMS**

What is a MEMS, and how does it relate to the UAS gyroscope?

As shown in Figure 13.9 MEMS Gyroscope,

- MEMS (Micro-Electro-Mechanical-Systems) gyroscopes are located in the rotor systems of most drones
- Visualization of a MEMS gyroscope is a single proof mass suspended above a substrate
- The proof mass is free to oscillate in two perpendicular directions, the drive, and sense
- (Said Emre Alper, December 2008)

**Figure 13.9: MEMS Gyroscope**



Source: (Said Emre Alper, December 2008)

A very interesting presentation on MEMS is available at (Said Emre Alper, December 2008).

### **Resonance Effects on MEMS – we have arrived at the NUB of this section**

Achieving resonance frequencies can have a significant effect on countering hostile UAS:

- ***MEMS Gyroscope can be degraded using harsh acoustic noise*** (Yunmonk Son, 2015)
- *MEMS Gyroscope has a resonant frequency that is related to the physical characteristics of its structure* (Usenix.org, 2019)
- *MEMS gyroscopes have resonant frequencies much higher than can be heard (audible and ultrasonic ranges)*
- ***Unexpected resonance output caused by an attack will cause the rotor system to malfunction*** (Yunmonk Son, 2015)
- ***Rotors will spin at differing speeds causing the drone to become unstable and crash***(Yunmonk Son, 2015)

## **What is Resonance Tuning?**

- “In the operation of MEMS gyroscopes, the bending changes the capacitance between the sensing mass and the sensing electrode, and this capacitance change is sensed as the gyroscope

‘s output.

- Using an additional feedback capacitor connected to the sensing electrode, the resonant frequency and the magnitude of the resonance effect can be tuned.
- A malicious attacker can induce resonance if resonant frequencies exist in gyroscopes”(Nichols R. K., 2019)

## **What is the “so what” for Acoustics?**

Here are the author’s thoughts:

- “Passive detection is much cheaper and cost-effective to operate vs. a complex radar system for a single installation (limited by detection range ~350ft- 1000ft)
- MEMS gyroscopes contained in rotor systems are very susceptible to malfunction when struck with rough noise that resonates inside the MEMS
- Offensive acoustic systems are currently mounted, could become man-portable
- National ELINT assets do not detect offensive systems
- not looking for acoustic energy signatures; the enemy can remain hidden from detection when using acoustics.”(Nichols R. K., 2019)

## **Are there Countermeasures for Acoustic attacks on gyroscope?**

“Yes, some but not totally effective:



- Physical Isolation – provide physical Isolation from the sound noise
- Surrounding the gyroscope with foam would also be a simple and inexpensive countermeasure
- Differential Comparator
- Using an additional gyroscope with a special structure that responds only to the resonant frequency, the application systems can cancel out the resonant output from the main gyroscope.
- Detect and cancel out analog sensor input spoofing against CIEDs.”(Nichols R. K., 2019)

### **South Korean Experiment**

In the author’s judgment, a brilliant and innovative paper by Yunmonk son et al. from the Korean advanced institute of science and technology (KAIST) is the seminal paper on taking down drones using sound noise on gyroscope sensors! (Yunmonk Son, 2015)

(Yunmonk Son, 2015) describes the relationship between *Sound Pressure Level (SPL)* and Sound Amplitude and derives the attack distance, *d* as (in dB):

$$\text{SPL} = \text{SPL}_{\text{ref}} + 20 \log (A / A_{\text{ref}}) \quad \text{Equation 13.6}$$

Where SPL = sound pressure level, SPL<sub>ref</sub> is the reference, A and A<sub>ref</sub> are the amplitudes of the source and reference point. Using real-world experiments (Yunmonk Son, 2015) found that:

$$\text{SPL} = \text{SPL}_{\text{ref}} - 20 \log (d / d_{\text{ref}}) \quad \text{Equation 13.7}$$

Where *d*, *d<sub>ref</sub>* are the attack scenario distances.

KAIST under (Yunmonk Son, 2015) primary conclusions are:

- 1) “Many sensing and actuation systems trust their measurements and actuate according to them. Unfortunately, this can lead to security vulnerabilities that cause critically unintended actuation.
- 2) The sound channel can be used as a side channel for MEMS gyroscopes from a security point of view.
- 3) Fifteen kinds of MEMS gyroscopes were tested, and seven were found vulnerable to disruption using intentional noise.
- 4) The output of the vulnerable MEMS gyroscopes was found using a consumer-grade speaker to fluctuate up to dozens of times due to the sound noise.
- 5) The authors found that an attacker with only 30% of the amplitude of the maximum sound noise could achieve the same result (disruption) at the same distance.
- 6) At 140 decibels, it would be possible to affect a vulnerable drone up from around 40 meters away,
- 7) Some drone gyroscopes have resonant frequencies in both the audible and ultrasonic frequency ranges, making them vulnerable to interference from intentional sound noise.
- 8) Authors found that accelerometers integrated with MEMS gyroscopes were also affected by high-power sound noise at certain frequencies.”(Yunmonk Son, 2015)[6]

## **NOISE**

Loud and abrupt sound as a countermeasure also brings the problem of exposure and loss. Chapter 17 of (Gelfand S. A., 2009) discusses the effects of noise and hearing conservation. Chapter 20 of (Gelfand S. A., 2009) discusses occupational standards. Safety is an important topic but outside the scope of this writing.

## **UAS. Collaboration – SWARM**

Recall that the authors previously defined in Chapter 3 of (Nichols & Mumm, Unmanned Aircraft Systems in the Cyber Domain, 2nd Edition., 2019) a UAS SWARM as a uniform mass of undifferentiated

individuals w/o Chief at automation level 4 or 5. SWARMS exhibit the following advantages:

- Efficient based on numbers, emergent large group behaviors, and reactions
- Not controllable or automated, decentralized intelligence
- Think shoal of fish w/ evolving local rules; highly resistant form
- Not changing based on survivability of members, no hierarchy

SWARM Countermeasures include disruption, i.e., changing the Strategic Global View of SWARM (its only real vulnerability), complete Defender collaboration with multiple kinetic and non-kinetic countermeasures, and use of Acoustic Countermeasures for identification as friend or foe (IFF) based on a library of manufacture detection signatures and complete, abrupt rotor disablement by attacking the SWARM units with resonant, loud (100-140 dB) sound noise aimed directly at the MEMS gyroscopes or close by on the unit. [Think of glass breaking at resonance frequency or a submarine under depth charge attack. The former breaks by super-excited molecules in the glass and literally shakes apart. The latter is destroyed by the violent shaking of the submarine so that its parts break, and flooding ensues. It is unnecessary to hit the submarine directly because explosions in water, hence sound waves and explosive forces, carry very far and effectively to the target.]

**Remember the Problem the Wildcat team has addressed in every book of our series.**

Which is:

**The Risk of success of Terrorist Attacks on US Air and Naval Defense Systems (ADS/NDS) via sUAS / UAS is higher and improving because of commercial capabilities and accessibility.** Advanced small drones capable of carrying sophisticated imaging equipment, significant (potentially lethal) payloads, and performing extensive Intelligence, Surveillance, and Reconnaissance (ISR)

missions are readily available to the civilian market. **They pose a significant threat to civilian and military UAS operations and safety in the NAS and operations on the sea. Hostile UAS presents the highest threat to ADS / NDS. Swarms.**

#### **A Problem Solution Not The ONLY Problem Solution:**

**The author's research suggests that UAS. Swarms can be both identified (IFF) and destabilized/mitigated/eliminated/countered in the air by applying harsh acoustic countermeasures at resonance frequencies.**UAS (in any formation – especially Swarms) present detectable acoustic signatures that can be collected in IFF sound libraries. They are unique to the make, model, and origin manufacturers like fingerprints or DNA. Once identified as hostile, UAS (Swarm units) may be destabilized by harsh – explosive amplitude acoustic countermeasures to the MEMS or rotor base of the UAS, causing destabilization of the UAS and grounding. Emergency and waypoint recovery functions do not work under this approach.

#### **Switching to A Dangerous Theater of Operations (TO) – Chinese Drones in the Spratly Islands, and Chinese Threats to USA forces in the Pacific**

The authors now take an abrupt turn to the South China Seas (SCS) and the threatening influence of China. We are certain of cyber weapons in the SCS, especially in the neighborhood of the Spratly's. We are not certain that acoustic weapons are being used in this TO. However, if PLAN has been watching, the Russians have already employed them against US diplomats. It would be an economic benefit to use them. Also, China (PLAN) has made significant moves to take over the Solomon Islands; they are negotiating deals in Papua, New Guinea and economic assistance to Kiribati, only 1900 miles south of Hawaii. In Pacific terms, Kiribati is America's next-door neighbor. (Chang, 2022) China continues years of persistent commercial, diplomatic, and military efforts to

own the Pacific. They intend to put military bases along with the New Silk Road Strategic Plan for land and sea. Like flies to a spider, money opens the door to future treachery to both the fly and its neighbors.

China uses economic framework agreements to hook its clients and bring in PLAN forces. These framework agreements, when fully implemented, will give China the ability to sever shipping lanes and air links connecting the US with its treaty ally Australia and partner New Zealand. (Nichols & Ryan, Unmanned Vehicle Systems & Operations on Air, Sea & Land, 2020) If Chinese forces should soon move on Taiwan ala the Russian Invasion of Ukraine, they will use ISR assets and special UAS / UUV capabilities developed in the Spratlys. They will use both kinetic and non-kinetic means to accomplish their control of Taiwan. **As recently as April 2022, Taiwan has been building up its defenses against Chinese drones. They have already been spotted over Dongsha Island.** The Coast Guard Administration (CGA) says the Chinese threat will likely rise as Taiwan-US cooperation strengthens. (Strong, 2022)

**Figure 13.10 Location of Dongsha Island and Taiwan**



Source: (Dongsha Island – Taiwan, 2022)

### **Location of the Spratly Islands and Their Strategic Importance**

The Spratly Islands are a disputed group of islands, islets, cays, and more than one hundred reefs in the South China Sea. Named after British Whaling captain Richard Spratly in 1843, they represent only 490 acres spread over 164,000 square miles. The archipelago lies off the coasts of the Philippines, Malaysia, and China (Wikipedia, 2022)

### **Figure 13.11 Spratly Islands**





Source: Courtesy of (Google, 2022)

Although there are some civilian settlements in the approximate 45 islands, all contain structures occupied by military forces from Malaysia, Taiwan (ROC), China (PRC), the Philippines, and Vietnam. Brunei has claimed an exclusive economic zone around the Louisa Reef (Wikipedia, 2022). Figures 13.8 and Figure 13.9 show the Spratly Islands. Officially they are in the South China Sea at 10 degrees N, 114 degrees E.

### **Target Drones**

The Spratlys may be disputed in theory, but the undeniable winner in any real in this TO would be China. China has made huge investments in defensive infrastructure, military, unmanned aircraft, and boats to solidify its position in the Spratlys. China has one of the largest UAS intelligence operations in the Spratlys and



regularly conducts drills. These drills simulate fending off an aerial attack. The drills, which involve three target drones making flyovers of a ship formation at varying heights and directions, are part of the ongoing efforts to improve its real-life combat ability. The drones have been sent out several hundred times during more than thirty drills. (Chinese navy deploys drones in South China Seas missile drills. Diplomacy and Defense article, 2018)

China announced in July 2021 that it conducted secret naval drills in the Taiwan Strait even as the self-governing island reasserts its sovereignty and wants to safeguard its free and democratic system. (Ghosh, 2021) According to South China Morning Post, Beijing has recently declassified a report on the development of *drone submarines*, a project it had started in 2010. While many countries are developing or have already developed unmanned underwater vehicles (UUVs), the timing of China's announcement is interesting. China has developed underwater drones capable of identifying, tracking, and attacking an enemy submarine without human interference. Sound plays a big part in the location of the target. (Ghosh, 2021)

### **Shark Swarm and Wanshan Marine Test Field**

China has tested an army of tiny drone ships that can “shark swarm” enemies during sea battles. It has a fleet of fifty-six unmanned craft sent out on maneuvers off the Wanshan Archipelago in the South China Sea. The Chinese firm Oceanalpha confirmed that the drones were designed to overwhelm enemies in sea battles. A mothership controls the armed swarm.<sup>[7]</sup> Oceanalpha confirmed that the Wanshan Marine Test Field was constructed sole purpose of conducting drone craft drills (Barnes, 2018)

### **Fast Drone Ship**

In December of 2017, HiSIBI, a Chinese nautical firm, announced the development of the world's fastest drone ship, which can travel at 50 knots (58 mph).<sup>[8]</sup> The new speed drone is being tested in the

Wanshan Marine Test field. The test field is still under construction and is believed to be the world's largest test field, covering over 297.9 square miles. Military observers have indicated that the test site for unmanned vessels is part of China's overall plans to develop autonomous systems for civilian and military applications. The new test site dovetails with China's push to use technology to safeguard China's maritime interests. (China starts work on world's biggest test site for drone ships near the South China Sea, 2018)

### **Long-Range UUV**

Tianjin University researchers completed a sea test of the Haiyan autonomous Unmanned Underwater Vehicle (UUV). It can endure for 30 days and has a 621.37miles range (Lin, 2014). Just as the US Navy is conducting UUV research for facing off against China's growing Anti-Access Area Denial capabilities, the Chinese are building up these capabilities. UUVs cover a larger area, can operate more efficiently, and use multiple sensors to monitor water temperature, conductivity, optical backscatter, and acoustics. Multiple sensor types increase the probability of finding the prey in the battle mode for detecting a stealthy submarine. Unlike fixed underwater sonar stations, UUVs can be rapidly deployed via ships or airdrops to newly uncovered areas (such as Taiwan Straits or the South China Sea), where mobility complicates enemy efforts to disrupt and destroy them. (Lin, 2014)

The Haiyan UUV is part of the deployed assets for an Underwater Great Wall, a network of sensors on the seabed, coupled with long endurance UUVs to identify and destroy enemy submarines and mines. The sister fish-like Qianlong autonomous underwater vehicle (AUV) can dive to 14,800 feet, indicating Chinese interests in deep-sea robotic ships. These UUVs can also attack targets anywhere in the Indian Ocean and collect enemy submarine acoustics and oceanographic conditions for improving stealth and anti-stealth measures. (Katoch, 2018)

### **Crisis Watch**

The US and China are in a power struggle in the South China Sea centered around the US countering Chinese military operations in the Spratlys. Prior Defense Secretary General Mattis addressed some of the disputed issues at the Shangri-La Dialogue Asia security summit in Singapore on June 2, 2018:

US Sec Defense Mattis outlined the US “Free and Open Indo-Pacific Strategy,” consisting of expanded maritime security support for US partners, helping regional navies become more interoperable with the US Navy, strengthening governance through defense engagements and private sector-led development. Mattis said the US wants to work with regional multilateral institutions, particularly ASEAN; new US national security and defense strategies emphasize Indo-Pacific; said cooperation with China is “welcome wherever possible.” Mattis criticized China’s militarization of features in the disputed Spratly archipelago. Also, addressing Shangri-La Dialogue, China, for the first time, publicly acknowledged that it was basing weapons and military personnel on disputed features it controls in Paracel and Spratly Islands, which it said are Chinese territory. Chinese military representative said Mattis’s comments were “irresponsible” and that the US was the one militarizing, citing US air and naval passages within twelve nautical miles of Chinese-controlled territory. US June 5 flew two B-52 bombers over disputed Scarborough Shoal near the Philippines; China sent ships and aircraft and said the US was “stirring up trouble.” Reuters June 3 reported that the US is considering stepping up its naval operations near disputed features. The US held an annual Malabar naval exercise with India and Japan from 7-16 June off the coast of Guam and in the Philippine Sea. Biennial U.S. Rim of the Pacific (RIMPAC) naval exercises began June 27 without China after US late May rescinded China’s invitation to participate. On June 8, ImageSat International reported that China had redeployed surface-to-air missile systems to Woody (Yongxing) Island in Paracels. PLA navy, on June 15, carried out missile drills in the South China Sea (SCS). The UK and French defense ministers on June 3 said they would send more naval ships through SCS to assert the right to freedom

of navigation. Meeting with Sec Defense Mattis in Beijing on June 27, President Xi Jinping reasserted that China would not give up any of its territorial claims in SCS; also called for deepening military-to-military ties. (Crisis Watch, 2018)

The Pentagon claims evidence that the Chinese have deployed anti-ship missiles, surface-to-air missiles (SAM) systems, and electronic jammers to the Spratly Islands. The Chinese have landed bomber aircraft at Woody Island. (Huang, 2018) This is along with the new drone systems and intelligence UAS assets discussed supra.

### **Red Drones over Disputed Seas**

One of the best reports on how the Chinese military uses unmanned drones for power projection and surveillance in the contested South and East China Seas was written by (McCaslin, 2017). China is currently undergoing a “drone” driven by heavy investment in the Chinese drone industry and by illegal acquisition of foreign drone technology (Katoch, 2018).

US DOD predicts China will produce tens of thousands of drones by 2023 (DoD Report, 2015). Drone sightings and proper identification are important because of the lack of international rules governing the treatment of drones, including in areas where sovereignty is contested (Lehman, 2017).

The report documents four drones known to be used by PLAN: The S-100, ASN-209, BZK-005, and the GJ-1. All but the S-100 are Chinese-produced. Scheibel makes the S-100 in Austria. The drones discussed fill a variety of roles, from surveillance (S-100) to military/weaponized (GJ-1, aka Wing Loong I model) (Lehman, 2017)

One limiting factor facing Chinese power projection is the inability of their current inventory to runway launch from aboard the Chinese Navy's sole aircraft carrier. This limits the BZK-005 (primary mission surveillance) from being launched from land (McCaslin, 2017). The S-100 uses vertical take-off and landing

(VTOL) system and does not have this problem. Additionally, drones can be launched from Chinese-controlled artificial islands in contested areas [i.e., the Spratly Group.] (Lehman, 2017)

***The author contends that the BKZ-005 is suspected of being outfitted with cyber and sonic weapons to harass the US Naval forces in the Spratly AO, causing chaos with the commercial and potentially US navy GPS systems.***

**Figure 13.13 S-100 Chinese Drone**



Source: (Wikipedia, 2018)

The S-100 has an 18,000-foot ceiling, weighs 75 pounds armed with Thales Lightweight Multi-role Missiles (LMM), with a range of 60 to 125 miles, and can be operational for 10 hours. They are

generally launched from a PLAN Type 054 /054A frigate. (McCaslin, 2017)

China uses the S-100 for intelligence, surveillance, and reconnaissance (ISR). They are equipped with Synthetic Aperture Radar (SAR), Maritime Radar, Signal Intelligence (SIGINT), and Communications Intelligence (COMINT) payloads. See Figures 13.14 for S-100 views and ranges.

**Figure 13.14 S-100 Drone Trajectories in the Spratly Islands**



Source: (McCaslin, 2017)

**Figure 13.15 BZK -005 Chinese Drone**



Source: (Wikipedia BZK-005, 2018) Chinese UAS

### **BZK -005**

The BZK-005 is also a MAME drone for specialized surveillance missions. It has an operational ceiling of 26,247 feet, with a maximum range of 1491 miles and an endurance of 40 hours. The range is limited by ground-based runways, i.e., the Spratly Islands group. (McCaslin, 2017)

It is equipped with electro-optical, infrared, SAR, SIGINT, and satellite communications systems, allowing real-time data transmission capability. See Figure 13.15 for the BZK-005 view.

The BZK-005 range permits surveillance over the entire South China Seas if launched from Chinese – controlled islands (artificial and natural): Woody Island, Subi Reef, Mischief Reef, and Fiery Cross Reef. (McCaslin, 2017)

**Figure 13.16 Chinese UAS. Chinese Intelligence Assets  
Deployment in Spratlys**



Source: (Nichols & Carter, RSCAD Presentation of Research to KSUP Faculty on SCS Drone Activity, (4 May 2018))

Professor Nichols and Carter have been tracking Chinese intelligence assets, UAS, UUV, underwater bases, cyber, spoofing, and sonic incidents involving American capital ships and submarines in the South China Seas (SCS) since 2017. They have compiled quite a storehouse of information and made multiple research presentations on the subject. Their present concern is the threat to Taiwan. The team uses DRONESEC tracking and a professional version of <http://www.globalincidentmap.com/> to support its work.

#### **DRONESEC Report April 2022**

We asked DRONESEC out of Singapore to use their tracking programs to update malicious and suspicious cyber or acoustic incidents involving UASs or UUVs or malicious incursions in SCS and near Taiwan. Arison Neo, the lead threat analyst, reported: "I



believe there are manned ships and aircraft incursions happening more rampantly in the SCS, but the Notify platform only tracks and collates drone incidents., I added some that were of the UUV category. Here are the results.” (Neo, Suspicious Drone Incidents in SCS Involving Cyber or Acoustic , 2022) See Figure 13.17.

**Figure 13.17 Malicious Drone Activities in SCS near Taiwan**

| Date      | Title  | Drone Classification                        | Reference   |
|-----------|--|---|---|
| 10-Sep-18 | China is deploying drones to spy on the South China Sea like never before                  | Not Stated                                  | <a href="https://www.burieninquirer.com/news-in-china/china-drones-to-spy-on-south-china-sea-23132/">https://www.burieninquirer.com/news-in-china/china-drones-to-spy-on-south-china-sea-23132/</a>   |
| 09-Aug-20 | South China Sea CH-9000: Beijing's drone proliferation ignites tensions in disputed region | Not Stated                                  | <a href="https://www.uscni.com/story/news/05/22/2020/south-china-sea-tensions-technology-052220-uscni">https://www.uscni.com/story/news/05/22/2020/south-china-sea-tensions-technology-052220-uscni</a>   |
| 30-Dec-20 | Three Chinese underwater drones found near Indonesia's Selayar Island                      | Heavy UUV                                   | <a href="https://www.usni.com/story/news/02/02/2021/chinese-submarine-drones-found-near-selayar-island-usni">https://www.usni.com/story/news/02/02/2021/chinese-submarine-drones-found-near-selayar-island-usni</a>   |
| 01-Apr-23 | Chinese drones spotted recently over Taiwan's Dongsha Islands                              | Not Stated                                  | <a href="https://www.islandnews.com.tw/news/1186180">https://www.islandnews.com.tw/news/1186180</a>   |
| 03-Apr-23 | Chinese drones spotted flying over Taiwan occupied Pratao Island in South China Sea        | Not Stated                                  | <a href="https://www.rfa.org/section/asia/asia-news/chinese-drones-04032023-021820.html">https://www.rfa.org/section/asia/asia-news/chinese-drones-04032023-021820.html</a>   |
| 16-Apr-23 | Chinese submarines claim to capture untested ship with surveillance equipment off Yokohama | Wave Glider                                 | <a href="https://www.usni.com/story/news/04/16/2023/chinese-submarine-ship-drones-capture-untested-foreign-robotic">https://www.usni.com/story/news/04/16/2023/chinese-submarine-ship-drones-capture-untested-foreign-robotic</a>                               |
| 08-Aug-21 | Japanese Fighters Intercept Three Chinese Drones in Ae Many Days                           | Angoon YB-001<br>Goception<br>Hudon RQV-005 | <a href="https://www.defence.com/asia-pacific/2154japan-says-fighters-intercept-three-chinese-drones-in-ae-many-days">https://www.defence.com/asia-pacific/2154japan-says-fighters-intercept-three-chinese-drones-in-ae-many-days</a>                           |
| 29-Sep-21 | Chinese tests new floats say UUV in South China Sea  | WWFJ UUV                                    | <a href="http://www.reuters.com/article/us/china-defense/analysis-china-tests-new-floats-say-uuv-in-south-china-sea-idUSKCN182001">http://www.reuters.com/article/us/china-defense/analysis-china-tests-new-floats-say-uuv-in-south-china-sea-idUSKCN182001</a> |

Source: (Neo, Aerial and UUV suspicious drone incidents in the SCS, 2019-2022)

Our last topic is the malicious acoustics affecting the brain. Our S.M.E., Robert McCreight, gives us a lesson on Havana Syndrome.

**Acoustic Dynamics: Havana Syndrome and Neurological Vulnerability** (McCreight, Acoustic Dynamics: Havana Syndrome and Neurological Vulnerability, 2022)

In 2022, we must reckon with a strategic threat that is invisible,

insidious and defies facile detection. It operates covertly and often inflicts permanent cognitive degradation effects on anyone unlucky enough to dwell within the scope and scale of its non-kinetic yet ethereal and disruptive beam. *Blending nano-pulsed RF signals and various acoustic wave technologies that have a measurably negative impact on the human brain can cause epigenetic neuro-modulation, including cognitive harm.* It is a distinct domain of warfare rooted in our neurological vulnerabilities. In popular parlance, its victims suffer from something we refer to as **Havana Syndrome**. While a degree of mystery surrounds its core elements, its origins, sponsors, or offending technologies verify the sheer authenticity of its harmful effects and damage to many hundreds of victims. It is a defiant witness to an existing and enduring threat we cannot afford to ignore. Operating now for more than six years, we still lack an effective solution.

Havana Syndrome symbolizes a unique form of hostility based partially on acoustic technologies that enter our brain through our vestibular and cochlear systems. Havana Syndrome should be viewed as an opening salvo in the long-term threat we understand dimly as ‘cognitive warfare.’ Cognitive warfare exists within the human/warfighter context. Arguably it is the sixth arguable dimension of future conflict and must be understood as such. Apart from land, sea, air, space, and cyber is a brain-based battlefield nested in human systems, which is well recognized but only dimly appreciated. In cognitive warfare, the human mind is the target. Cognitive warfare aims to change what people think, what they perceive, what they remember, and how they think or act—indeed, it externally manipulates brain functions and corrupts the Central Nervous System [CNS]. While its victims thus far have been overwhelmingly American, there were also Canadian victims, and the threat this poses to America’s allies cannot be dismissed. Operating silently amongst us and engaging selected targets within the alliance, cognitive warfare—just as AI and cyber threats are seen—becomes a doorstep towards redefining what a true ‘act of

war' really is. As recently noted in the NATO Review, "*Waged successfully,[cognitive warfare] shapes and influences individual and group beliefs and behaviors to favor an aggressor's tactical or strategic objectives. In its extreme form, it has the potential to fracture and fragment an entire society so that it no longer has the collective will to resist an adversary's intentions. An opponent could conceivably subdue a society without outright force or coercion.*" (Kathy Cao, 2021)

Remembering Sun Tzu's dictum that the pinnacle of skill is to "subdue the enemy without firing a shot,"...we find cognitive warfare amply demonstrates the power of that observation. Fostering social upheaval and chaos through cognitive warfare effectively reflects the confidence, confusion, and controversy that the public invests in media outlets and social media. Sordid experiences involving propaganda, disinformation, and psychological warfare exerted degrees of measurable societal disruption, planting public unrest among restive groups and classes, undermining the legitimacy of government, subverting lawful authority via staged civil disturbances, or enflaming separatist movements. (McCreight, Cognitive Warfare 2021: Latent AllianceThreats in Neurostrike and Havana Syndrome, 2021)

### **Acoustics and Havana Syndrome Illustrate our Collective Neurological Vulnerability**

When CIA Director William Burns traveled to India in September 2021; a team member reported symptoms consistent with Havana Syndrome and received medical attention. A month earlier, Vice President Kamala Harris temporarily delayed her arrival in Vietnam after the State Department made her office aware of a "possible anomalous health incident" in the US Embassy in Hanoi. The description of the incidents there as "acoustic" indicates that the affected diplomats heard strange sounds. Then in July 2021, the State Department and the Austrian government said they were investigating possible cases in Vienna that had emerged in previous

months. In addition, other cases involved two senior national security officials adversely affected during the Trump administration. They included Olivia Troye and Miles Taylor, who CBSNEWS that they too had experienced symptoms consistent with Havana Syndrome. (Pelley, 2022) Ms. Troye served as homeland security and counterterrorism adviser to Vice President Mike Pence. Then in February 2022, Mr. Burns, Director of the CIA, found that some incidents of Havana Syndrome are most likely caused by directed energy or acoustic devices and can't be explained by other factors. (Strobel, 2022)

Experts studying the suspected technologies behind Havana Syndrome have concluded that “pulsed electromagnetic energy, particularly in the radiofrequency range, plausibly explains the core characteristics.” However, they concede that such a theory is riddled with “information gaps.” Such nefarious devices exist with capabilities that could generate the required wave beam stimulus. Some said acoustic signals, easily concealable and requiring moderate power requirements, might be responsible. For example, some experts claim that “using nonstandard antennas and techniques, the signals could be propagated with low loss through the air for tens to hundreds of meters, and with some loss, through most building materials.” With the possible exception of ultrasound devices, the report rules out the plausibility of all other proposed causes. The authors point out that their report does not provide evidence for using any such device, nor does it address the issue of who may be behind any hypothetical attack. (DNI, 2022)

The State Department originally said that in 2019 the adversely affected Embassy Havana employees developed what became known as “**Havana Syndrome**” – headaches, dizziness, nausea, and other symptoms that arose when they heard penetrating high-pitched sounds. According to a study by the University of Pennsylvania, MRI scans from 23 men, and 17 women showed changes in brain structure and functional connectivity between

different organ parts compared with 48 other adults. *The difference in the brains between the two groups “is pretty jaw-dropping at the moment,”* lead researcher Dr. Ragini Verma, a professor of radiology at Penn, [told Reuters](#). “Most of these patients had a particular type of symptoms, and a clinical abnormality is reflected in an imaging anomaly” (McCreight, Cognitive Warfare 2021: Latent Alliance Threats in Neurostrike and Havana Syndrome, n.d.)

NIH FBI saw victims of Havana Syndrome. The University of Miami and University of Pennsylvania medical and neuroscience experts. Then in December 2020, a report issued by the National Academy of Sciences [NAS] said the victims were exhibiting “... *a constellation of acute clinical signs and symptoms with directional and location-specific features that were distinctive....unlike any disorder in the neurological or general medical literature*”. (NAP, 2022)

Independently, numerous medical studies and research reports affirm the central NAS theory behind what the Academy and its experts say triggered Havana Syndrome. One such example illustrates the core issue.

“Pulsed microwaves may injure brain tissue by transduction of microwave energy into damaging acoustic phonons in brain water. We have shown that low-intensity explosive blast waves likely initiate phonon excitations in brain tissues. Brain injury, in this instance, occurs at nanoscale subcellular levels as predicted by physical consideration of phonon interactions in brain water content. The phonon mechanism may also explain similarities between primary non-impact blast-induced mild Traumatic Brain Injury (mTBI) and recent clinical and imaging findings of unexplained brain injuries observed in US embassy personnel, possibly due to directed radiofrequency radiation. Certain RF frequencies and power levels can trigger pulsed microwaves and potentially injure brain tissue. Microwaves can also be focused into narrow field-of-view beams to target individuals. Experimental evidence indicates that pulsed microwaves can disrupt brain tissue

producing subsequent behavioral and cognitive dysfunction. In addition, pulsed microwaves reportedly may alter blood-brain barrier permeability, disrupt long-term potentiation, and result in DNA strand breaks” (Graham K. Hubler<sup>1</sup>, 2020)

In 2021 numerous press reports were identified of parallel Havana Syndrome complaints from US diplomats posted to Berlin, Hanoi, Borgata, Managua, Vienna, and Guangzhou and at least 19 other posts overseas. This provides additional impetus to find the offending technology and determine how best to protect vulnerable employees. With a net cluster of potential victims among US military, intelligence, and diplomatic ranks, which may exceed 800 in number and rising, serious guardians of America’s security should pay attention to these disturbing developments. (McCreight, *Cognitive Warfare 2021: Latent Alliance Threats in Neurostrike and Havana Syndrome*, n.d.)

### **Acoustic Technologies**

We know that acoustic technologies can be used to suppress civil disturbances. We offset military threats using a non-kinetic but effective to a width of 120-degree beam out for more than 500 meters. Compared to ultrasonic high-frequency systems, these low-frequency systems have demonstrated their effectiveness in deterring certain categories of maritime threats. This should be seen as universally available to American allies and foes as acoustic systems provide an additional technological tool to enhance the combat power of the United States military. This would include terrestrial, airborne, and underwater acoustic spectrum systems. Rooted in directed energy [DE], we find laser, microwave, and acoustic aspects. Systems such as LRAD illustrate the power and influence of <1000 MGh in delivering piercing sound effects and disruption, which inflicts nausea, headaches, and severe imbalance issues. More must be studied and understood about the net strategic implications of various acoustic technologies devised and developed for possible military use because of their unique non-

kinetic properties and the implied battlefield effects of their targeted use as a prelude to, or augmentation of, combat operations. (NCBI, 2005).

## SCREAMERS

We see the future of acoustic weapons in the 1995 film **Screamers**, a science fiction horror film starring Peter Weller. In the year 2078, the planet Sirius 6B, once a thriving mining hub, has been reduced to a toxic wasteland by a war between the mining company, known as the New Economic Block (NEB), and “The Alliance,” a group of former mining and science personnel. After miners discovered that their ore extraction released toxic gases, they went on strike, and the mining company hired mercenaries as strikebreakers. Five years into the war, Alliance scientists **created and deployed Autonomous Mobile Swords (AMS)** — artificially intelligent self-replicating machines that hunt down and kill NEB soldiers on their own. They are nicknamed “screamers” *because of the high-pitched noise they emit as they attack*. Screamers track targets by their heartbeats, so Alliance soldiers wear “tabs” which broadcast a signal canceling out the wearer’s heartbeat and rendering them “invisible” to the machines.

**There is nothing to prevent LRAD technology combined with AI from being reduced to cylinder form – payload and deployed by UAS as a SCREAMER against any target of opportunity.** (Wikipedia, 2022) [\[9\]](#)

**Figure 13.18 AMS – SCREAMER**



Source: (autonomous-mobile-sword-miniature-screamers, 2022)

### **Bibliography**

Adamy, D. -O. (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.

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

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

*autonomous-mobile-sword-miniature-screamers*. (2022, April 2). Retrieved from [www.liveauctioneers.com/](https://www.liveauctioneers.com/): [https://www.liveauctioneers.com/item/6321634\\_940-autonomous-mobile-sword-miniature-screamers](https://www.liveauctioneers.com/item/6321634_940-autonomous-mobile-sword-miniature-screamers)

Barnes, T. (2018, June 7). *China Tests an army of tiny drone ships that can 'shark swarm' enemies during sea battles*. Retrieved from



[www.independent.co.uk/](https://www.independent.co.uk/news/world/asia/china-drone-ships-unmanned-test-video-military-south-sea-sha): <https://www.independent.co.uk/news/world/asia/china-drone-ships-unmanned-test-video-military-south-sea-sha>

Chang, G. G. (2022, March 31). *China Takes over the Solomon Islands – and the Pacific*. Retrieved from [www.gatestoneinstitute.org/](https://www.gatestoneinstitute.org/): <https://www.gatestoneinstitute.org/18384/china-takes-over-solomon-islands>

*China has started work on world's biggest test site for drone ships near the South China Sea*. (2018, July 6). Retrieved from [www.todayonline.com](https://www.todayonline.com/): <https://www.todayonline.com/world/china-starts-work-worlds-biggest-test-site-drone-ships-gateway-south-china-sea>.

*Chinese navy deploys drones in South China Seas missile drills. Diplomacy and Defense article*. (2018, June 6). Retrieved from [www.scmp.com/](https://www.scmp.com/): <https://www.scmp.com/news/china/diplomacy-defence/article/2150957/chinese-navy-deploys-drones-south-china-sea-missile/>

Corr, a. (2018). *Great Powers, Grand Strategies: The New Game in the South China Sea*. Naval Institute Press Annapolis.

*Crisis Watch*. (2018, June). Retrieved from [Retrieved from map overlay, https://www.crisisgroup.org/crisiswatch](https://www.crisisgroup.org/crisiswatch): <https://www.crisisgroup.org/crisiswatch>

DNI. (2022, Feb 2). *statement-from-dni-haines-and-dcia-burns*. Retrieved from [www.dni.gov/](https://www.dni.gov/): <https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2022/item/2274-statement-from-dni-haines-and-dcia-burns>

*Dongsha Island – Taiwan*. (2022, April 1). Retrieved from <https://i2.wp.com/taiwanenglishnews.com/wp-content/uploads/2020/06/Dongsha.jpg?resize=752%2C445&ssl=1>: <https://i2.wp.com/taiwanenglishnews.com/wp-content/uploads/2020/06/Dongsha.jpg?resize=752%2C445&ssl=1>

English, L. (2022, February 20). *whats-an-lrad-explaining-the-sonic-weapons-police-use-for-crowd-control-and-communication*. Retrieved from [theconversation.com/](https://theconversation.com/):

<https://theconversation.com/whats-an-lrad-explaining-the-sonic-weapons-police-use-for-crowd-control-and-communication-177442>

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/>

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.

Ghosh, A. (2021, July 8). *China's Most Ambitious, Highly Secretive Military Program To Dominate The South China Sea Declassified*. Retrieved from *eurasianimes.com/*: <https://eurasianimes.com/chinas-most-ambitious-highly-secretive-military-program-to-dominate-the-south-china-sea-declassified/>

Google. (2022, April 1). *spratly-islands map*. Retrieved from *www.spratlys.org/*: [http://www.spratlys.org/maps/1/spratly-islands\\_95.jpg](http://www.spratlys.org/maps/1/spratly-islands_95.jpg)

Graham K. Hubler<sup>1</sup>, S. W. (2020, Aug 4). *Pulsed Microwave Energy Transduction of Acoustic Phonon Related Brain Injury* . Retrieved from <https://doi.org>: <https://doi.org/10.3389/fneur.2020.00753>

Huang, P. (2018, May 23). *US Disinvites China from International Naval Exercise in Response to South China Sea Aggression* . Retrieved from [www.theepochtimes.com/](http://www.theepochtimes.com/): <https://www.theepochtimes.com/us-disinvites-china-from-international-naval-exercise-in-response-to-so>

Kathy Cao, S. G. (2021, May). *Countering Cognitive Warfare—Awareness & Resilience* . *NATO Review*.

Katoch, P. G. (2018, July 4). *New Chinese Drones – formidable challenge*. Retrieved from *spsmai.com/*: <https://spsmai.com/experts-speak/?id=556&q=new-chinese-drones-formidable-challenge>

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

<https://www.computerworld.com.au/article/581231/sounds-can-knock-drones-sky/>

Lehman, C. (2017, august 29). *Report: China Increasing Drone Operations in Disputed Seas* . Retrieved from [freebeacon.com/](http://freebeacon.com/): <http://freebeacon.com/author/charles-lehman>

Lin, J. &. (2014, June 4). *Not a Shark, But a Robot: Chinese University Tests Long-Range Unmanned Sub.* Retrieved from [www.popsci.com/](http://www.popsci.com/): <https://www.popsci.com/blog-network/easter-arsenal/not-shark-robot-chinese-university-tests-long-range-unmanne>

LRAD . (2022, April 2). Retrieved from [i.stack.imgur.com/](https://i.stack.imgur.com/): <https://i.stack.imgur.com/EO1Kg.png>

LRAD. (2019, May 189). *LRAD 450XL Datasheet*. Retrieved from LRADX: [http://www.lradx.com/wp-context/uploads/2015/05/LRAD\\_datasheet\\_450XL.pdf](http://www.lradx.com/wp-context/uploads/2015/05/LRAD_datasheet_450XL.pdf)

McCaslin, I. (2017). *Red Drones over Disputed Seas: A Field Guide to Chinese UAVs/ UCAVs Operating in the Disputed East and South China Seas.* Retrieved from [project2049.net/](http://project2049.net/): [http://project2049.net/documents/Red%20Drones%20over%20disputed%20seas\\_PLA](http://project2049.net/documents/Red%20Drones%20over%20disputed%20seas_PLA)

McCreight, R. (2021, November). *Cognitive Warfare 2021: Latent Alliance Threats in Neurostrike and Havana Syndrome* . Retrieved from [www.vernetztesicherheit.de](http://www.vernetztesicherheit.de): [www.vernetztesicherheit.de](http://www.vernetztesicherheit.de).

McCreight, R. (2022, April 1). *Acoustic Dynamics: Havana Syndrome and Neurological Vulnerability*. Carlisle, PA, USA.

McCreight, R. (n.d.). *Cognitive Warfare 2021: Latent Alliance Threats in Neurostrike and Havana Syndrome*. Retrieved from [vernetztesicherheit.de](http://www.vernetztesicherheit.de): <https://vernetztesicherheit.de/cognitive-warfare-2021-latent-alliance-threats-in-neurostrike-and-havana-syndrome/>

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

NAP. (2022). *An Assessment of Illness in U.S. Government Employees and Their Families at Overseas Embassies*. Retrieved from

<https://nap.nationalacademies.org/read/25889/chapter/1>:  
<https://nap.nationalacademies.org/read/25889/chapter/1>  
 NATP OTAN. (2014, October).  
*naval\_mines\_mine\_countermeasures\_hunting\_sweeping\_destroyer\_neutralization\_counter\_measures*. Retrieved from  
[www.bluebird-electric.net/](http://www.bluebird-electric.net/): [https://www.bluebird-electric.net/submarines/](https://www.bluebird-electric.net/submarines/naval_mines_mine_countermeasures_hunting_sweeping_destroyer_neutralization_counter_measures.htm)  
[naval\\_mines\\_mine\\_countermeasures\\_hunting\\_sweeping\\_destroyer\\_neutralization\\_counter\\_measures.htm](https://www.bluebird-electric.net/submarines/naval_mines_mine_countermeasures_hunting_sweeping_destroyer_neutralization_counter_measures.htm)  
 NCBI. (2005, Sept 29). *Long-Term Effects of Acoustic Trauma on Electrically Evoked Emissions*. Retrieved from  
[www.ncbi.nlm.nih.gov/](http://www.ncbi.nlm.nih.gov/): <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2504617>  
 Neo, A. (2019-2022). *Aerial and UUV suspicious drone incidents in the SCS*. SCS: DRONESEC.  
 Neo, A. (2022). *Suspicious Drone Incidents in SCS involving Cyber or Acoustic*. Singapore: DRONESEC.  
 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., & Carter, C. M. ((4 May 2018)). *RSCAD Presentation of Research to KSUP Faculty on SCS Drone Activity*. Salina: KSU Aerospace & Technology.  
 Nichols, R. K., & Mumm, H. C. (2019). *Unmanned Aircraft Systems in the Cyber Domain*, 2nd Edition. Manhattan, KS: [www.newprairiepress.org/ebooks/27](http://www.newprairiepress.org/ebooks/27).  
 Nichols, R., & al., e. (2020). *Counter Unmanned Aircraft Systems Technologies and Operations*. Manhattan, KS: new prairie press #31.  
 Nichols, R., & Ryan, J. M. (2020). *Unmanned Vehicle Systems & Operations on Air, Sea & Land*. Manhattan, KS: New Prairie Press #35.  
 Pelley, S. (2022, February 20). *Havana Syndrome: High-level national security officials stricken with unexplained illness on White House grounds*. Retrieved from [www.cbsnews.com](http://www.cbsnews.com):

<https://www.cbsnews.com/news/havana-syndrome-white-house-cabinet-60-minutes-2022-02-20/>

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

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.

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

Strobel, W. P. (2022, Feb 2). *some-havana-syndrome-cases-likely-caused-by-electromagnetic-waves-panel-finds*. Retrieved from www.wsj.com: [https://www.wsj.com/articles/some-havana-syndrome-cases-likely-caused-by-electromagnetic-waves-panel-finds-11643833721?mod=article\\_inline](https://www.wsj.com/articles/some-havana-syndrome-cases-likely-caused-by-electromagnetic-waves-panel-finds-11643833721?mod=article_inline)

Strong, M. (2022, April 1). *Taiwan to build up defenses after Chinese drones were spotted over Dongsha Island*. Retrieved from www.taiwannews.com.tw: <https://www.taiwannews.com.tw/en/news/4166166>

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

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

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

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

USS Essex conducts a Straits Transit exercise in the Pacific Ocean by #PACOM. (2015, April 17). Retrieved from <https://www.alamy.com/stock-photo-uss-essex-conducts-a->

straits-transit-exercise-in-the-pacific-ocean-174046140.html?irclickid=U3BRbxTTAxyITAkW-l0pixlsUkGQ7MSQNUhbyQ0&irgwc=1&utm\_source=77643&utm\_campaign=Sho p%20Royalty%20Free%20at%20Alamy&utm\_medium=impac

Wikipedia. (2018, August 8). *Chinese Schiebel S-100*. Retrieved from en.wikipedia.org/: [https://en.wikipedia.org/wiki/Schiebel\\_Camcopter\\_S-100](https://en.wikipedia.org/wiki/Schiebel_Camcopter_S-100), Retrieved 08082018.

Wikipedia. (2022, April 2). *Screamers*. Retrieved from en.wikipedia.org: [https://en.wikipedia.org/wiki/Screamers\\_%281995\\_film%29](https://en.wikipedia.org/wiki/Screamers_%281995_film%29)

Wikipedia. (2022, April 1). *Spratly Islands*. Retrieved from en.wikipedia.org: [https://en.wikipedia.org/wiki/Spratly\\_Islands](https://en.wikipedia.org/wiki/Spratly_Islands)

Wing, C. (1998). *One Minute Guide to the Nautical Rules of the Road*. Camden, ME: McGraw-Hill.

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>

## Endnotes

[1] Strictly authors speculation. Not supported by US official reports. Not the opinions of KSU or NPP press or co-authors. (See Discussion Question 3 in Chapter 3 Understanding Hostile Use and Cyber-Vulnerabilities of UAS: Components, Autonomy v Automation, Sensors, SAA, SCADA, and Cyber Attack Taxonomy

[2] 3 dB is an interesting cutoff datum. Because decibels are logarithmic, the log (base 10) of 3 = 0.477  $\approx$  50% power. So, a 3-decibel cutoff is where the power drops by approximately half. 3 dB implies  $\frac{1}{2}$  of the power. An increase of 3dB doubles the sound intensity, but a 10-dB increase is required before the sound is perceived to be twice as loud. A small increase in decibels represents a large increase in intensity. For example, 10 dB is 10x

more intense than 1 dB, while 20 dB is 100x more intense than 1 dB. (Adamy D. , 2001)

[3] It is left to the reader to obtain any standard trigonometry text to see all the parameters of the well-known sine wave.

[4] There are other ways to down the drone or catch it in a net. Our focus here is just the use of sound.

[5] It also has been used by the US Navy as an anti-piracy countermeasure. It has been tested from a boat offshore to disrupt soldiers within range to devastating effect.

[6] Although not specified in (Yunmonk Son, 2015), according to the chapter author's research and experimentation, the frequencies turn out to be the resonance frequencies. So agrees Dr. Kim at KAIST. "You would think that the gyroscopes used in unmanned aircraft systems (UAS) would have been designed to have resonant frequencies above the audible spectrum – i.e., above 20 kHz – but Kim and his team found that some have not." (Yunmonk Son, 2015) In the case of a gyroscope, "you can get it to spit out very strange outputs, as researcher Yongdae Kim, a professor in the electrical engineering department of the Korea Advanced Institute of Science and Technology (KAIST), told ComputerWorld" (Kirk, 2015) An example of resonance frequency and breaking glass can be found on youtube.be at <https://youtu.be/BE827gwnnk4>

[7] This is more of a TEAM formation as discussed in chapter 3. Swarms do not have a team leader or Mother ship.

[8] The author is Captain of /owns a recreational yacht, 36-foot CRYPTOWIZ, that can do supposedly 32-35 knots at peak performance top speed on dual Volvo-Penta GXI 315 Hp inboard engines. Cruising above 23 knots is nuts for control – especially in near Small Craft Warning winds, (unless you have a death wish and/or are married to a wife and children onboard). Just imagine being in the rough South China Seas (all the time)

[9] SCREAMERS are a natural weapons payload. It would be much cheaper than lasers or explosives. It only knows close-up (hand-to-hand, or sphere-to-sphere, so to speak) combat. Throwing in some AI and UASs could be a formidable weapon. Think Rollerball or Battle Bots engaging in the sky.



# 14. Satellite Killers

**By Dr. Mark Jackson**

## **Student Learning Objectives**

The student will be able to:

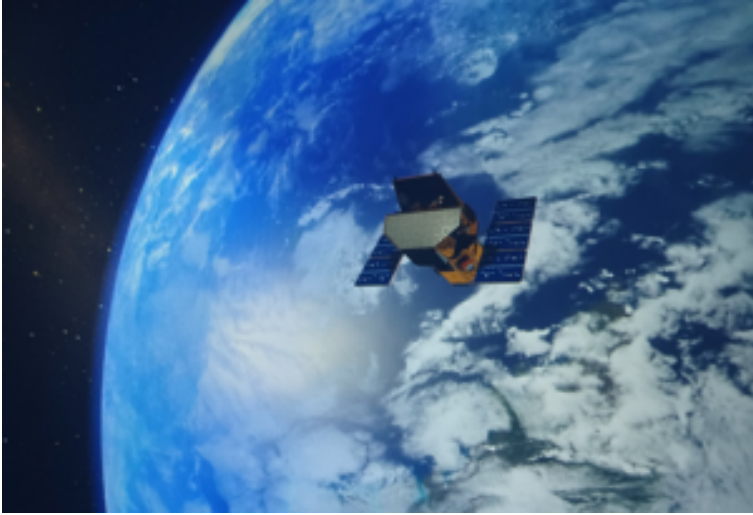
- Understand what a satellite is and how they are classified;
- Understand how satellites orbit and why they overlap in terms of orbital position;
- Understand the concept of denying space and satellite killers;
- Define the differences between directed energy weapons, ground-based killer missiles, and space-based weapon systems.

## **Satellites**

### **Introduction**

An artificial satellite is a stationary or rotating object intentionally put into orbit around Earth. The first artificial satellite was launched in 1957, and since that time, around 9,000 from 40+ countries have been launched into orbit. Currently, there are approximately 5,000 remaining in orbit where 2,000 are operational, and the rest are considered space debris. Two-thirds of the operational satellites are in low-Earth orbit, while the remaining third are in medium-Earth, geostationary and elliptical orbits (Figure 14.1).

**Figure 14.1. A satellite in Low Earth Orbit (LEO) around Earth**



Source: (U.S. Naval Academy, Colorado Springs, March 2022)

Space stations have been launched and assembled in orbit, while spacecraft have been placed in orbit around Earth's moon, Venus, Mars, Jupiter, Saturn, Mercury asteroids, comets, and the Sun. Satellites are used to map surfaces of planets and maps of distant stars and are military and civilian Earth-observing satellites. Some satellites are used for communication and navigation; they map weather patterns and are used as telescopes for deep space purposes. Constellations of satellites can also overlap orbits for many different purposes, such as weather tracking and communications.

Satellites are normally launched from a rocket from land, sea by submarine or mobile launch platforms, or launched from the air by aircraft. Sub-systems usually perform many different tasks that aid the satellite as it is launched and in orbit. The subsystems provide power, control temperature, control position and attitude, communicate and provide scientific data using sensors.

## **Classification of Satellites**

Satellites are classified in terms of their purpose and are classified as follows:

Astronomical satellites – observation of distant planets and galaxies;

Biosatellites – carry living organisms to aid scientific experiments;

Communication satellites – communications satellites use geosynchronous or Low Earth orbits to communicate with each other and other systems;

Earth observation satellites are satellites intended for non-military uses such as environmental monitoring, meteorology, and producing maps;

Killer satellites are designed to destroy warheads, satellites, and space-based objects;

Navigational satellites use radio time signals transmitted to enable mobile receivers on the ground to determine their exact location. The relatively clear line of sight between the satellites and receivers on the ground allows satellite navigation systems to measure location to accuracies on the order of a few meters in real-time;

Reconnaissance satellites are communications satellites deployed for military or intelligence applications;

Recovery satellites provide a recovery of reconnaissance, biological, space-production, and other payloads from orbit to Earth;

Space stations are orbital structures designed for human beings to live in space. A space station is distinguished from other crewed spacecraft by its lack of major propulsion or landing facilities. Space stations are designed for medium-term living in orbit;

Tether satellites are connected to another satellite by a thin cable called a tether; and

Weather satellites are used to monitor Earth's weather and climate.

## **Satellite Orbits**

The most common type of orbit is a geocentric orbit, with over 3,000 active artificial satellites orbiting the Earth. Geocentric orbits may be further classified by their altitude, inclination, and eccentricity.

The commonly used altitude classifications of the geocentric orbit are Low Earth Orbit (LEO), Medium Earth Orbit (MEO), Geosynchronous Orbit (GEO), and High Earth Orbit (HEO). Low Earth Orbit is any orbit below 2,000 km, Medium Earth Orbit is any orbit between 2,000 and 36,000 km, and High Earth Orbit is greater than 36,000 km (Figure 14.2).

### **Centric classifications**

A galactocentric orbit is an orbit around the center of a galaxy.

A heliocentric orbit is an orbit around the Sun. In our Solar System, all planets, comets, and asteroids are in such orbits, as are many artificial satellites and pieces of space debris.

Geocentric orbit is an orbit around Earth, such as the Moon or artificial satellites. Currently, there are over 2,500 active artificial satellites orbiting the Earth.

### **Altitude classifications**

Low Earth Orbit (LEO): Geocentric orbits ranging in altitude from 180 km – to 2,000 km;

Medium Earth Orbit (MEO): Geocentric orbits ranging in altitude from 2,000 km – to 20,000 km;

Geosynchronous Orbit (GEO): Geocentric circular orbit with an altitude of 36,000 km. The orbit period equals one sidereal day, which coincides with the Earth's rotation period. The speed is 3,075 m/s (10,090 ft/s).

High Earth orbit (HEO): Geocentric orbits above the altitude of a geosynchronous orbit (GEO) > 36,000 km (~ 40,000 km).

**Figure 14.2. Classification of altitude orbits and uses**



Source: ((Challenges to Security in Space, Defense Intelligence Agency, 2022 (www.dia.mil)))

### Inclination classifications

Inclined orbits are those whose inclination about the equatorial plane is not zero degrees;

Polar orbits pass above or nearly above both poles of the planet on each revolution. It has an inclination of ~ 90 degrees; and

Polar sun-synchronous orbits are polar orbits that have nodal

precessions such that a satellite in orbit passes the equator at the same local time on every pass.

### **Eccentricity classifications**

Circular orbits have an eccentricity of 0 degrees, and their path traces a circle;

Using two engine impulses, Hohmann transfer orbits move spacecraft from one circular orbit to another. The perihelion of the transfer orbit is at the same distance from the Sun as the radius of one planet's orbit, and the aphelion is at the other. The two rocket burns change the path from one circular orbit to the transfer orbit and later to the new circular orbit;

Elliptic orbits have eccentricities greater than  $> 0$  and  $< 1$ , whose orbit traces the path of an ellipse;

Geosynchronous transfer orbits are elliptic orbits where the perigee is at the altitude of a Low Earth Orbit (LEO) and the apogee at the altitude of a geosynchronous orbit. Satellites use this orbit to transfer to a geostationary orbit;

A geostationary transfer orbit is a transfer orbit that is used to transfer to a geostationary orbit;

Molniya orbit is a highly eccentric orbit with an inclination of  $63.4^\circ$  and an orbital period of half of a sidereal day ( $\sim 12$  hours). Such a satellite spends most of its time over two designated areas of the planet (Russia and America); and

Tundra orbit is a highly eccentric orbit with an inclination of  $63.4^\circ$  and an orbital period of one sidereal day ( $\sim 24$  hours). Such satellites spend most of their time over a single designated area of the planet.

### **Synchronous classifications**

Synchronous orbits where the satellite has an orbital period equal to the average rotational period of the body being orbited and in the same direction of rotation as that body. The satellite would trace an analemma in the sky;

Semi-synchronous orbits (SSO) with an altitude of approximately

20,200 km (12,600 miles) and an orbital period equal to one-half of the average rotational period of the body being orbited;

Geosynchronous orbits (GSO) with an altitude of approximately 35,786 km (22,236 miles);

Geostationary orbits (GEO) with an inclination of zero;

Disposal orbits are a few hundred kilometers above geosynchronous that satellites are moved into at the end of their operation;

Areosynchronous orbits around Mars with an orbital period equal in length to Mars' sidereal day, 24.6229 hours; and

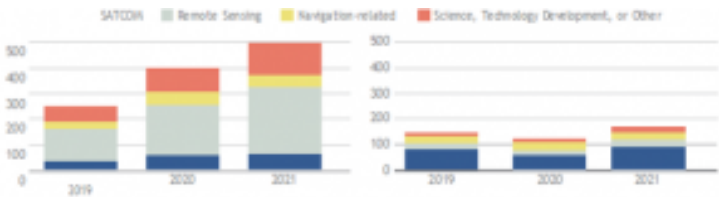
Heliosynchronous orbit is a heliocentric orbit about the Sun where the satellite's orbital period matches the Sun's period of rotation.

**Satellite Killers**

**Introduction**

Since 2019 the space fleets of China and Russia have grown by 70 % and continue to contribute to the congestion of the orbits. The continued expansion follows a period of growth since 2015 where China and Russia had increased their satellites numbers by 200 % in areas such as satellite communications (SATCOM) ~ 148 satellites, remote sensing ~ 294 satellites, navigation-related satellites ~ 77 satellites, and science and technology satellites ~ 143 satellites (Figure 14.3).

**Figure 14.3. Number of Russian (left) and Chinese (right) satellites in orbit between 2019 and 2021**



Source: (Union of Concerned Scientists – Satellite Database (1/1/2022) ([www.dia.mil](http://www.dia.mil)))

As space and counter-space capabilities increase, China and Russia integrate space scenarios into their military exercises. They continue to develop anti-satellite (ASAT) weapons, or killer satellites, that threaten the U.S. and allied space assets. China and Russia are pursuing ‘non-weaponization of space’ agreements at the U. N. to curb the strength of the U. S. The expansion of Chinese and Russian space weapons is changing the way nations formulate and formalize their space capabilities. This may lead to the denial of space for many different reasons.

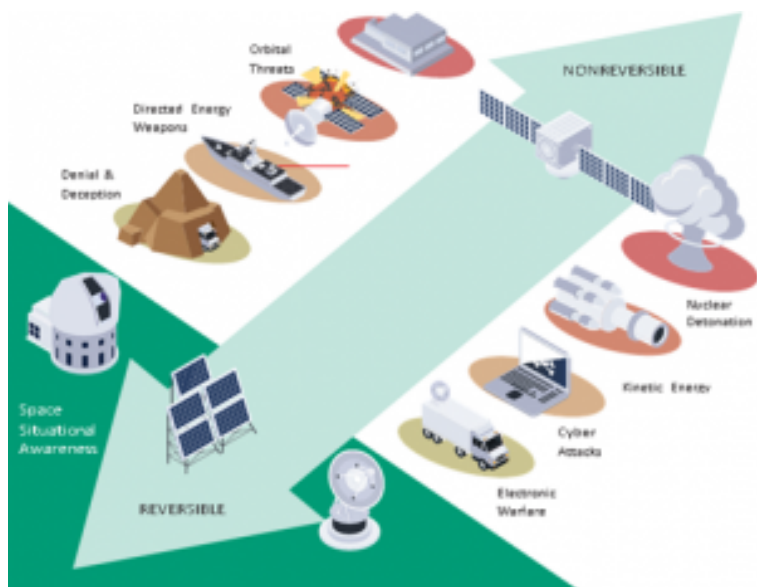
### **Denying space**

Space is critical for U.S. and allied military forces during operations, exercises, and logistics, providing for instantaneous communications, situation awareness, and precision navigation for the military. Military and civilian space services are not easily distinguished. Counterspace weapons are intended to degrade space capability others kill satellites permanently. The following conditions can occur (Figure 14.4):

- Physical or cyber-attacks against ground sites and infrastructure supporting space operations can threaten satellites;
- Space awareness sensors predict when satellites pass overhead allowing for the tracking, warnings, and targeting of space systems;
- Global navigation and communications satellites can be jammed by enemies that are used for naval, ground, and air forces as well as manned and unmanned vehicles;
- Adversaries that target satellites can blind imagery satellites and other strategic sensors, denying the ability to monitor, track, and target forces.



**Figure 14.4. The counter-space continuum shows the range of threats to space-based satellite services. Reversible effects include temporarily affecting space services, while irreversible effects include direct energy weapons, orbital threats, and nuclear detonations that permanently kill satellites services.**



Source: (DIA, 2022).

- Killer missiles can be used to kill satellites in LEO and produce debris that can remain in orbit for decades or even centuries. China tested a killer missile against its defunct weather satellite in 2007 that created a debris cloud posing a threat to satellites in close orbits. Russia also used a killer missile in December 2021 to destroy one of its satellites.

Other space-based weapons can kill satellites. Countries with nuclear weapons can launch a warhead on a long-range booster

ICBM and conduct a high-altitude nuclear detonation, which would create widespread electromagnetic disruptions in space and on Earth, leading to killing or severely disrupting satellites.

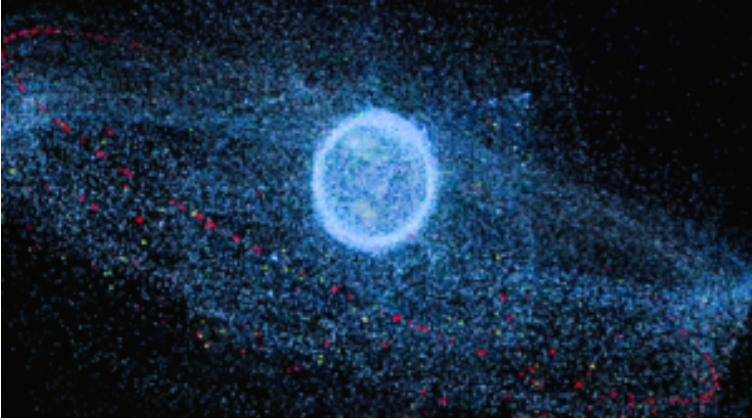
### **Satellite Killers: China**

China destroyed one of its weather satellites more than 800 kilometers above the Earth with a satellite-killing missile in 2007. This destructive test generated more than 3,000 pieces of trackable space debris, of which more than 2,700 remain in orbit, and most will continue orbiting the Earth for decades (Figure 14.5). China's military units have continued training with satellite killing missiles.

China intends to develop more killer satellite weapons to destroy satellites up to GEO. In 2013, China launched an object into space on a ballistic trajectory with a peak orbital radius above 30,000 kilometers to GEO altitudes suggesting that a basic capability could exist to use satellite killers at great distances beyond LEO. China is also developing other space-based capabilities such as satellite inspection and repair. China has launched multiple satellites to conduct scientific experiments on space maintenance and is conducting research on space debris cleaning. In January 2022, Shijian-21 moved a navigation satellite to a high graveyard orbit above GEO. Space-based robotic arm technologies may be used in a future system for capturing space debris.

Since 2006, universities in China began investigating aerospace engineering aspects associated with space-based kinetic weapons used to kill satellites and other space-based assets. Space-based kinetic weapons research includes re-entry methods, separation of pay-load, delivery vehicles, and transfer orbits for targeting purposes. China also conducted the first fractional orbital launch of an ICBM with a hypersonic glide vehicle in July 2021. This demonstrated the greatest distance flew (~40,000 kilometers) and the longest flight time (~100+ minutes) recorded for a hypersonic glide vehicle.

**Figure 14.5. Computer simulation of tracked objects in Earth's orbit. Red, yellow, and green objects are representations of active satellites and debris in the GEO and MEO.**



Source: (DIA, 2022)

### **Satellite Killers: Russia**

Russia is developing a mobile missile defense complex capable of destroying ballistic missiles and low-orbiting satellites. The weapon system created over 1,500 pieces of trackable space debris and tens of thousands of pieces of lethal debris in November 2021. The debris endangers spacecraft in LEO, including astronauts and cosmonauts on the ISS and China's Tiangong space station. Russia demonstrated the capability of the missile to destroy satellites in LEO and is developing an air-launched killer weapon targeting spacecraft in LEO. Further orbital threats include a killer weapon developed by Russia that targets foreign satellites but protects Russian satellites. The same technology can inspect and diagnose satellites' technical conditions before repairing or killing them.

In 2019, Russia launched two satellites, with one following a U.S. national security satellite. In July 2020, Russia launched an object into orbit near a similar Russian satellite to test a space-based killer

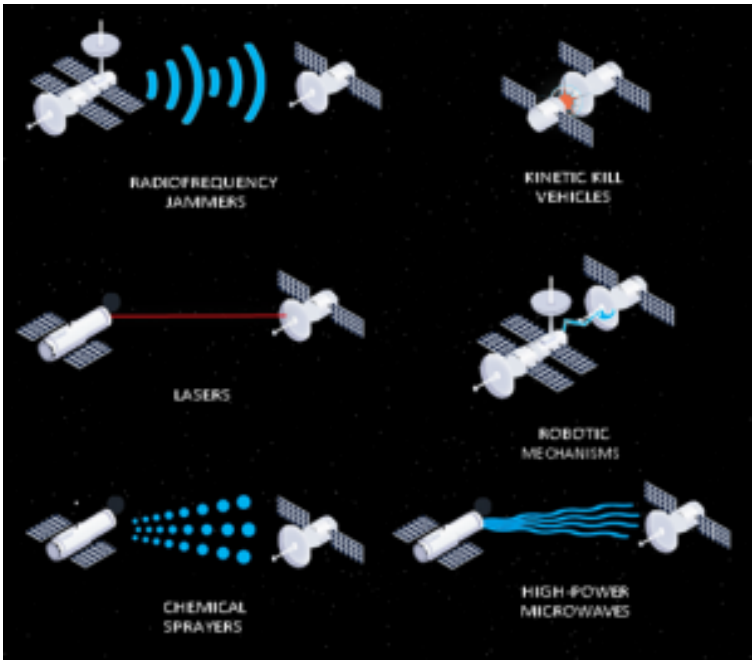
weapon. Cosmos 2504 and Cosmos 2536 are prototype Russian killer weapons that can kill satellites in LEO.

### **Space Awareness and Space-Based Weapons**

Directed energy weapons are designed to produce reversible or non-reversible effects against space systems to disrupt, damage, or destroy enemy equipment and facilities. Directed energy weapons include lasers, high-power microwaves, and radiofrequency weapons. Reversible effects include temporarily blinding optical sensors to deny imagery of targeted military forces. Non-reversible effects include permanently damaging or destroying sensors or other satellite components.

Killer missiles are designed to destroy satellites without being in orbit. The weapons typically consist of a fixed- or mobile-launch system, a missile, and the kinetic kill vehicle. The weapons may also be launched from aircraft, ships, and submarines. The kinetic kill vehicle uses a seeker to intercept the satellite. Ground-based create orbital debris and can easily be detected (Figure 14.6).

**Figure 14.6. Space-based weapons**



Source: (DIA, 2022)

Space-based weapons are satellites that can attack other spacecraft, thus making spacecraft sitting targets. They include radiofrequency jammers, kinetic kill vehicles, lasers, chemical sprayers, and high-power microwave weapons.

### Questions

1. What is a satellite?
2. Describe the orbits of satellites and the type of orbit required for communication satellites?
3. What are the altitude and centric classifications of satellites?
4. What is a satellite killer, and why deny space to a particular nation?
5. Explain why Russia and China need to kill satellites and how

they achieve this?

6. What is space debris, and why is it so damaging to other satellites?
7. What are the implications of space awareness?
8. Describe the multitude of space-based weapons.

## **Bibliography**

(n.d.).(*Challenges to Security in Space*, Defense Intelligence Agency, 2022 ([www.dia.mil](http://www.dia.mil))).

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 Navy Unmanned Undersea Vehicle Master Plan*. Washington DC, USA: US Government.

DIA. (2022). *Challenges to Security in Space*. Retrieved from [www.dia.mil](http://www.dia.mil): [www.dia.mil](http://www.dia.mil)

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.

(n.d.).The U.S. Naval Academy, Colorado Springs, March 2022.

(n.d.). *Union of Concerned Scientists – Satellite Database* (1/1/2022) ([www.dia.mil](http://www.dia.mil)).

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

## **Informative Readings and Additional Bibliography**

### **Satellite Killing and Denying Space:**

Azanov, Roman; 24 December 2019; “‘Armament Is Not a Chess Game.’ What Equipment the Russian Army Received in 2019: TASS on Principal Deliveries of Military Equipment and Arms to the Country’s Armed Forces Arms and Branches According to the Year’s Results”; TASS.

Claus, Malcom; 9 November 2018; “New Russian missile likely to be part of the anti-satellite system”; Jane’s Intelligence Review.

Comprehensive Nuclear Test Ban Treaty Organization; 5 November 2020; “9 July 1962: ‘Starfish Prime,’ Outer Space”; <https://www.ctbto.org/specials/testing-times/9-july-1962starfish-prime-outer-space>. Accessed February 17, 2022.

Dickinson, James H., Gen.; 21 April 2021; United States Space Command Presentation to the Subcommittee on Strategic Forces, House Armed Services Committee, U.S. House of Representatives: Fiscal Year 2022 Priorities and Posture of the United States Space Command, p. 6; <https://docs.house.gov/meetings/AS/AS29/20210421/112467/HHRG-117-AS29-Wstate-DickinsonJ-20210421.pdf>. It was accessed on March 12, 2022.

Gazeta; 28 July 2018; “In Russia, new strategic weapons are being created.”

Gundarova, Lyudmila; 27 May 2021; “Star/Junk Wars: How to Blind the Enemy and Not Blind Yourself”; Nezavisimoye Voennoye Obozreniye; <https://nvo.ng.ru>.

Hendrickx, Bart; 27 September 2018; “Russia Develops Co-Orbital Anti-Satellite Capability”; Jane’s Intelligence Review.

Hennigan, W.J.; 23 July 2020; “America Really Does Have a Space

Force. We Went Inside to See What It Does”; Time; <https://time.com/5869987/spaceforce/>.

Izvestiya; 28 May 2019; “An Expert Has Spotted the Russian VKS’s New Missile Interceptor.”

Jones, Andrew; 29 October 2021; “China launches classified space debris mitigation technology satellite”; Space News; <https://spacenews.com/china-launches-classified-space-debris-mitigation-technology-satellite/>. It was accessed on March 15, 2022.

Khodarenok, Mikhail; 19 June 2020; “Russia: Defense Industry Source Provides Delivery Schedule for S-500 Prometey, Nudol Systems”; Gazeta; <https://www.gazeta.ru/army/2020/06/19/13123189.shtml>.

Milkavkaz.net; 23 December 2015; “Russia: Aerospace Forces Order of Battle.”

Mizokami, Kyle; 1 October 2018; “Russia’s MiG-31 Spotted with Possible Anti-Satellite Missile”; Popular Mechanics; <https://www.popularmechanics.com/military/weapons/a23549729/russia-s-mig-31-spotted-with-possible-anti-satellite-missile/>.

Mizokami, Kyle; 16 August 2018; “Is Russia’s Mysterious New Satellite a Space Weapon?” Popular Mechanics; <https://www.popularmechanics.com/military/weapons/a22739471/is-russias-mysterious-new-satellite-a-space-weapon/>.

Nebehay, Stephanie; 14 August 2018; “U.S. Warns on Russia’s new space weapons”; Reuters; <https://www.reuters.com/article/us-russia-usa-space-idUSKBN1KZ0T1>.

O’Connor, Tom; 12 March 2018; “Russia’s Military has Laser Weapons that Can Take out Enemies in Less than a Second”; Newsweek; <http://www.newsweek.com/russia-military-laser-weapons-take-out-enemies-less-second-841091>.

Office of the Director of National Intelligence; 11 May 2017; Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community, p. 9.

Office of the Director of National Intelligence; 13 February 2018;



Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community, p. 13.

Office of Director of National Intelligence; 11 December 2020; “Support to U.S. Space Command Messaging.”

Office of the Secretary of Defense; April 2015; Annual Report to Congress: Military and Security Developments Involving the People’s Republic of China 2015, p. 14; [https://dod.defense.gov/Portals/1/Documents/pubs/2015\\_China\\_Military\\_Power\\_Report.pdf](https://dod.defense.gov/Portals/1/Documents/pubs/2015_China_Military_Power_Report.pdf). It was accessed on March 8, 2022.

Office of the Secretary of Defense; 1 September 2020; Annual Report to Congress: Military and Security Developments Involving the People’s Republic of China 2020, p. 65; <https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF>. It was accessed on March 8, 2022.

Poblete, Yleem D.S.; 14 August 2018; “United States Remarks at the Conference on Disarmament as Delivered by Assistant Secretary of State for Arms Control, Verification, and Compliance”; U.S. State Department; <https://eneva.usmission.gov/2018/08/14/remarks-by-assistant-secretary-yleem-d-s-poblete-at-the-conference-on-disarmament/>.

Ramm, Alexei; 19 April 2019; “Targeting Stars: What is Known about the New ASAT Weapon? Project NUDOL”; Izvestiya.

Space Control Squadron; “Box Score”; Space-Track.org; <https://www.space-track.org/#boxscore>. It was accessed on March 15, 2022.

TASS; 6 December 2019; “The Ministry of Defense Conducted an Experiment in Space to Separate a Small Satellite from Another Device.”

13. S. Joint Chiefs of Staff; 26 October 2020; Joint Publication 3-14: Space Operations (10 April 2018, Incorporating Change 1), p. I-13.

U.S. Space Command Public Affairs; 15 November 2021; “Russian direct-ascent anti-satellite missile test creates significant, long-lasting space debris”; <https://www.spacecom.mil/news/article-display/article/2842957/russia-direct-ascent-anti-satellite-missile-creates-significant-long-last/#.yzrxfviqu4>. Accessed March 14, 2022.

Vyatkin, Yaroslav; 16 April 2015; “Russian Potential for Combating, Acquiring Prompt Global Strike Capability Examined”; Argumenty Nedeli.

Yezhenedelnik Zvezda; 29 September 2020; “Russian Military-Industrial Complex: Debt, Red Tape Impact the Execution of the State Defense Order.”

Zvezda Television; 29 December 2019; “Russia to deploy airborne Peresvet laser.”

### **Space Awareness and Space-based Weapons:**

AP News; 21 September 2020; “German military opens new space operations center”; <https://apnews.com/article/national-security-germany-europe-archive-russia-94aaa4939c5c736e268f-388700b49c6b>. Accessed March 5, 2022.

Blenkin, Max; 3 February 2020; “Germany signs up for multinational Combined Space Operations Initiative”; Space Connect; <https://www.spaceconnectonline.com.au/operations/4116-germanysigns-up-for-multinational-combined-space-operations-initiative>. Accessed March 4, 2022.

Challenges To Security In Space – Space Reliance in an Era of Competition and Expansion, Defense Intelligence Agency, March 2022, p.p. 1 – 70. ISBN 978-0-16-095566-2.

Chuter, Andrew; 15 January 2020; “Former Fighter Pilot Picked to Lead British Military’s Space Command”; Defense News; <https://www.defensenews.com/global/europe/2020/01/15/former-fighter-pilot-picked-to-lead-british-militarys-space-command>. They were accessed on March 16, 2022.

DOD News; 5 September 2014; “DoD Agrees to Share Space Data

with South Korea”; <https://www.defense.gov/Explore/News/Article/Article/603194/>. It was accessed on April 2, 2022.

EuroNews; 13 July 2019; “France’s Macron announces creation of French Space Force”; <https://www.euronews.com/2019/07/13/france-s-macron-announces-creation-of-french-space-force>. It was accessed on March 17, 2022.

Johnston, Eric; 2 June 2020; “Japan’s New Space Squadron Takes a Giant Leap Forward”; The Japan Times; <https://www.japantimes.co.jp/news/2020/06/02/national/japan-space-force-self-defense-forces/>. Accessed March 5, 2022.

Jungholt, Thorsten; 21 August 2019; “Armament in Space – Still Without Weapons”; Die Welt; <https://www.welt.de/politik/deutschland/plus198779675/Bundeswehr-So-laeuft-die-Aufruestung-im-Weltraum.html>. Accessed March 7, 2022.

Lye, Harry; 2 April 2020; “Will the UK get a Space Command?” Airforce Technology; <https://www.airforce-technology.com/features/will-the-uk-get-a-space-command/>. Accessed March 4, 2022.

Miles, Cody, Maj.; 11 February 2020; “German delegation visits Vandenberg, discusses future of space operations”; Combined Force Space Component Command Public Affairs; <https://www.spacecom.mil/MEDIA/NEWS-ARTICLES/Article/2081290/german-delegation-visits-vandenberg-discusses-future-space-cooperation/>. Accessed March 6, 2022.

Republic of Korea Ministry of National Defense; 11-1290000-000446-11; 31 December 2018; 2018 Defense White Paper, p. 19; <https://www.mnd.go.kr/user/mnd/upload/pblicitn/PBLICTNE->

Republic of Korea Ministry of National Defense; 11-1290000-000446-11; 31 December 2018; 2018 Defense White Paper: [https://www.mnd.go.kr/user/mnd/upload/pblicitn/PBLICTNE-BOOK\\_201907110548253080.pdf](https://www.mnd.go.kr/user/mnd/upload/pblicitn/PBLICTNE-BOOK_201907110548253080.pdf). It was accessed on April 2, 2022.

UK Ministry of Defense; 11 November 2015; National Security Strategy and Strategic Defense and Security Review 2015, p. 19. [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/478933/](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/)

52309\_Cm\_9161\_NSS\_SD\_Review\_web\_only.pdf. It was accessed on March 2, 2022.

UK Ministry of Defense; 28 March 2018; National Security and Capability Review, p. 19; [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/705347/6.4391\\_CO\\_National-Security-Review\\_web.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/705347/6.4391_CO_National-Security-Review_web.pdf). Accessed March 2, 2022.

UK Ministry of Defense; 17 June 2020; Toward a Defense Space Strategy; [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/712376/MOD\\_Pocket\\_Tri-Fold\\_-\\_Defence\\_Space\\_Strategy\\_Headlines.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/712376/MOD_Pocket_Tri-Fold_-_Defence_Space_Strategy_Headlines.pdf). Accessed March 2, 2022.

### **Space Breakthroughs and Inventions:**

Brinson, Linda C.; March 2011; “What breakthroughs in medicine came from NASA?” How Stuff Works; <https://science.howstuffworks.com/innovation/nasa-inventions/nasa-breakthroughs-in-medicine.htm>. They were accessed on March 25, 2022.

International Space Exploration Coordination Group; Benefits Stemming from Space Exploration; September 2013; <https://www.nasa.gov/sites/default/files/files/Benefits-Stemming-from-Space-Exploration-2013-TAGGED.pdf>. They were accessed on March 25, 2022.

NASA Jet Propulsion Laboratory; 20 Inventions We Wouldn't Have Without Space Travel; <https://www.jpl.nasa.gov/infographics/infographic.view.PHP?id=11358>. It was accessed on March 26, 2022.

# 15. Cyber Weapons and CBRNE

**By Professor Randall K. Nichols, Kansas State University**

## **Student Objectives**

In this chapter, we will explore:

- 1) Threats to Air Defense Systems and CBRNE facilities by hostile use of sUAS / UAS,
- 2) A look at the history to demonstrate the increasing threat level that sUAS/UAS poses to ADS and CBRN?
- 3) Discuss the Infrastructure interdependencies and leveraging ability of cyber-attacks,
- 4) Classify Cyber-attacks by area on CBRN facilities
- 5) Discuss the Counter – UAS problem (how do we intercept the UAS headed for an ADS or CBRN facility. Emphasis will be on the ADS because the CBRN is low-hanging fruit without it.
- 6) Discuss the operational measures and active/passive measures against hostile-controlled sUAS /UAS targeting an ADS

## **Problem – The Risk of Terrorist Attack vs. U.S. Air Defense System or CBRN Facilities**

The risk of successful terrorist attacks on U.S. Air Defense Systems (ADS) and CBRNE facilities by sUAS /UAS is growing because of increased commercial capabilities and accessibility of advanced small drones. They can carry sophisticated imaging equipment with significant and potentially lethal payloads, perform extensive Intelligence, Surveillance, and Reconnaissance (ISR) missions, and are readily available to civilians. A significant threat

to civilian and military UAS operations, CBRN facilities, and safety is posed by UAS/drones controlled by hostile actors, including large potential threats to U.S. Air Defense Systems and CBRN facilities from UAS SWARMS. (Nichols R. K., Chapter 18: Cybersecurity Counter Unmanned Aircraft Systems (C-UAS) and Artificial Intelligence, 2022) Another significant threat is maritime operations and navigation / GPS / GNSS signals spoofing. (Nichols R. K., Chapter 14: Maritime Cybersecurity, 2021)

*Think of the UASs / Drones as flying SCADA machines or flying advanced telephones.* All the SCADA vulnerabilities or wireless communications vulnerabilities exist and can be exploited from a defensive POV. These vulnerabilities were discussed in detail in (Nichols R. R., 2020), (Nichols R. K. et al., 2019) and (Nichols R. K., Chapter 18: Cybersecurity Counter Unmanned Aircraft Systems (C-UAS) and Artificial Intelligence, 2022)

*However, from the attack POV, UAS / drones are effective delivery systems, and the same SCADA vulnerabilities and wireless exploits are available on their targets.* The weapon systems used in potential attacks on Critical Infrastructure Systems (CIS)[\[1\]](#) or Industrial Control Systems (ICS) are more powerful than the defenses when they involve CBRNECy payloads. Advancing technologies have integrated with ICS as one. Remote access to controlled equipment facilities has become the standard in almost every industry. (Martinelli, 2017)

**Cybersecurity** is defined as the protection of information systems from theft or damage to the hardware, the software, and the information on them, and from disruption or misdirection of the services they provide identified. (Gasser, 1988) **CBRNE cybersecurity** is defined as the practice of security of computer systems, ICS, and networks in the critical industry that involves CBRNE agents. **CBRNECy** introduces the cyber components, security, and management if damaged entails global danger.

For the special case of CBRNECy assets, whether attacked via UAS /drone, any nuclear or chemical facility is equal to a warfare attack. As of today, and as publicly revealed, the maximum damage caused by cyberattacks was related to:

- CBRNE agent device rendered unstable or non-fit to the purpose (Stuxnet, Iran),
- though theoretical analysis confirms that the attackers could physically
- destroy the device.
- Power distribution was rendered offline (BlackEnergy3, Ukraine), where the power supply

ply (APS) device was reconfigured to disable the power distribution.

- Communications disabled (BlackEnergy3, Ukraine). (Martinelli, 2017)

As per the predictions by Bruce Schneier and IEEE (Staff I., 2013), the possible cyber-attack capabilities in the future will relate to (Schneier 2015):

- Hybrid warfare (Cyber and any other warfare domains)
- Global Denial of Service (e.g., Internet infrastructure collapse)
- Refined delivery via email (advancements in spam and spear phishing)
- Advanced malware delivery via web applications
- Substantially increased malware sophistication and AI
- Attacks on critical infrastructure will increase
- Lone-wolf terrorism

Cyber-attacks are already a threat to national security, and NATO recognizes cyberspace as one of the warfare domains. (Nichols R.

R., 2020) With the exponential growth of cyber technologies, the threat to embedded devices and ICS will only increase and, if not prevented, will reach the global level. *The authors predict that the next evolution of cyber weapons will be deployed from UAS/ drones against CBRNE assets.* After the U.S. Afghanistan withdrawal debacle in 2021, the hard-core terrorists have a billion dollars plus of advanced military UAS toys to experiment with and plenty of offered technical help from its neighbors to the South and North. The Taliban have inherited some unmanned weapons from their fellow terrorists in Afghanistan. (DRONESEC, 2021)

### **CBRN Infrastructure Attacks**

Not very public, not often, but CBRN infrastructure cyber-attacks / disruptions have occurred.[2] In January 2002, malware successfully breached the perimeter network defenses at Ohio's Davis-Besse nuclear power plant, infiltrated the private networks, and disabled the safety monitoring system for five hours. (Poulsen, 2003) In October 2006, cyber attackers gained access to computer systems at Harrisburg, PA, water treatment plant. The ICS network was compromised, threatening the plant's water treatment operations. (CIO Staff, 2006) In October 2008, the derailment of the tram in the city of Lodz injured 12 people. The attacker used a repurposed T.V. remote control to change the track points through an Infrared sensor. (Schneier on Security, 2008) The 2010 event in Iran confirmed that information technology could trigger remote CBRN attacks and be a direct threat to physical CBRN ICS equipment. Stuxnet was the first CYBERWEAPON. [3] It was designed to infiltrate and cause physical disruption in multiple ICS in the Natanz CBRN facility and other facilities. It slowed the Iranian nuclear ambitions by about six months. (Wilson, 2014) In 2011, the Trojan "Poison Ivy" was used to collect intellectual property from twenty-nine international chemical companies. (Dark Reading Staff, 2013) In 2014, Malware Shamoon wiped 30,000 workstations in Saudi Aramco's corporate network by bypassing firewalls and intrusion detection systems (IDS) on a large scale. (Staff, 2014) Again,



in 2014, 13 different types of malware disguised as ICS/SCADA software updates to major corporations' systems were detected in spear-phishing emails. Forensic analysis determined that malware was a repurposed banking Trojan designed to capture private identifying information (PII) and credentials. (Higgins, 2015) In 2015, a BlackEnergy3 DOS attack on a power plant and multiple substations in Ukraine triggered a severe power outage. (Miller, 2022) Since 2015, it is estimated that corporations globally have suffered over 1,518 million ransomware attacks. (Johnson, 2022)

*The events listed above indicate a constant evolution of attack CBRNE capabilities of threat actors. The next evolution is swift, silent, and deadly by air delivered by UAS / drones.*

### **Contributing Technologies**

Commercial and military UAS are integrally linked to the payload, navigation, communications, and control linkages from the ground, air, or satellite. These advanced small /medium-sized drones are vulnerable to cyber-attack and hostile takeover, so UAS designers and operators must be aware of cybersecurity countermeasures and defenses to reduce the risk of takeover and penetration by hostile or negligent forces on either ADS or CBRN facilities. (Nichols, Mumm, Lonstein, Ryan, & and Carter, 2018)

UAS are being designed with increasingly advanced Artificial Intelligence (AI) and automation capabilities that can be beneficial and harmful. The increased automation and AI capabilities can be used to complete Dull, Dangerous, and Dirty (DDD) missions in all weather conditions and are capable of longer flying times and endurance at more effective altitudes. Unfortunately, when human decisions are taken out of the loop, software and firmware code can be intercepted, replaced, re-engineered, spoofed, exploited, destroyed, and used against the originator. Iran accomplished this in 2011 (Jaffe & Erdbrink, 2011).

The number and type of possible cyber exploits against UAS key

CBRN control systems (payloads, navigation, rotors, battery) represent a large, diverse, and lethal attack vector set. However, the UAS designer and operator are not without an effective arsenal of Counter Unmanned Aircraft Systems (C-UAS) measures. (Nichols R. R., 2020)

***Attack / Defense Scenarios***

When hostile forces fly a UAS against ADS or CBRN facilities, the cyber risk analyst’s mission is to determine the Risk, Threats, Vulnerabilities, Impacts, and Countermeasures that may apply in an attack/defense scenario. The attacker has the advantage of flexibility, source, type of cyber-vector, location, height, frequency, and lethality of his cyber-attack. The more difficult job of the defense includes identifying the intruder and intrusion measure and applying the correct countermeasure [cybersecurity (non-kinetic), physical (kinetic), or electronic] in real-time.

AI[4] plays a role on both sides of this attack/defense scenario. It speeds up the decision-making capabilities of both attacker and defender and can determine the risk mismatch between opposing forces. Cybersecurity attacks on UAS or CBRNE assets should never be underestimated; damage to ships, navigation systems, commercial airplanes, property, and privacy is possible. (Nichols, Mumm, Lonstein, Ryan, & and Carter, 2018)

**Description of the sUAS/UAS Landscape – What’s available for Deployment against CBRNE Assets?**

***Autonomy v Automation Levels***

sUAS/UAS automation is divided into five classes of technology. Table 15.1 shows a breakdown of the automation landscape.

**Table 15.1 Automation Levels**

| Automation Level | Name  | Characteristics   | Examples   |
|------------------|---|---|--|
| Level 1          | Slave   | Assist with piloting, reacting to disturbance, Remote Control Tethers (R.C.)  | Drone Parrot, Quad Flyer GAUI  |
| Level 2          | Automated   | Maintains its flying orders and receives higher-level orders and commands.<br><br>Levels 1 and 2 are commonplace in the market. They require pilot intervention and a continuous communication link(s). Reasonable prices <\$1500 US, small size, weight < 10 lbs.: | Chinese Dove, DJI Phantom series, Raven, Scan Eagle, Harpy   |
| Level 3          | Automated -Navigation                             | Automated navigation (pre-programmed flight plan, based on GPS coordinates). Some with Follow Me autopilot settings enable the sUAS to follow the operator automatically. Micro-UAS premium cost < \$20,000 US.   | Dragonfly, Microdrone GMBH, Fly-n-Sense, Micro copter, ASN-205, GJ-1, aka Wing Loong I. Fire Scout, WASP III, Shadow, Heron, Hermes, Barracuda |
| Level 4          | Contextual Response<br><br>CA <a href="#">[5]</a> | Response from contextual data (w/o human intervention) for Collision Avoidance (C.A.). They use active SAA and require a mission plan. Costs and missions are classified.   | Predator, Reaper, Avenger, Global Hawk, BZK-005, Mantis, Soaring Dragon, Sentinel  |

|         |                |  |   |
|---------|----------------|--|---|
| Level 5 | Decision Maker | Full AI does not require human intervention. Includes AI Decision-making with heavily networked computer support, has perceptive sensors for space and time. Can complete complex missions in unknown environments, capable of intelligent adjustments including mission rescheduling and key word-adaptive control. Decision-Maker (expert system) works from contextual data with coordination and collaboration of signals [Think “Terminator”] | Levels 4 and 5 are confined to laboratories.<br><br>X47C series<br><br>Classified Cost and Missions |
|---------|----------------|--|---|

---

Source: (Nichols R. K., Drone Wars: Threats, Vulnerabilities and Hostile Use of UAS, 2017) and (Nichols, Mumm, Lonstein, Ryan, & and Carter, 2018)

Table 15.1 shows the normal five levels of automation that characterize UAS systems with some examples of commercial vehicles at each level. NASA has a more detailed automation breakdown based on the OODA (Observe, Orient, Decide, and Act) decision loops (Barnhart, 2012).

Level 1 Slave and Level 2 minimally automated UASs are commonly sold by Amazon, Walmart, and similar outlets. The human pilot makes all the decisions and has complete control of the flying orders. Level 3 steps up the navigation capabilities with the ability to use a mission plan.

Levels 4 and 5 add higher-level decision-making capabilities; collision avoidance without human intervention, complex mission planning in all weather conditions, expert systems intelligence without human intervention [i.e., Artificial Intelligence (AI) and advanced Sense and Avoid systems (SAA)]. Level 5 is not commercially available, but many designers are well on their way to

a fully operational Level 5 UAS. Much of the information on Level 5 designs and capabilities are classified. In the author's opinion, removing humans from the decision loop in weaponized Level 5 UASs is a very risky venture.

### **UAS Collaboration**

Table 15.2 UAS Collaboration shows four types of possible UAS collaborations. At the lower end of a threat scale is the *isolated* attack by one UAS or a small group of UAS. The Type 1 specific missions may be piloted or autonomous. They carry light payloads, are affordable, and are easily assembled in the field. An example is the Raven used by U.S. Special Forces. The countermeasure for this type of attack is to identify the pilot or leader vehicle and destroy or disable it.

A UAS attack *team* is particularly effective against divided attack targets since disabling part of the UAS Team does not guarantee mission failure. The real vulnerability of the UAS team is the Chief; all synchronization and updates go through the Chief. If the Chief is disabled or destroyed, the team is rendered useless. Identifying the Chief is critical and is normally accomplished through intercepting communications (Nichols, Mumm, Lonstein, Ryan, & Carter, 2018).

Far more dangerous is the SWARM configuration, especially at the higher levels of autonomous engagement. SWARMS have several advantages. They are efficient through sheer numbers, and even when not controlled or automated, they display a decentralized intelligence, much like a shoal of fish that moves together synchronously. UAS SWARMS are not dependent on the survival of all of the members. Destroy part of the SWARM, and the rest will continue their mission without abatement (Nichols, Mumm, Lonstein, Ryan, & Carter, 2018).

Known countermeasures for a SWARM are:

- 1) Disruptors change the Strategic Global View of SWARM (its only real vulnerability)
- 2) Force defender collaboration
- 3) Long-range acoustical weapons aimed at MEMS to disrupt SCADA and rotor subsystems
- 4) Classified / OPEN methods involving DEW, Drone catchers, Lasers, GPS spoofing (Nichols R. K. et al., Counter Unmanned Aircraft Systems Technologies, and Operations, 2020)

Research on acoustic countermeasures indicates that they are successful against SWARMS and have the secondary advantage of being able to Identify Friend or Foe (IFF) using searchable sound frequency libraries (Nichols R. K. et al., 2019). (Nichols R. K. et al., Counter Unmanned Aircraft Systems Technologies, and Operations, 2020) China appears to be the leader in innovative UAS SWARM intelligence through the Chinese Electronics Technology Group Corporation (CETC) (Kania, 2017).

**Table 15.2 UAS Collaboration**

| Type | Name   | Advantages  | Disadvantages   | Countermeasures   |
|------|--|---|---|---|
| 1    | Isolated Individual UAS  | Piloted or autonomous w/ a specific mission to perform. Small, easy to assemble, affordable, light payloads.  |   | Stop, disable, or destroy the pilot and remove the threat.  |
| 2    | Group of Individual UASs   | Each UAS has its mission, but the group is not a coordinated team.<br><br>An increased number of attackers increases the potential for success by saturating the defenses.  | The sphere of action may be different for each UAS's mission. Mission will not be fully completed when individual UASs are destroyed. | Stop, disable, discover, and deter or destroy pilot(s), and threat(s) may be removed.   |
| 3    | Team of UASs (All members assigned specialized tasks and coordinated by Chief) | Particularly effective against divided attack targets. Level 3 allows automatic navigation and synchronized actions but no update to mission plans based on-field activities.<br><br>Level 5 permits continuous updates and communications, commando style. | Level 4 (w/o humans) yields surrounding reactions but may lose synchronization between team members.                                  | Stop, disable, or destroy team members. Determine behavior logically and intervene. The survival of team members is critical to defense actions. Mitigate the threat. |

|   |  |  |  |   |
|---|--|--|--|---|
|   |  | Efficient based on numbers, emergent large group behaviors and reactions, not controlled or automated, decentralized intelligence – think shoal of fish w/ evolving local rules. A highly defense resistant form, not based on the survivability of individual members, with no hierarchy. |  | Disrupt/Change the Strategic Global View of SWARM (its only real vulnerability). Defender collaboration. (Kania, 2017)  |
| 4 | UAS SWARM (Uniform mass of undifferentiated individuals w/o Chief at level 4 or 5) | Strategic Weapon   | None except maybe cost and launch coordination | Subject to Acoustic Countermeasures up to a mile. Research at short distances and loud sound at resonance is particularly effective against MEMS and rotor systems (Nichols R. K. et al., 2019) |

---

Source: (Nichols R. K., Drone Wars: Threats, Vulnerabilities and Hostile Use of UAS, 2017)

### Cyber Related CBRNE Attacks

A cyberattack against ADS or CBRN launched from a UAS / drone, or SWARM can be conducted in many ways and for many reasons. Cyber-attacks on CBRNE can be classified by area, industry, perceivable damage, and possible attack scenario. Cyber-attack vectors have many custom-designed exploits such as flying false routers, access points, network layers, and specialized software/malware/ransomware. (Martinelli, 2017) Nichols presents a taxonomy of wireless cyber-attacks which can be launched against or by UAS. (Nichols R. K., Chapter 18: Cybersecurity Counter Unmanned Aircraft Systems (C-UAS) and Artificial Intelligence, 2022) (Nichols R. K. et al., Counter Unmanned Aircraft Systems Technologies, and Operations, 2020)

Table 15.3 reflects potential CBRNECy cyber-attacks by area.

There are four attack vectors on any facility as a structure.



Attacks #s 1-3 may be launched by air vehicle / UAS. Attack 4 may be assisted by UAS. Cyber-attack: the attackers have no physical access to the systems or devices.

1. Physical attack: the attackers have no remote access to systems or devices.
2. Cyber-enabled physical attack: security system is compromised to enable easy physical access for the attackers.
3. Physical-enabled cyber-attack: physical actions allow remote access to unreachable computer systems or networks. (Martinelli, 2017)
4. Physical-enabled cyber-attack: physical actions allow remote access to unreachable computer systems or networks (rogue devices or rogue access points or spy)

See Figure 15.1 and 15.2 for a view of CIS interrelations and dependencies. (Peerenboom, 2001)

**Figure 15.1 CIS Shared Threats**



Source: (Peerenboom, 2001)

Figure 15.2 Infrastructure Interdependencies



Source: (Peerenboom, 2001)

Table 15.3 Cyber-attacks by area of CBRNE

| <b>CRBNECy Industry</b> | <b>Applications</b>   | <b>Perceivable Damage</b>  | <b>Possible Airborne Attack Scenarios[6]</b>   |
|-------------------------|---|--|--|
| Chemical                | Chemical production   | Destruction  | Industrial espionage   |
|                         | Logistics Storage   | Area contamination<br>Loss of life industrial                                | ICS controlling chemical delivery  |
| Biological              | Medical facilities  | Destruction  | Espionage  |
|                         | Research facilities   | Area contamination<br>Disease outbreak<br>Loss of life                       | Fake medical details<br>Reputation loss based on false information   |
| Radioactive             | Production  | Destruction  | Espionage  |
|                         | Storage<br>Logistics<br>Decontamination                         | Area contamination<br>Loss of life   | Denial of Service (DOS)  |
| Nuclear                 |   | Destruction  | Espionage  |
|                         | Power production destruction                                    | Area contamination<br>Planet scale disaster<br>Loss of life                  | Destruction<br>Loss of life<br>Terrorism<br>Guerrilla warfare<br>Civil war   |
| Explosives              |   |  | Espionage  |
|                         | Production<br>Logistics<br>Demolitions<br>Excavation<br>Warfare | Destruction<br>Area contamination<br>Terrorism act<br>Loss of life           | Counterespionage<br>Psychological warfare<br>Cyberwarfare<br>Warfare support<br>Electronic warfare synchronization / vector intersection |
| Cyber Domain            |   | Misinformation   |  |
|                         | Cyber command   | False signals<br>Destruction<br>Area contamination<br>Loss of life formation |  |

Source: Modified by the author from (Martinelli, 2017)

### **Drones as Rogue Access Points**

The fourth Cyber-attack vector is particularly interesting (Physical-enabled cyber-attack: physical actions allow remote access to unreachable computer systems or networks (rogue devices or rogue access points or airborne spy). The drone acts as a mobile airborne access point. Cyber techniques that incorporate physical access to internal systems and networks are:

1. Wired network physical access (wiretapping or remote keylogging)
2. Wireless network physical access [long-range antenna's, HAPS, [\[7\]](#) WiFi attack vectors, BYOD) – connecting to the network by the physical proximity of the wireless routing device (Access point or Router)]
3. Insider threat by an employee flying a drone inside the security perimeter. The drone can communicate with other drones or a command post. It may be used as a jump-off station to deploy malware. (Martinelli, 2017)

### **CBRNE Attack Scenarios**

The Norwegian Defense Research Establishment developed the following CBRNE attack scenarios. (Heireng, 2015):

1. Chemical attack in the city center – Explosion and dispersion of Sulphur mustard
2. Chemical transport accident – Train derailment causing chlorine dispersal
3. Radiological dispersal in the city – Radioactive cesium spread in fire
4. Radiological attack on public transportation – hidden radioactive source

5. Nuclear power plant accident – Release of fission products
6. Nuclear submarine accident – Onboard fires
7. Hoax – Unknown powder in the congress center

***It is easy to contemplate how a UAS Team or SWARM could force multiply (WMDD) most of the scenarios above, especially number 7!***

(Martinelli, 2017) provides a palatable set of Cyber-attack scenarios on CBRNE infrastructure. They are listed in Table 15.4. UAS Cyber-attacks can enable or support conventional attacks by enhancing the remote access on Table 15.4 CIS facilities. They can:

1. Provide information about city traffic, mass gatherings, emergency events to plan the attack on the target;
2. Enable false alarms or disable the positive alarms to better control the municipal response during the attack;
3. Trigger remote detonation devices or electronically controlled release valves on chemical tanks. (Martinelli, 2017)

**Table 15.4 Cyber Attack Scenarios by Area in CBRNE**

| AREA        | THREAT   | SCENARIO  |
|-------------|--|---|
| Chemical    | Denial of Service (DoS) and area contamination | DoS in ICS may cause the shutdown, critical malfunction, and/or chemical leakage, contaminating the area inside or outside a facility.  |
| Chemical    | Water supply contamination                     | Tampering with the configuration of the water purification system, endangering consumer lives   |
| Biological  | Public figure setup                            | Medical records of a public figure accessed, edited with compromising values, and widely released to the public as truth  |
| Medical     | Pharmaceuticals formula change biological      | Biological research facility accessed. Critical information is tampered with to divert funds or slow down research  |
| Radioactive | Terrorist attack causing                       | Causing the radiation outbreak with the physical or remote attack, and by accessing the ICS switching off the radiation sensors, prevents it from triggering alarms, thus preventing timely response, and multiplying the damage. |
| Nuclear     | Equipment corruption production                | Production of valuable material is intentionally slowed down nuclear power blackouts  |
| Nuclear     | Power blackout                                 | ICS of the power plant is accessed to disable power distribution  |
| Nuclear     | Meltdown                                       | The critical scenario of disabling the reactor cooling system, causing the meltdown and explosion and eradication.  |

Source: (Martinelli, 2017)

The use of drones to plan CBRNECy attack scenarios is not far afield. A special report by DRONESEC Notify on the Taliban in August 2021 confirms the Taliban's serious interest, operational planning, and aborted attempts. (DRONESEC, 2021)

(Nichols R. R., 2020) and (Nichols R. K., Chapter 18: Cybersecurity Counter Unmanned Aircraft Systems (C-UAS) and Artificial Intelligence, 2022) provide a detailed discussion of SCADA, ICS, and

Cyber-attack taxonomy for threats and countermeasures involving these systems.

### **What Is the Counter**

Picture one hundred plus hostile UASs headed toward a military target, ADS, or CBRN facility with lethal payloads. How do military planners envision defenses against a hostile UAS SWARM attack? The author will concentrate on the ADS side of the equation for defense because if the ADS is disabled, the CBRN facility is low-hanging fruit based on its physical defenses. From our previous discussion, we note that CBRN facilities can be attacked from the air using UAS and leveraging cyber technologies.

The risk of successful terrorist attacks on U.S. Air Defense Systems (ADS) or CBRN facilities by hostile UASs increases by improving commercial capabilities and accessibility. Advanced small drones, capable of carrying sophisticated imaging equipment and significant payloads, are readily available to the public. A range of terrorist, insurgent, criminal, corporate, and activist threat groups have demonstrated their ability to use civilian drones and gather intelligence. How does the country defend against a growing UAS threat? *This is known as the Counter-UAS Problem.* General James D. Mattis, SECDEF (U.S. Secretary of Defense), summed up the problem succinctly:

“Unmanned Aircraft are being developed with more technological systems and capabilities. They can duplicate some of the capabilities of manned aircraft for both surveillance/reconnaissance and attack missions. They can be small enough and/or slow enough to elude detection by standard early warning sensor systems and could pose a formidable threat to friendly forces.” (Chairman, 2012)

### **Operational Protection from Hostile UAS Attacks – A Helicopter View**

According to LCDR Boutros of the Navy War College, developing technologies do not paint a pleasant picture of the Counter-UAS problem (Boutros, Operational Protection 2015). UAS has seen a widespread proliferation among both state and non-state actors. This is cause for concern to U.S. Operational Commanders. (Boutros, 2015). General James D. Mattis, SECDEF, concluded:

“The proliferation of low cost, tactical unmanned aerial systems demands we think about this potential threat now... we must understand the threat these systems present to our joint force and develop the tactics, techniques, and procedures to counter the problem.” (Chairman, 2012) (Myer, 2013)

It can be argued from the quantity and diversity of products that China is the current leader in this technology, and China is thoroughly exercising its UAS capabilities in the Spratly Islands (Nichols, Mumm, Lonstein, Ryan, & and Carter, 2018). However, more than 90 countries and non-state actors have UAS technology and foster terrorism. “Most of the UAS systems, except for China, Russia, USA, Turkey, Saudi Arabia, and Iran inventories are low-technology, Intelligence, Surveillance, and Reconnaissance (ISR) platforms” (Boutros, 2015). Experts believe that by 2025 China will produce over 50% of UAS systems (Yan, 2017). Yan predicts that China’s commercial drone market will top USD 9B in 2020 (Yan, 2017). The market value will triple to 180 billion yuan by 2025, according to the guidelines from the Chinese Ministry of Industry and Information Technology. This estimate is much higher than a forecast by an iResearch report last year (iResearch, 2016), which said that the overall market of UAVs, commonly known as drones, could reach 75 billion yuan by 2025 in China (Yan, 2017).

Iran has supplied long-range, low technology Ababil UAS weapons systems to Syria and Sudan and extremist groups like Hezbollah, Hamas, and ISIS. Hezbollah’s inventory is estimated at over 200 UAS, which concerns the Israeli military commanders (Zwijnwenburg, 2014).



The DOD's 2018 Joint Publication (J.P.) 3-01 "Countering Air and Missile Threats" identifies friendly assets that an adversary may attack during a campaign using UAS. A theater commander must plan counter-UAS actions against air defense sites, logistics centers, and critical national infrastructure (Boutros, 2015). "Due to their small size and unique flying signatures, many UAS are difficult to detect, identify, track, and engage with current joint air defense systems. The increasing proliferation of global UAS has exposed a critical vulnerability in the protection function of operational commanders, requiring joint efforts to include intelligence, electronic warfare (EW), cyber warfare (CW), and FIRES (the use of weapons systems to create a specific lethal or non-lethal effect on a target)" (Boutros, 2015). But UAS are not invincible. Neutralizing threats or mitigating risk includes active and passive defense methods with kinetic and non-kinetic FIRES.[8] (DoD, J.P. 3-0 Joint Operations, 2018).

### **Countering UAS Air Threats**

Advanced UAS can carry large payloads at great distances. U.S. Predator and Global Hawk UAS, "Chinese Pterodactyl and Soar Dragon counterparts, and Iranian Ababil can carry at least 500 Kg payloads greater than 300 km" (Boutros, 2015). "They can be armed or unarmed, with ISR payloads, communications relays, Over-The-Horizon (OTH) target acquisition, and precision strike capabilities" (Boutros, 2015).

"Shorter range, tactical, small/micro UAS may not have the distance or payload capacity of more advanced systems, but they can seriously impact a campaign (or U.S. Homeland Defense). Because of their size, their heat signatures are almost nonexistent and easily evade detection. They offer more freedom of action. They can be launched from within U.S. air defense zones and fly to their targets in less time than it takes for a coordinated response" (Boutros, 2015). [Nightmare alert: Imagine a swarm of UAS carrying small, potent binary bomb payloads attacking a U.S. carrier at port

less than one mile away from the UAS launch point.] The enemy can effectively balance space, time, force, and arguably frequency. (Beaudoin, 2011). “Small UAS (sUAS) can perform short-range ISR, be outfitted with explosive charges or chemical and biological agents for aerial dispersion, or simply fly over troops or civilians to demoralize” (Boutros, 2015). Given the effectiveness of enemy use of IEDs in Iraq and Afghanistan, a mobile, airborne version would take the problem to an entirely new level! (Nichols R.-O. , 2016).

### **Vulnerabilities Perspective**

sUAS are vulnerable to kinetic and non-kinetic outside influence in four different areas: their link to a ground station, the ground station itself, the aircraft’s various sensors, and cyber weapons. The military recognizes the first three factors; the authors will concentrate on the fourth.

“In 2009, Iraqi insurgents successfully hacked into U.S. Reaper drones, crashing them.” (Boutros, 2015) (Horowitz, 2014). “In September of 2011, ground control stations at Creech AFB were infected by a virus, temporarily grounding the entire UAS fleet.” (Boutros, 2015) (Hartman, 2013). UAS onboard sensors can be manipulated in many ways. “High-intensity light directed at an optical sensor can blind it. GPS receivers can be cyber-spoofed, transmitting a stronger, but false GPS signal to a receiver, resulting in inaccurate navigation. Influencing the local magnetic field can adversely affect both onboard hard drives. Would it be best to call them a processor/chipset/ or form factor? and sensors that require magnetic orientation to operate correctly.” (Boutros, 2015) (Hartman, 2013).

The attacker’s objective is to understand better UAS subsystems, which facilitates exploiting their weaknesses. The author contends that the hostile technology of remote-controlled warfare is difficult to control or abort; the best defense (counter-UAS) is to address the root drivers of these threats. Cyber offensive weapons against UAS

SAA and SCADA targets (Nichols, Mumm, Lonstein, Ryan, & Carter, 2018).

### **Conventional Vulnerabilities of Air Defense Systems (ADS), Attacks By sUAS, and Countermeasures**

A simplified, non-classified view of the U.S. Air Defense System (ADS) against a hostile UAS attack occurs in two stages: [\[9\]](#)

1. Early Detection and Identification of “Danger Close” (Myer, 2013) [\[10\]](#)
2. We have applied appropriate countermeasures with the secondary goal of restricting collateral damage.

The traditional ADS family of tools for detection include:

1. Active Radar Surveillance – generate waves and use rebound echoes from the UAS to locate and estimate distance, approach speed, size, penetration vector, and short-term trajectory.
2. Passive Monitoring – cover the electromagnetic spectrum of visible, thermal infrared, and radio waves on common communications channels.

When considering hostile UAS defense, planners need to consider several issues. The U.S. ADS is optimized for missiles and aircraft deployed at high altitudes and speeds. ADS data fusion (detection, identification, weapon lock-on, execute countermeasures) works better with larger targets, not very small ones like UAS/sUAS. The U.S. ADS is effectively reactive for longer ranges; close reactive engagements, such as sUAS /UAS, are sub-optimal. (Nichols R.-O. , 2016).

There are clear vulnerabilities of the U.S. ADS to UAS:

- sUAS can be launched into action close to the target(s), less than 1 mile.
- sUAS exhibit a small radar signature, which hinders the detection phase.
- Reactive action dictates a quick response near the target. This is not always possible.
- sUAS/UAS are designed for slow, low flight. Low flying sUAS avoid radar identification.
- sUAS/UAS electric motors are quiet and have a limited thermal signature. This makes for difficult noise detection, especially if stealth technologies have been employed. (Nichols, Mumm, Lonstein, Ryan, & and Carter, 2018)
- sUAS /UAS operates in urban areas. The urban sphere presents additional problems and potential collateral damage. (Nichols R.-O. , 2016)

### ***Conventional Countermeasures Against sUAS / UAS***

Two families of conventional countermeasures are used to disrupt and destroy hostile UAS/sUAS systems. (Excluding FAA Regulations, locked in firmware GPS No-Fly Zones, Registration, FAA rules and the like)

### ***Active Measures***

Active measures are designed to incapacitate and/or directly destroy the sUAS/UAS threat. This method may employ Ground-to-Air Defense (GTA), missiles, acoustical guns, or a simple cyber rifle.

However, there are some defensive issues to be considered:

- GTA efficiency against sUAS reactive targets is reduced and is even less efficient in urban zones where civilians are at risk.
- Simultaneous attacks on multiple fronts (See: Team or SWARM formats, Table 15.2) make countermeasures very difficult to apply, and defense measures are mitigated,

- Commercial company Liteye has developed an Anti-UAV Defense System (AUDS), which can detect, track, and disrupt sUAS operations using pulsed, brief focused broadcasts of directional frequency jamming. Liteye has also developed a mobile version called M-AUDS (Liteye, 2018).
- China has developed a “5-sec” laser weapon to shoot down sUAS at low altitude (500 m) with a 10KW high-energy laser beam. Its range is 1.2 mi and handles sUAS at speeds up to 112 mph (Nichols R.-O. , 2016).

UAS countermeasure research is improving. Latency via AI has been greatly reduced. The goal is to increase the ability of Ground-to-Air (GTA) to react and improve their capabilities to a defined saturation limit. Team formation allows decoys and shields. SWARM formation is easier to detect; the arrival of a cloud of robot drones is hard to mask but tough to neutralize.

### **Passive Measures**

Passive measures are designed to use physical protection around the target to protect it indirectly. Some methods used are decoys, shields, organized roadblocks, nets, jamming the aggressor’s sensors, or total or partial GPS signal cyber-spoofing. Passive countermeasures have some positive outcomes. Decoys can be effective if the ADS knows which sensors are employed for an sUAS Kamikaze attack and how they are used in the SAA subsystem. Communication jamming, which can disrupt the inter-drone communications required for the team or swarm formations, is effective against level 1 and 2 drones (Table 15.1), which require pilot interaction. Sensor Jamming is effective regardless of automation. It is especially effective when false GPS signals give false GPS information, cause camera/gimbal dislocation, and demagnetize the heading sensor (Nichols, Mumm, Lonstein, Ryan, & Carter, 2018).

The 2011 Iranian incident taught the U.S. ADS planners some

lessons about passive spoofing waypoints and Loss of Signal (LOS) via GPS. LOS is an emergency condition that causes sUAS/UAS to execute programmed responses. One of those responses may be “return to waypoint .”Two types of spoofs can be executed. A complete spoof uses the friendly SAA to estimate course, groundspeed, and time to target, then force a LOS and change the final waypoint. A partial spoof reports false positions and changes waypoints for perceived emergency conditions during LOS. Both spoofs are difficult to detect and effective (Editor, 2012).

### **Conclusions**

Unmanned Aircraft Systems represent some of the most advanced U.S. air assets. They are critical to the USA ADS and the defense of CBRN facilities. Based on the sheer diversity and number of potential cyber weapons that can be deployed at every stage of the UAS mission and the significant growth of UAS for defense purposes, the risk of their hostile use against U.S. ADS or CBRN facilities is steadily increasing. Coupled with the huge growth and increased sophistication of the UAS commercial technologies, the threat of hostile use cannot be minimized. (Nichols R. K. et al., 2019) (Nichols R. K. et al., Counter Unmanned Aircraft Systems Technologies, and Operations, 2020)

### **Discussion Topics**

Consider the following real case scenario and theory about U.S. Navy Vessel Collisions in the Pacific:

Given Facts:

In 2017, a chain of incidents/collisions involved four U.S. Warships and one U.S. Submarine. On August 20, the guided-missile destroyer USS John S McCain collided with the 600-foot oil and chemical tanker Alnic MC at 0624 JST. Ten sailors died. On June 17, the destroyer USS Fitzgerald collided with the ACX 30,000-ton container ship at 1330 JST, leaving seven dead. Records show that the ACX turned sharply right at the time of the collision. The route of the destroyer is not shown on maps because commercial tracking

data does not include military ships. Damage to the starboard side of the USS Fitzgerald indicates it would have been on a bearing of approximately 180 deg. (South). *The captain of the Philippine-flagged container ship accused the Navy destroyer of failing to heed warning signs before the crash.* On May 9, the guided-missile cruiser USS Lake Champlain collided with a South Korean fishing boat off the Korean Peninsula. There were no injuries. On January 31, the guided-missile cruiser USS Antietam ran aground, dumping more than 1000 gallons of oil into Tokyo Bay. On August 18, the ballistic-missile submarine USS Louisiana collided with the Navy Offshore Support Vessel in the Strait of Juan de Fuca. No injuries. (Office of CNO, 2020) (Lagrone, Chain of Incidents Involving U.S. Navy Warships in the Western Pacific Raise Readiness, Training Questions, 2017)

### **U.S. Navy Official Response**

The U.S. Navy blamed its field leadership for not responding appropriately in all five incidents. Court marshals and relief from duty are the punishments of the day. The Navy blames funding, lack of readiness, and lack of training. Investigations and maintenance “hold” has been initiated. Reading between the lines, this response would imply that the Skipper/XO/COB and at least five watch sailors on each Naval vessel (roughly –forty to fifty personnel including bridge staff) were judged incompetent. Many U.S. Navy careers were finished. Further, this would also imply that all five vessels’ radar, emergency positioning alert systems, AIS, sonar, and long-range collision avoidance equipment must have been functioning perfectly, without a catastrophic failure or interference of any kind. (Office of CNO, 2020)

### **The Case for a Cyber Weapon**

There appears to be valid evidence to support the theory that at least two of the U.S. Navy Warships above and the commercial vessels they struck were on the wrong end of a hostile cyber-weapon. (Lagrone, Cyber Probes to be Part of All Future Navy

Mishap Investigations After USS John S. McCain Collision, 2017) They were receiving the wrong GPS-generated positional information (GPS Spoofing). **Our research theorizes that UAS may have deployed the Cyber Weapon off a small, nearby vessel by an adversary.** The subject cyber weapon may be an advanced modular entity that can spoof the GPS signals received by all vessels in its range. Vessels given misleading data will make incorrect decisions in terms of navigation and emergency responses – potentially leading to collisions and deaths. Contemplate and comment on the viability of the researcher's cyber-weapon theory. Research and choose one specific cyber threat / or cyberweapon deployed against SCADA systems used by UAS. Discuss the chosen SCADA threat and how it exploits the vulnerabilities of the target system, the implications (impact) of the attack, and what defenses and countermeasures might be used to defend or mitigate the threat to the target.

### **Bibliography**

A.A. Zavala, J. R. (2008). *High-Altitude Platforms for Wireless Communications*. West Sussex, UK: John Wiley.

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

Boutros, D. (2015, May 15). U.S. Navy War College. Retrieved from Operational Protection from Unmanned Aerial Systems: <http://www.dtic.mil/dtic/tr/fulltext/u2/a621067.pdf>

Chairman, U. (2012, March 23). Countering Air and Missile Threats, final coordination, J.P. 3-01. CJCS.

CIO Staff. (2006, November 1). *Pa. Water-System Network Hacked*. Retrieved from <https://www.cio.com/>: <https://www.cio.com/article/262869/it-strategy-pa-water-system-network-hacked.html>

Dark Reading Staff. (2013, April 22). *Poison Ivy Trojan Just Won't Die*. Retrieved from <https://www.darkreading.com/>: <https://www.darkreading.com/attacks-breaches/poison-ivy-trojan-just-won-t-die>



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

DoD. (2018). J.P. 3-0 *Joint Operations*. Washington, DC: DoD.

DRONESEC. (2021). *Taliban UAS Threat Actor Special Report*. Melbourne, AU: DRONESEC Notify (Dronsec.com).

Editor. (2012, April 22). R.T. *Question More*. Retrieved from Iran starts cloning of American spy drone: <https://www.rt.com/news/iran-spy-drone-copy-667/>

Gasser, M. (1988). *Building a Secure Computer System*. New York City: Van Nostrand Reinhold.

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

Heireng, H. S. (2015). *The development and use of CBRN Scenarios for Emergency Preparedness Analysis*. FOI Research Institute, Norwegian Armed Forces.

Higgins, K. J. (2015, January 23). *Banking Trojans Disguised As ICS/SCADA Software Infecting Plants*. Retrieved from <https://www.eetimes.com/>: <https://www.eetimes.com/banking-trojans-disguised-as-ics-scada-software-infecting-plants/#>

Horowitz, M. C. (2014). *Droning On Explaining the Proliferation of Unmanned Aerial Vehicles*. The University of Pennsylvania and Texas A&M Universities. The University of Pennsylvania and Texas A&M Universities.

iResearch. (2016, June 21). *iResearch Forecasts China's Civilian Small Drone Trend*. Retrieved from iResearch: [http://www.iresearchchina.com/content/details7\\_23815.html](http://www.iresearchchina.com/content/details7_23815.html)

Jaffe, G., & Erdbrink, T. (2011, December 5). Iran says it downed U.S. stealth drone; Pentagon acknowledges aircraft downing. *The Washington Post*.

Johnson, J. (2022, July 22). *The number of Ransomware attacks per year 2016-2020*. Retrieved from [www.statista.com](http://www.statista.com): [www.statista.com](http://www.statista.com)

Lagrone, S. (2017, August 21). *Chain of Incidents Involving U.S. Navy Warships in the Western Pacific Raise Readiness, Training Questions*.

Retrieved from news.usni.org/2017: <https://news.usni.org/2017/08/21/chain-incidents-involving-u-s-navy-warships-western-pacific-raise-readiness-training-questions>

Lagrone, S. (2017, September 14). *Cyber Probes to be Part of All Future Navy Mishap Investigations After USS John S. McCain Collision*. Retrieved from <https://news.usni.org:https://news.usni.org/2017/09/14/cyber-probes-part-future-navy-mishap-investigations-uss-john-s-mccain-collision>

Liteye. (2018, August 25). AUDS. Retrieved from Liteye Corporation: <http://liteye.com/products/counter-uas/auds/>

Martinelli, S. A. (2017). Selected Issues of Cyber Security Practices in CBRNECy Critical Infrastructure. In M. & Malizia, *Cyber and Chemical, Biological, Radiological, Nuclear, Explosives Challenges* (pp. 11-34). Rome: Springer International.

Miller, C. (2022, January 22). *throwback Attack: BlackEnergy attacks the Ukrainian power grid*. Retrieved from <https://www.industrialcybersecuritypulse.com/:https://www.industrialcybersecuritypulse.com/throwback-attack-blackenergy-attacks-the-ukrainian-power-grid/>

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

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

Nichols, R. K. (2008, September 5). Counterintelligence & Sensitive Compartmented Information Facility. (SCIF) Needs – Talking Points.

Nichols, R. K. (2017, October 4). *Drone Wars: Threats, Vulnerabilities and Hostile Use of UAS*. 2nd Annual Cyber Forum Event. Wichita, KS, USA: Wichita State University.

Nichols, R. K. (2019, March 14). *Hardening U.S. Unmanned Systems Against Enemy Counter Measures*. Invited Speaker / Panelist (13-14 March 2019) 7th Annual DoD UAV Countermeasures Summit (p. Hardening USA Unmanned Systems Against Enemy

Countermeasures). Alexandria, VA: Proceedings of 7th Annual UAV Countermeasures DoD Summit.

Nichols, R. K. (2021). Chapter 14: Maritime Cybersecurity. In R. K. Nichols, & J. J. Ryan, *Unmanned Vehicle Systems & Operations on Air, Sea, Land* (pp. 330-356). Manhattan, KS: New Prairie Press #35.

Nichols, R. K. (2022). Chapter 18: Cybersecurity Counter Unmanned Aircraft Systems (C-UAS) and Artificial Intelligence. In D. M. R. K. Barnhart, *Introduction to Unmanned Aircraft Systems, 3rd Edition* (pp. 399-440). Boca Raton, FL: CRC.

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

Nichols, R. K., Ryan, J., Mumm, H., Lonstein, W., Carter, C., & Hood, J. (2020). *Counter Unmanned Aircraft Systems Technologies and Operations*. Manhattan, KS: Pressbooks: <https://kstatelibraries.pressbooks.pub/counterunmannedaircraft/>.

Nichols, R. K., Ryan, J., Mumm, H., Lonstein, W., Carter, C., & Hood, J. P. (2018). *Unmanned Aircraft Systems (UAS) in Cyber Domain: Protecting USA's Advanced Aircraft Assets*. Manhattan, KS: New Prairie Press (NPP) Ebooks. Retrieved from <https://newprairiepress.org/ebooks/21>

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. R. (2020). *Counter Unmanned Aircraft Systems Technologies and Operations*. Manhattan: New Prairie Press #31.

Nichols, R.-O. (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 the author or in CANVAS. Memphis, TN, USA: INFOWARCON16.

Office of CNO, U. N. (2020, May 14). *Collision Reports for USS Fitzgerald and USS John S McCain 2017 Incidents in Pacific*. Retrieved from <https://s3.amazonaws.com/CHINFO:https://s3.amazonaws.com/CHINFO/USS+Fitzgerald+and+USS+John+S+McCain+Collision+Reports.pdf>

Paske, E. L. (2015). *Cybersecurity of Industrial Control Systems. Global Conference on Cyberspace*.

Peerenboom, F. a. (2001). *CIS Shared Threats*. Retrieved from <http://www.ari.vt.edu/>: <http://www.ari.vt.edu/workshop/Whitfield-presentation.ppt>

Poulsen, K. (2003, August 20). *Slammer Worm Crashed Ohio Nuke Plant Network*. Retrieved from <https://rense.com/:https://rense.com/general40/worm.htm>

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

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

Richard K. Barnhart, S. B. (2012). *Introduction to Unmanned Aircraft Systems*. Boca Raton, FL: CRC Press.

Schneier on Security. (2008, 01). *Hacking Polish Trams*. Retrieved from <https://www.schneier.com/>: [https://www.schneier.com/blog/archives/2008/01/hacking\\_the\\_pol.html](https://www.schneier.com/blog/archives/2008/01/hacking_the_pol.html)

Schneier, B. (2015). Vizsec 2015. *IEEE 12th Symposium on Visualization for Cyber Security*. IEEE.

Staff. (2014, April 28). *Infosecurity Europe 2014 Case Study: Shamoon, a two-stage targeted attack*. Retrieved from <https://www.slideshare.net/>: <https://www.slideshare.net/Seculert/case-study-shamoon-a-two-stage-targeted-attack>

Staff, I. (2013). *IEEE Communications Surveys & Tutorials: Introduction to Industrial Control Networks*. IEEE.

Technopedia. (2019, May 28). *Technopedia*. Retrieved from Artificial Intelligence: <https://www.techopedia.com/definition/190/artificial-intelligence-ai>

Wilson, C. (2014). *Cyberterrorism: Understanding, Assessment, and Response*. Wales: Swansea University.

Yan. (2017, December 23). *China's commercial drone market to top 9 bln USD by 2020*. Retrieved from Xinhuanet: [http://www.xinhuanet.com/english/2017-12/23/c\\_136847826.htm](http://www.xinhuanet.com/english/2017-12/23/c_136847826.htm)

Zwijnwenburg, W. (2014, October 8). *ZwijnwenbDrone-tocracy? Mapping the Proliferation of Unmanned Systems*. Retrieved from Sustainable Security.org.

## Endnotes

[1] **CRITICAL INFRASTRUCTURE (CI)** is the production, storage, logistics of CBRN materials and devices, and reconnaissance and disaster response. CBRNE Infrastructure is CI that produces, handles, transports recycles, decontaminates, or otherwise incorporates CBRNE agents. (Paske, 2015) (Martinelli, 2017)

[2] None of the CIS cyber attacks have been deployed via drone. But that is the whole point they can be, and it would be more effective to do so!

[3] Sources described it as a worm or malware. Nothing could be further from the truth. It was a joint Israeli – USA operation creating

a powerful Cyber Weapon involving multiple attack surfaces, counter defenses, zero-day exploits, false flags, etc. The development was both sensitive and compartmentalized and carried out in several locations. The only two drawbacks were it was discovered and then re-engineered to hit additional targets.

[4] Artificial intelligence (AI) is an area of computer science that emphasizes the creation of intelligent machines that work and react like humans. Some of the activities computers with artificial intelligence are designed for include:

Speech recognition, learning, planning, problem-solving, and decision-making. Research associated with artificial intelligence is highly technical and specialized. The core problems of artificial intelligence include programming computers for certain traits such as knowledge, reasoning, problem-solving, perception, learning, planning, and

the ability to manipulate and move objects. (Technopedia, 2019)

[4] Dr. Julie J.C.H. Ryan is a superstar in the INFOSEC community. Her research is prolific. See <https://www2.seas.gwu.edu/~jjchryan/research.html>. So is Dr. Dan J. Ryan. See: <https://security.iri.isu.edu/ViewPage.aspx?id=926&rebuild=true>

[5] Some Level 3 UASs have capabilities that fall into the Level 4 category. Datasheets do not necessarily follow neatly into the author's taxonomy.

[6] Adapted for UAS deployment from Table 1, Chapter 2, page 21 (Martinelli, 2017)

[7] Consider HAPP applications using High Altitude Drones. (A.A. Zavala, 2008)

[8] **FIRES** definition (U.S. DoD – J.P. 3-0) is the use of weapon systems to create a specific lethal or nonlethal effect on a target. (DoD, Dictionary of Military Terms, 2018)

[9] ADS is emphasized because CBRN facilities are low-hanging fruit if these defenses fail.

[10] Danger Close Definition [www.benning.army.mil/infantry/magazine/issues/2013/May-June/Myer.html](http://www.benning.army.mil/infantry/magazine/issues/2013/May-June/Myer.html) November 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 P.I. is used to define **danger close** for aircraft delivery. **Pi** = Probability of incapacitation.

2) **Definition of “danger close”** (U.S. 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 the fire which indicates that friendly forces are within **close** proximity of the target.





PART III

# SECTION 3 RISK ASSESSMENT AND POLICY CONSIDERATIONS



# 16. Assessing the Drone Delivery Future WMDD and DEW Threats/Risks

**By Dr. Hans C. Mumm & Wayne D. Lonstein, Esq.**

## **STUDENT LEARNING OBJECTIVES**

The student will gain knowledge of the concepts and framework related to the future uses and misuses of autonomous systems in the Weapons of Mass Destruction (WMD), Directed Energy Weapons (DEW), and cyber weapons. This will include multiple autonomous systems attack vectors, legal ramifications, air space/freedom of movement considerations, and assessment recommendations for a safe and secure future.

The student will review the legal considerations and consequences regarding artificial intelligence in WMD/DEW applications. The student will appreciate the potential legal consequences when the autonomous systems are deployed thousands of miles away from the operator.

## **A LOOK BACK AT THE TRADITIONAL DELIVERY SYSTEMS**

CBNRE weapons can be delivered “via various mechanisms including but not limited to; ballistic missiles, air-dropped gravity bombs, rockets, artillery shells, aerosol canisters, land mines, and mortars” (Kimball, 2020). This list is based on warfare in the pre-pandemic years, as it is now clear that biological weapons can be delivered through means different than traditional warfare. The speed of commerce, travel, and cultures around the world proved a model of how quickly biological agents can spread and negatively affect the entire plant.

UAS platforms are ideal for dispersing chemical agents. “Like cruise missiles, UAVs are ideal platforms for slower dissemination due to controllable speeds and dispersal over a wide area. UAVs can fly below radar detection and change directions, allowing them to be retargeted during flight” (Kimball, 2020).

The Islamic State (I.S.) has worked to create “inventive and spectacular ways of killing people has long been a hallmark of Islamic State’s modus operandi. The use of mustard gas and chlorine against Kurdish Peshmerga fighters is well documented, as is research by I.S. to develop radiological dispersion devices” (Dunn, 2021).

### **STACK INTEGRATION-EMERGING TECHNOLOGIES OFFERS NEW TACTICS, TECHNIQUES, AND PROCEDURES (TTPS)**

The integration and cooperation of the seven recognized autonomous systems (UAS, UGV, UUV, USV, humanoid, cyber, and exoskeleton) would forever change the landscape of our world. Introducing the soon-to-be-eighth autonomous system “nanobiologics” will inject complexity into this discussion that humankind may not be ready to confront. The worldwide

“healthcare market will fuel human/machine enhancement technologies primarily to

augment the loss of functionality from injury or disease, and defense applications will

likely not drive the market...the gradual introduction of beneficial restorative cyborg

technologies will, to an extent, acclimatize the population to their use.” (Emanuel, 2019)

This change will be difficult for most cultures to embrace as “Societal apprehension following

the introduction of new technologies can lead to unanticipated political barriers and slow

domestic adoption, irrespective of value or realistic risk” (Emanuel, 2019).

The changing nature of the autonomous systems space, from

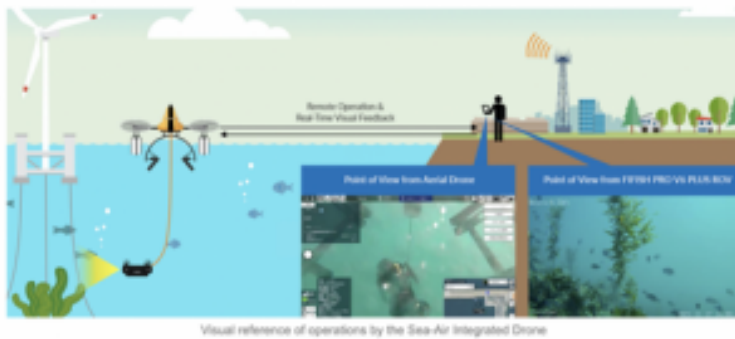
remote-controlled toy airplanes to drones to military UAVs, is now about to be upended yet again as the industry starts creating hybrid multi-purpose systems. These “drones are now capable of moving from a wheeled system to an airborne system. Other drones are capable of moving from subsurface (underwater) to airborne modality” (Pledger, 2021). An example of this is “QYSEA, KDDI, and PRODRONE have teamed up to create the World’s first sea-to-air drone” (Allard, 2022).

**Figure 16.1: Picture of a Sea-Air Integrated Drone**



Source: (Allard, 2022)

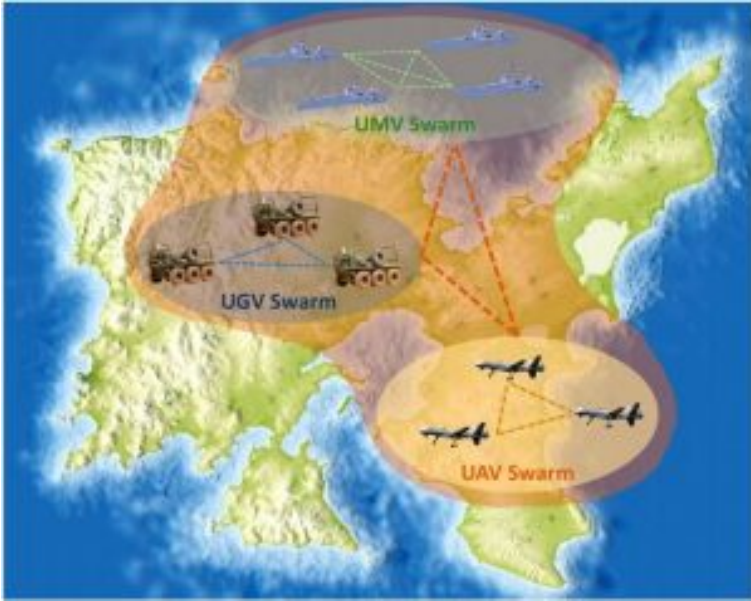
**Figure 16.2: Diagram showing communications between the sea-air drone and remote operator**



Source: (Allard, 2022)

Integrating all autonomous systems will move the industry from a single point of use system to a cooperative goal-oriented artificial ecosystem. The swarm concept will move from a single system type swarming with their kind to the ability to mix with different types of autonomous systems to swarm and goal seek, allowing some to be destroyed for the group's overall goal.

**Figure 16.3: Illustration of UUVs, UGVs, and UAVs swarms working together**



Source: (Stolfi, 2021)

As the world has become more dangerous, new capabilities must be developed to counter the violence and evil that is becoming too prevalent. With the National Defense University in Washington, D.C., Harry Wingo worked on a counter-sniper, counteractive shooter system.

“a collaborative design (“co-design”) approach to accelerating public and political acceptance of the cyberspace and information risks, inherent to the development and deployment of indoor smart building unmanned aircraft systems (UAS) to provide immediate “visual access” to law enforcement and other armed first responders in the case of an active shooter incident inside of a building, including risks concerning (1) system safety and reliability; (2) supply chain security; (3) cybersecurity; and (4) privacy. The paper explores the potential to use a virtual world platform as part of a phased pilot

at the U.S. Service Academies to build trust in the privacy, security, and efficacy of a counteractive shooter UAS (Wingo, 2020).

### **Assessment of Emerging Threats of Mini-WMD**

The threat of mini-WMD grows as circuits get smaller, cheaper, and faster. The ability for anyone to buy parts from the internet and gain the knowledge to assemble such a system by watching a YouTube video is only accelerating. Terrorist groups have adapted commercial drones for their own use, “including intelligence collection, explosive delivery (either by dropping explosives like a bomb, the vehicle operating as the impactor, or the drone having an equipped rocket-launching system of some type) and chemical weapon delivery” (Pledger, 2021). The array of chemical and biological material that can easily be obtained, weaponized if required, and then assembled into a weapon for disbursement and use is only keystrokes away and sometimes as close as the nearest superstore.

Terrorists do not need to acquire exotic chemical weapons to be effective “even gasoline spread like a vapor when ignited has 15 times the explosive energy of the equivalent weight of TNT. Moreover, even if the gasoline were ignited, its effect on a crowd would be devastating” (Dunn, 2021).

The challenge of dealing with these issues is becoming more difficult as terrorist groups continue to ramp up their technical know-how and put this knowledge to use. Consider,

Once Pandora’s box was opened, bad actors adapted quickly and used drones to plan and conduct attacks. Between 1994 and 2018, more than 14 planned or attempted terrorist attacks took place using aerial drones. Some of these were:

- in 1994, Aum Shinrikyo attempted to use a remote-controlled helicopter to spray sarin gas, but tests failed as the helicopter crashed;
- in 2013, a planned attack by Al-Qaeda in Pakistan using multiple drones was stopped by local law enforcement;



- in 2014, the Islamic State began using commercial off-the-shelf and homemade aerial drones at scale during military operations in Iraq and Syria;
- in August 2018, two GPS-guided drones, laden with explosives, were used in a failed attempt to assassinate Venezuelan President Maduro; and,
- in January 2018, a swarm of 13 homemade aerial drones attacked two Russian military bases in Syria (Pledger, 2021).

The U.S. military incorporates and integrates mini-systems, including the FLIR Black Hornet PRS illustrated in Figure 16.4. This mini-UAV enables a soldier to have situational awareness without being detected. The Black Hornet PRS has electrical optical (E.O.) and infrared (I.R.) capabilities like larger UAVs and can provide the same reconnaissance as UGVs. The FLIR Black Hornet PRS provides the “Game-changing E.O. and I.R. technology [that] bridges the gap between aerial and ground-based sensors, providing the same amount of S.A. as a larger UAV and threat location capabilities of UGVs” (FLIR, 2022)

**Figure 16.4: Image of a soldier and a Black Hornet UAV**



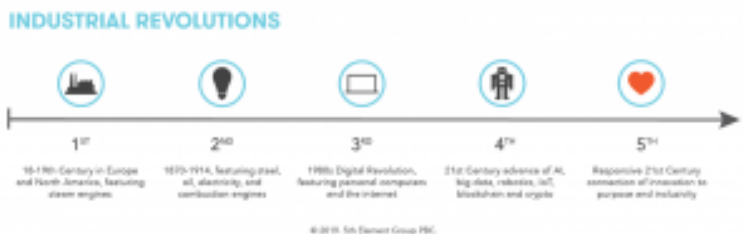
Source: (FLIR, 2022)

The PRS is reported to be nearly silent, with a flight time of up to 25 minutes. The mission of these mini drones is expanding as sensor systems come online and the military discovers new ways to employ the technology.

Does the World Have an Answer to These Emerging Threats?

The fourth industrial revolution, which we are currently experiencing, encompasses “disruptive technologies and trends such as the Internet of Things (IoT), robotics, virtual reality (V.R.) and artificial intelligence (A.I.) are changing the way we live and work. In the Fifth Industrial Revolution, humans and machines will dance together, metaphorically” (Gauri, 2019)

### **Figure 16.5: Timeline of Industrial Revolutions**



Source: (Gauri, 2019)

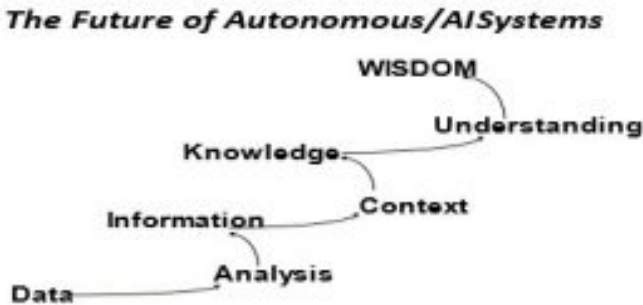
The fourth industrial revolution allows innovation to flourish and humans to do more with less. Yet, the emerging threats that this revolution is creating are seemingly ignored as the world continues to run headlong toward the fifth industrial revolution. The cyber threat in the A.I. and IoT industries is cause for pause. The caution does not even begin to encompass the evolution of quantum computing that the world is racing towards with little security, ethics, or understanding of this technology and how it will transform humanity. Quantum computing will change how our “national security institutions conduct their way of business in all its forms and functions. Data protection, risk modeling, portfolio management, robotic process automation, digital labor, natural language processing, machine learning, auditing in the cloud, blockchain, quantum computing, and deep learning may look very different in a post-quantum world” (Mumm, 2022). Consider that in 2022, the human brain is being connected to machines, machines that can control all layers of autonomous systems, including swarms of different autonomous systems that can goal seek, adjust on the fly, and evolve within the architecture more it is used. This is exciting; however, it may not make for a safer world.

The development of direct neural enhancements of the human brain for two-way data transfer would create a revolutionary advancement in future military capabilities. This technology is

predicted to facilitate read/write capability between humans and machines and between humans through brain-to-brain interactions. These interactions would allow warfighters direct communication with unmanned and autonomous systems and other humans to optimize command and control systems and operations. (Emanuel, 2019)

What the technology world is hoping to bring to humanity is wisdom, not simply the ability to send data, humanity is seeking wisdom, and it is this wisdom that will allow the fourth and fifth industrial revolutions to enhance humankind, and with guidance and care, allow a more peaceful world to emerge.

**Figure 16.6: Future capabilities of autonomous/A.I. systems**



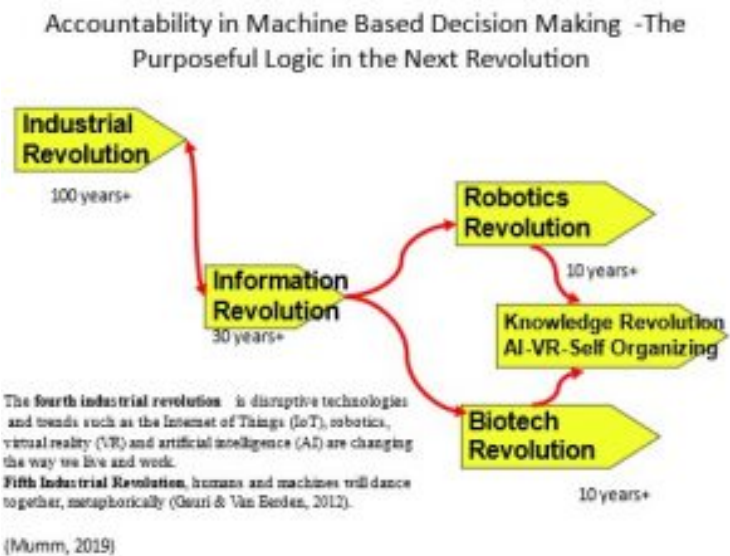
Source: (Mumm, 2022)

History has taught humanity that the world must have accountability throughout these industrial revolutions. This becomes an even greater burden in the fifth industrial revolution as “The threat of unchecked technology and the ability to weaponize

quantum computing continue to evolve. Technology flourishes as free markets expand. Quantum computers will be the next productivity accelerator expanding the market’s breadth and depth”.

(Mumm, 2022)

**Figure 16.7: Image of the Industrial Revolution and the next revolution**



Source: (Mumm, 2022)

The world does have an answer to future emerging threats; however, history has repeatedly shown that the will of humanity to solve future threats is low, if not non-existent. The threat of

autonomous systems combined with the CBNRE and escalating cyber security issues have all been briefed to the world leaders. Industry and government should support the continued work to

establish a whole-of-nation approach to human/machine enhancement technologies versus a whole-of-government approach. Federal and commercial investments in these areas are uncoordinated. They are being outpaced by Chinese research and development efforts, which could result in a loss of U.S. dominance in human/machine enhancement technologies. (Emanuel, 2019)

These discussions have occurred over decades in academic, military, and political arenas. Yet, the technology continues to move forward, mostly unchecked, with few laws, policies, governance, or even agreements on how these threats should be curtailed. Consider the cultural struggle around the world today and how technology can bring us all together as the “fifth revolution will create a new socio-economic era that closes historic gaps in last-mile inclusion and engages the “bottom billion” in creating quantum leaps for humanity and a better planet. (Gauri, 2019) Humanity struggles even to define the ethical parameters of technology and its implementations, forget about what happens when multiple technologies such as autonomous systems begin to communicate, and goal seek together and what secondary and tertiary effects this is going to cause. Sadly, all too often, a community will install a stop sign at a dangerous intersection after someone gets killed in the intersection. Humanity treats technology much the same as the known dangerous intersection, and thus the answer to controlling the emerging threat of CBNRE, cyber and integrated autonomous systems is possible. The question is will humanity break from historical tradition and create the framework and solutions before the threats are allowed to go unchecked and flourish to the detriment of humankind.

### **Legal Considerations for Autonomous Systems as WMD/DEW Delivery Platforms**

Scientists believe that the earliest blending of technology and warfare occurred in 400,000 BC. Researchers found evidence of humans using spears in what is now known as Germany. In 5,300 BC, horses were domesticated and used for transporting and mobilizing warfare. Military technology warfare advanced quickly from China's Ming Dynasty, developing the matchlock, muskets in the 1500s, underwater mines in the 1770s, submarines in the 1870s, and nuclear bombs in the early 1940s. The arc of military history is rampant advancements in technology in many ways. (Marshall, 2009) While it is true that the transition from the spear to the nuclear bomb took thousands of years, one advancement, the computer, has led to an exponential increase in the speed of advancement of military warfare and humanitarian law.

George Washington once wrote: "My first wish is to see this plague of mankind, war, banished from the earth." (Hoynes, 1916) Sadly, his sentiment and those of untold others have proven more aspirational than realistic. The harsh reality is that conflict between humans is nearly as old as humanity itself. It was only through evolution and enlightenment that some individuals began to ponder that if war is inevitable, shouldn't there be some way of limiting its horrors to combatants only and theoretically protect the innocent?

According to Leslie Green, "From earliest times, some restraints were necessary during armed conflict. Thus, we find numerous references in the Old Testament wherein God imposes limitations on the warlike activities of the Israelites." (Green, 1998) The Chinese, Roman, and Greek empires sought to address the subject. Though repeated attempts were made to codify some universal rules of warfare, it was not until the 1860s when Henri Durant, founder of the Red Cross, began to codify a generally accepted international set of rules regarding warfare and the treatment of civilians and combatants. (Lu, 2018)

**Figure 16.8: WWII Red Cross Prisoner of War Gift Package**



Source: (National WWII Museum, 2020)

According to the International Committee of the Red Cross, six crucial principles must be adhered to by all combatants:

1. **No targeting civilians;**
2. **No torture or inhumane treatment of detainees;**
3. **No attacking hospitals and aid workers;**
4. **Provide safe passage for civilians to flee;**
5. **Provide access to humanitarian organizations; and**
6. **No unnecessary or excessive loss and suffering.** (anonymous, 2022)

Although the technology discussed in this book is groundbreaking, the technology may ultimately remove humans from the decision-making process to determine if deadly force is appropriate to use in a particular situation, against whom, and when. Humans must currently choose to deploy autonomous technology in battle;



however, A.I. and machine learning may soon make that decision without human intervention. Without some set of rules and standards for nations making such a critical decision, the likelihood of a mass casualty event involving the civilian population will increase.

### **Assessment of the State of Readiness for the Legal Community to Prosecute Cases with Autonomous Systems Use in the WMD/DEW space**

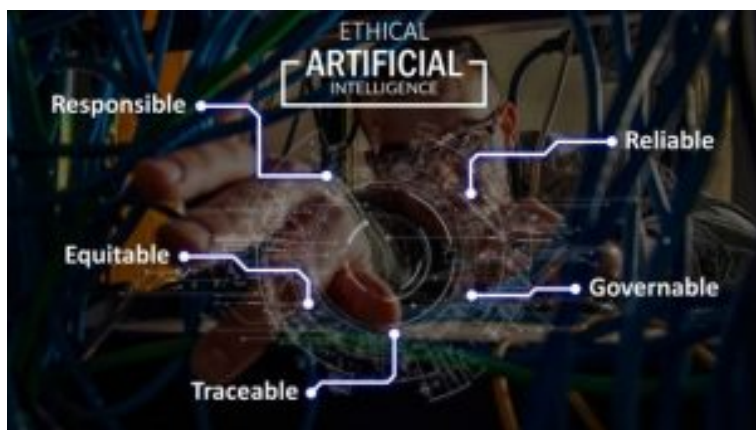
With rapid advances in military technology in the 1900s and 2000s, the need for some practice of uniform international humanitarian warfare rules arose. Gas, chemical, and nuclear weapons carried an inherent likelihood of significant civilian casualties. Advances in the rapid delivery of these weapons globally and without warning results in less time to prepare civilian populations for an attack. Without new rules of warfare and adjudication processes for violators, the risk to mankind becomes untenable. The first attempts to address this new reality started with the First Hague Conference of 1898-1899, the Second Hague Convention of 1907, the Geneva Conventions, the League of Nations, and eventually the United Nations. (Klare, 2019)

Enter the most recent and perhaps most significant technological advance or change in decades, Artificial Intelligence (“A.I.”). A.I. and autonomous warfare may be a dream for many in the military, yet others foresee a nightmare. Without some foundational understanding of its development and use on the battlefield, many fear runaway technology which could cause catastrophic damage. In 2018, the United States Department of Defense (“DoD”) Defense Innovation Board (“DIB”) developed foundational principles for the safe and ethical implementation of A.I. (United States Department of Defense, Defense Innovation Board, 2019). The DIB issued its recommendations to the DoD in 2019. (Lopez, 2020) In February 2020, the DoD adopted the following five A.I. principles:

1. **Responsible:** DoD personnel will exercise appropriate levels of

- judgment and care while remaining responsible for the development, deployment, and use of A.I. capabilities.
2. **Equitable:** The department will deliberate steps to minimize unintended bias in A.I. capabilities.
  3. **Traceable:** The department's A.I. capabilities will be developed and deployed such that relevant personnel possesses an appropriate understanding of the technology, development processes, and operational methods applicable to A.I. capabilities, including transparent and auditable methodologies, and data sources, and design procedures and documentation.
  4. **Reliable:** The department's A.I. capabilities will have explicit, well-defined uses, and the safety, security, and effectiveness of such capabilities will be subject to testing and assurance within those defined uses across their entire life cycles.
  5. **Governable:** The department will design and engineer A.I. capabilities to fulfill their intended functions while possessing the ability to detect and avoid unintended consequences and disengage or deactivate deployed systems that demonstrate unintended behavior. (Lopez, 2020)

**Figure 16.9: United States Department of Defense AI Interests**



Source: (Lopez, 2020)

Whether these rules of warfare have had the intended effect is still a subject of much debate. With the parallel access to new technology such as A.I., many Non-Governmental Organizations (NGOs), terror groups, and individuals have gained through the internet, muted efficacy of humanitarian rules of warfare may be the result. The discussion of the legal considerations of implementing A.I. on the battlefield deserves a complete and detailed analysis. To limit the discussion in this textbook, students must understand that there may be real-life legal consequences relating to the use of A.I. automation or augmentation. Given the devastating capability of WMD/DEW technology to inflict mass casualties, the possibility of legal consequences must be considered in all aspects.

**Legal and Cyber Considerations While Building the Legal Framework Towards Peaceful Containment/Use of Autonomous Systems in the Future**

To successfully promulgate rules of warfare using A.I., it is essential to determine who is responsible for unintended harm or intentional improper use of AI-based military systems. Is it the soldier who pushes a button to engage an A.I. weapons system that

wrongfully kills thousands of civilians, or is it the superior officer who ordered the soldier to engage the system? In civil law, the legal principles of proximate cause are key.

According to John Kingston of the University of Brighton, “Criminal liability usually requires an action and a mental intent (in legalese and *actus rea* and *mens rea*).” (MIT Technology Review, 2018) Kingston examines the groundbreaking work of Gabriel Hallevy, who examined if and how A.I. systems that cause injury or death could be held criminally liable. (Hallevy, 2015) (Kingston, 2018)

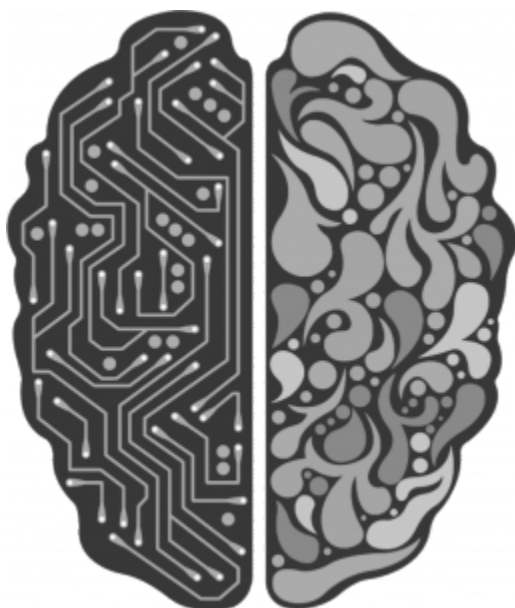
Hallevy discussed three different legal theories by which A.I. systems might be held criminally responsible for harm or civilly liable for damages.

1. “Perpetrator-via-another. Suppose an offense is committed by a mentally deficient person, a child, or an animal. In that case, the perpetrator is held to be an innocent agent because they lack the mental capacity to form a *mens rea* (this is true even for strict liability offenses). However, if the innocent agent was instructed by another person (for example, if the owner of a dog instructed his dog to attack somebody), then the instructor is held criminally liable.”
2. “Natural-probable-consequence. In this model, part of the A.I. program intended for good purposes is activated inappropriately and performs a criminal action.”
3. “Direct liability. This model attributes both *actus reus* and *mens rea* to an A.I. system. It is relatively simple to attribute an *actus reus* to an A.I. system. If a system takes an action that results in a criminal act or fails to take any action when there is a duty to act, then the *actus reus* of an offense has occurred.” (Hallevy, 2015)

Although seemingly a complex legal theory, the concept of criminal or civil liability for A.I. harm, be it on the battlefield or

in everyday civilian life, the adjudication process will require determining what type of A.I. technology is at issue.

**Figure 16.10: MIT Technology Review**



Source: (Hallevy, 2015)

Given the speed of technology and the seemingly endless uses for A.I., it is challenging to create definitions for the type of A.I. in a particular instance. In striving for simplicity, this definition from 2020 seems to work:

“A.I. solutions are meant to work in conjunction with people to help them accomplish their tasks better, and A.I. solutions are meant to function entirely independently of human intervention. The sorts of solutions where A.I. is helping people do their jobs

better is usually referred to as “augmented intelligence” solutions while those meant to operate independently as “autonomous” solutions.” (Walch, 2020)

Initially, legal doctrine focused upon autonomous applications for A.I. technology. The concept of robots performing automated tasks or autonomous vehicles transporting people and goods globally, on, under, above the ground and seas of the earth. From a legal perspective, the analysis of autonomous intelligence is far less complicated than the legal issues relating to augmented intelligence.

“Prior scholarship has therefore focused heavily on autonomous vehicles, giving rise to two central themes. The first is that by automating the driving task, liability for car accidents will move away from negligence on the driver’s part toward product liability for the manufacturer. Because there is no person to be negligent, there is no need to analyze negligence. Scholars instead move straight to analyzing product liability’s doctrinal infirmities in the face of A.I.” (Selbst, 2020)

The legal analysis relating to augmented intelligence is more challenging than automated intelligence. Because A.I. guides a human who then acts or disregards the information. As General Mike Murray put it: “Where I draw the line — and this is, I think well within our current policies – [is], if you’re talking about a lethal effect against another human, you have to have a human in that decision-making process” (Freedberg, 2021)

Instead of determining whether an autonomous technology did not perform as designed or was incorrectly designed, the challenges created by augmented intelligence require an additional component of the interaction between man and A.I., and what if the human took any subsequent action.

A final consideration of a very brief overview of this subject is that legislation and legal precedents can have far-reaching consequences. What may seem like a logical path may be insufficient for new applications of existing A.I. technology. Generally speaking, the law moves much slower than technology.

While technology is actively evolving, the law of technology moves by comparison at a snail's pace. Larry Downes of the Harvard Business Review took this view of why slow and steady a far better legal strategy is than creating what many call "knee jerk" regulation. He wrote:

"That, in any case, is the theory on which U.S. policymakers across the political spectrum have nurtured technology-based innovation since the founding of the Republic. Taking the long view, it's clearly been a winning strategy, especially compared to the more invasive, command-and-control approach taken by the European Union, which continues to lag on every measure of the Internet economy. (Europe's strategy now seems to be little more than to hobble U.S. tech companies and hope for the best." (Downes, 2018)

## **CONCLUSIONS**

As all autonomous systems begin to integrate and communicate, they will begin to goal seek and assist each other as part of an evolving network of devices. These devices can be modular and can enter and exist in this artificial ecosystem to obtain goals, assist other autonomous systems, or assist humans as required. The proliferation of the smaller autonomous systems is of unique concern as they have an inexpensive price point and can be operated out of the box with very little training. "As the first iteration of the robotics revolution, they have proliferated on a massive scale with estimates of over five million drones having been sold worldwide." (Dunn, 2021)

As technology continues to push human intervention aside, the legal parameters and consequences become more complex. The national and international laws will need to be created and upheld to broad standards for the future and still hold those accountable for atrocities done by autonomous systems.

## **Questions**

1. Do you think human evolution will see the WMD/DEW as a

- positive or negative outcome toward peace?
2. List three disruptive technologies in WMD/DEW arena.
  3. How would you take advantage of airspace and freedom of movement with autonomous systems versus manned systems?
  4. Name three ways legal ramifications can deter the use/misuse of autonomous systems in the WMD/DEW arena.
  5. Describe two catastrophic scenarios caused by autonomous systems that are not defined by the legal arena?

### **Bibliography**

Allard, M. (2022, January 21). QYSEA, KDDI & PRODRONE team up to create the world's first sea-to-air drone. Retrieved from [www.newsshooter.com](https://www.newsshooter.com/2022/01/21/qysea-kddi-prodrone-team-up-to-create-the-worlds-first-sea-to-air-drone/): <https://www.newsshooter.com/2022/01/21/qysea-kddi-prodrone-team-up-to-create-the-worlds-first-sea-to-air-drone/>

anonymous. (2022). *rules-war-why-they-matter*. Retrieved from [www.icrc.org/en/document/](https://www.icrc.org/en/document/rules-war-why-they-matter): <https://www.icrc.org/en/document/rules-war-why-they-matter>

Defense, U. S. (2020, March 11). DOD adopts five principles of artificial intelligence ethics. Retrieved from Army, mil: [https://www.army.mil/article/233690/](https://www.army.mil/article/233690/dod_adopts_5_principles_of_artificial_intelligence_ethics)

Downes, L. (2018, February 9). *How More Regulation for U.S. Tech Could Backfire*. Retrieved from Harvard Business Review: <https://hbr.org/2018/02/how-more-regulation-for-u-s-tech-could-backfire>

Dunn, D. H. (2021). *Small drones and the use of chemical weapons as a terrorist threat*. Retrieved from [www.Birmingham.ac.UK/research/perspective/](https://www.birmingham.ac.uk/research/perspective/): <https://www.birmingham.ac.uk/research/perspective/small-drones-chemical-weapons-terrorist-threat.aspx>

Emanuel, P. W. (2019). *Cyborg Soldier 2050: Human/Machine*



*Fusion and the Implications for the Future of the DOD*. Retrieved from community.apan.org/: <https://community.apan.org/wg/tradoc-g2/mad-scientist/m/articles-of-interest/3004>

FLIR. (2022). *Black Hornet PRS for Dismounted Soldiers*. Retrieved from [www.flir.com/products/](http://www.flir.com/products/): <https://www.flir.com/products/black-hornet-prs/>

Freedberg, S. J. (2021, April 23). *Artificial Intelligence, Lawyers, And Laws Of War*. Retrieved from Breaking Defense: <https://breakingdefense.com/2021/04/artificial-intelligence-lawyers-and-laws-of-war-the-balance/>

Gauri, P. &. (2019, May 16). *what-the-fifth-industrial-revolution-is-and-why-it-matters/*. Retrieved from [europeansting.com/](http://europeansting.com/): <https://europeansting.com/2019/05/16/what-the-fifth-industrial-revolution-is-and-why-it-matters/>

Green, L. C. (1998). *The Law of War in Historical Perspective*. Providence, RI: U.S. Naval War College.

Hallevy, G. (2015). *Liability for Crimes Involving Artificial Intelligence Systems*. Switzerland: Springer.

Hoynes, C. W. (1916). *Preparedness for War and National Defense*. Washington, DC: Government Printing Office.

International Committee of the Red Cross. (2022, March 19). *The Geneva Conventions of 1949 and their Additional Protocols*. Retrieved from The International Committee of the Red Cross: <https://www.icrc.org/en/doc/war-and-law/treaties-customary-law/geneva-conventions/overview-geneva-conventions.htm>

Kimball, D. &. (2020, March 1). *Chemical Weapons: Frequently Asked Questions*. Retrieved from [www.armscontrol.org/factsheets/Chemical-Weapons-Frequently-Asked-Questions#::https://www.armscontrol.org/factsheets/Chemical-Weapons-Frequently-Asked-Questions#:~:text=Chemical%20weapons%20can%20be%20delivered,converted](http://www.armscontrol.org/factsheets/Chemical-Weapons-Frequently-Asked-Questions#::https://www.armscontrol.org/factsheets/Chemical-Weapons-Frequently-Asked-Questions#:~:text=Chemical%20weapons%20can%20be%20delivered,converted)

Kingston, J. K. (2018). *Artificial Intelligence and Legal Liability*. Ithaca, NY: Cornell University ARXIV.

Klare, M. T. (2019). *Autonomous Weapons Systems and the Laws of War*. Washington, D.C.: Arms Control Association.

Lopez, T. (2020). *dod\_adopts\_5\_principles\_of\_artificial\_intelligence\_ethics*. Retrieved from [www.army.mil/](https://www.army.mil/article/233690/dod_adopts_5_principles_of_artificial_intelligence_ethics): [https://www.army.mil/article/233690/dod\\_adopts\\_5\\_principles\\_of\\_artificial\\_intelligence\\_ethics](https://www.army.mil/article/233690/dod_adopts_5_principles_of_artificial_intelligence_ethics)

Lu, J. (2018, June 28). *The 'Rules Of War' Are Being Broken. What Exactly Are They?* Retrieved from NPR.Org: <https://www.npr.org/sections/goatsandsoda/2018/06/28/621112394/the-rules-of-war-are-being-broken-what-exactly-are-they>

Marshall, M. (2009, July 7). *Timeline: Weapons technology*. Retrieved from New Scientist: <https://www.newscientist.com/article/dn17423-timeline-weapons-technology/>

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

MIT Technology Review. (2018, March 12). *When an A.I. finally kills someone, who will be responsible?* Retrieved from MIT Technology Review: <https://www.technologyreview.com/2018/03/12/144746/when-an-ai-finally-kills-someone-who-will-be-responsible/>

Mumm, D. H. (2022). *Securing Quantum Computers Through the Concept of In-Memory Computing (IMC)*. Retrieved from [www.victorysys.com](http://www.victorysys.com)

National WWII Museum. (2020, June 5). *Curator's Choice: Gifts from the "Geneva Man "*Retrieved from National WWII Museum: <https://www.nationalww2museum.org/war/articles/curator-kim-guise-geneva-collections>

Pledger, T. (2021). *The Role of Drones in Future Terrorist Attacks*. Retrieved from [www.ausa.org/](https://www.ausa.org/publications/role-drones-future-terrorist-attacks): <https://www.ausa.org/publications/role-drones-future-terrorist-attacks>

Selbst, A. D. (2020). NEGLIGENCE AND AI'S HUMAN USERS. *Boston University Law Review*, 1323.

Stolfi, B. D. (2021). *Swarm-based-counter-UAV-defense-system*. Retrieved from [www.semanticscholar.org/https://www.semanticscholar.org/paper/Swarm-based-counter-UAV-defense-system-Brust-Danoy/24179f7cf9854cb41ca2595c811d26563a49014e](https://www.semanticscholar.org/paper/Swarm-based-counter-UAV-defense-system-Brust-Danoy/24179f7cf9854cb41ca2595c811d26563a49014e)

United States Department of Defense. (2020, February 254). *Department Of Defense Press Briefing on the Adoption of Ethical Principles for Artificial Intelligence*. Retrieved from Defense.gov: <https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/2094162/departement-of-defense-press-briefing-on-the-adoption-of-ethical-principles-for/>

United States Department of Defense, Defense Innovation Board. (2019). *A.I. Principles*: Washington, DC: United States Department of Defense.

Walch, K. (2020, January 12). *Is There A Difference Between Assisted Intelligence Vs? Augmented Intelligence?* Retrieved from Forbes: <https://www.forbes.com/sites/cognitiveworld/2020/01/12/is-there-a-difference-between-assisted-intelligence-vs-augmented-intelligence/?sh=418b012426ab>

Wingo, H. (2020). Smart City IoT: Co-Designing Trustworthy Public Safety Drones for Indoor Flight Missions. *Academic Conferences International Limit*, 406-409, XX. Retrieved from Wingo, H. (2020). Smart City IoT: Co-Designing Trustworthy Public Safety Drones for Indoor Flight Missions. In (pp. 406-409,XX). Reading: Academic Conferences International Limit.

# 17. Unique Challenges of Responding to Bioterrorism & Chemical Threats & Attacks Delivered by Drones

**By Dr. Suzanne Sincavage & Professor Candice M. Carter**

## **STUDENT OBJECTIVES**

- What are the national security risks posed by the advancement of emerging robotic technologies and their enabling effects in the bioweapons/Weapons of Mass Destruction (WMD) space?
- What potential platforms exist for delivering biological weapons (BW) used by terrorists?
- What new opportunities or solutions do advanced robotics offer to national security problems and/or their challenges in countering chemical threats?
- What challenges and opportunities exist for global governance to mitigate the CBRN risk?

## **INTRODUCTION**

The convergence of drone and 3D printing technologies may allow terrorists to acquire CBRN weapons with minimal identifiable signatures. (Kallenborn, 2019) As technology continues to evolve, its availability becomes more common and attractive to all levels of threat actors. The use of explosive-laden quadcopter drones to try to assassinate the Iraqi prime minister, Mustafa al-Kadhimi, at his residence in November 2021 was yet another wake-up call about the utility of small drones to armed non-state groups and the dangers

they pose when operated by people who embrace violence to effect change. (Rassler & al-'Ubaydi, 2021) Modified drones for chemical and bioterrorism attacks by terrorist organizations might not look like Nation-state actors, but the drones still provide the element of surprise and damaging attack.

### **ADVANCED ROBOTICS**

Advanced robotics generates both new risks and opportunities for the WMD

space. Increasingly, sophisticated robots are available commercially for industrial and domestic use, with commercial drones at the forefront of this trend. Whereas commercial drones offer states and nonstate actors a potential delivery system for WMD, the wide range of robotics across the sea, land, and air domains enhances defense capabilities for countering WMD by providing agile and cheap platforms for detecting WMD operating in hazardous environments.

### **ROBOTICS: Technology Overview**

The development of advanced robotics, a branch of mechanical engineering, electrical engineering, and computer science, began in the 1960s with a basic robotic arm designed to perform difficult or too dangerous tasks for humans. The field of advanced robotics has been tracked closely with advances in computing, artificial intelligence (AI), and energy storage. Today, increasingly sophisticated robots are widely available on the commercial market, and prices are dropping dramatically, expanding their use. (Brown, 2014) A robot is a reprogrammable, multifunctional manipulator designed to move material, parts, tools, or specialized devices through various programmed functions to perform various tasks. (Brown, 2014) All robots have certain defining features, including a mechanical structure designed to carry out a specific task, electrical components that power and control the machinery, and some level of computer programming code.

Artificial intelligence refers to the near-human, human, or super-human ability to respond to a complex environment. Robots are intelligent systems that apply a certain level of AI to a specific problem or domain. The sophistication of the computer program embedded in a robot determines its level of autonomy and the nature of its human oversight. Weak artificial intelligence, the cognitive ability to solve specific problems or perform certain tasks, has supported many applications for many decades. (Brown, 2014) Humans control robots using weak AI. A remote-control robot has programmed with a preexisting set of commands that it will perform when it receives a signal from a control source, typically a human with remote control. This is called “in the loop,” where a human confirms actions, denies actions outside designed constraints and denies actions outside the operational context.

On the opposite side of the spectrum are autonomous robots, which are intelligent machines capable of performing tasks in the world by themselves, normally requiring human intelligence (e.g., perception, conversation, decision-making) without explicit human control. This is referred to as “out of the loop” since machines function without the ability of humans to intervene. To be autonomous, a system must have the capability to independently compose and select among different courses of action to accomplish goals based on its knowledge and understanding of the world, itself, and the situation.

In the future, robots will be increasingly able to operate autonomously

without human intervention. Hybrid systems involve both elements of human control and autonomy. This is referred to as “on the loop,” where a human can allow actions outside designed constraints or the operational context to take advantage of evolving context.

In addition to different levels of complexity, robots can be developed to address many types of problems or for use in and across many different domains, including industry, commerce, land,

sea, and air. Of these domains, UAVs (or “drones” as they are popularly known) are taking off in the civilian and commercial sectors.

Industry experts are hailing 2016 as the dawn of the drone age. Consumer sales are expected to reach four million in 2016 and 16 million by 2020. The number of operators of drones, both large and small, is rising rapidly. Many affordable commercial drones offer significant off-the-shelf capabilities. UAV technology has enabled thousands of individuals to enter the field of aviation with comparably little training and oversight and the growing market for civilian drones.

Companies like Amazon and Google, among others, are developing drones as a platform for making rapid deliveries across cities. According to the Federal Aviation Administration, the most significant uses of UAVs come from agriculture, photography, and mapping. In the agricultural sector, for example, drones allow for precision farming. This method reduces the number of chemicals sprayed on crops by precisely dusting crops. Drones can also fly close to the ground and stream videos to allow producers to be more efficient in addressing growth issues and even monitoring unexpected pests. This can help farmers address water damage or dryness levels and aid in monitoring large crops that need a lot of attention.

Although robotics is becoming more accessible, cheaper systems remain limited in autonomy and capabilities. The utility of drones for many applications is constrained by range, flight time, and payload or carry weight (enabled by battery/energy storage). Typically, there are trade-offs between flight time and weight. The heavier the carry weight,

the shorter the flight time. Much of the promise of robotics remains a prospect of the future. Engineers have thus far not been able to build a machine capable of human-like cognition. However, advances in computing and energy storage may offer near-term leaps in advanced robotics.

### 3D PRINTING

3D printers can be used to create equipment components at reduced cost and have been used to create bioreactors, microscopes, and other key elements. (Kallenborn, 2019). The digital build-files for 3D printed items can also be sent and received online, perhaps from black market sellers or individuals sympathetic to the terrorist's ideology. (Kallenborn, 2019) 3D printers make it possible to create a custom drone to deliver a CBRN attack.

Professor Lee Cronin from the University of Glasgow has trademarked the process called "*chemputer*." Chemputer uses intelligent biomatter to 3D print drones and planes, giving militaries a huge advantage in the new frontier of warfare.

**Figure 17.1 Chemputer Drones**



Source: (Watkin, 2016)

"We have been developing routes to digitize synthetic and materials chemistry and at some point, in the future, hope to assemble complex objects in a machine from the bottom up or with minimal human assistance. Creating small aircraft would be very challenging, but I'm confident that creative thinking and convergent digital technologies will eventually lead to the digital programming



of complex chemical and material systems,” states Professor Lee Cronin. (Watkin, 2016)

**Figure 17.2 3D Printed Drone**



Source: (Global Guerrillas, 2012)

Converging with 3D printing, some drones can now be printed relatively quickly; they are lighter, travel farther, and have a greater capacity to carry payloads than other remote-controlled electronics. For example, researchers at the University of Virginia were tasked to create a drone similar to current military drones, but that could be 3D-printed and used only off-the-shelf parts. The Razor drone is tailorable to meet operational needs and is capable of variable flight time (45+ minutes) and speeds (40+ mph). Its cost was about \$2,500, most of which was for the cellphone that acts as the entire electronics package of the drone and is capable of command

and control via cell signal. The Razor drone can be built in just over 24 hours. The costs are expected to drop even further.

In March 2014, engineers in the United Kingdom successfully developed a 3D-printed drone that cost \$9 per copy and could be built and assembled in less than 24 hours. If a non-state actor group acquired the blueprint and ten printers, it could print 10 per day and 300 per month at the cost of \$2,700 plus the cost of the printers.

**Figure 17.3 ISIS 3D Printed Bomb**



Source: (Koslow, 2016)

### **BIOPRINTERS**

Bioprinting uses 3D printing-like techniques to combine cells, growth factors, and biomaterials – collectively named ‘bioinks’ – to create living tissues that almost perfectly mimic their structure in the body. (Pavey, 2021) Bioinks are deposited layer by layer onto a supporting hydrogel, which functions like paper in conventional printing. (Pavey, 2021) However, unlike normal printing, the hydrogel dissolves once the product matures, leaving it freestanding. (Pavey,

2021) This is a remarkable advancement for drug research, fighting human disease, and creating customized medicine. However, this opens the door for a great amount of evil. This could be used to create custom poison, bioprinted killer bacteria, and recreate a vaccine to be lethal to the global community. Researchers at Rutgers-New Brunswick School of Engineering believe they have found a way to protect against using 3D printing for evil. The first solution focuses on designing a sensor that can measure the composition and diameter of raw materials passing through the printer's extruder to ensure they meet expectations before the object is printed. A dielectric sensor can detect a change of 0.1mm in filament diameters and a change of 10% in concentration composition. (RUTGERS UNIVERSITY, 2021) The second solution uses high-resolution computed tomography images to detect residual stresses in printed objects that contrast benign and malicious designs before activation of the attack. This CT detection has an accuracy of 94.6% in identifying 4D attacks in a single printing layer. (RUTGERS UNIVERSITY, 2021), (2021) The researchers are also working on combining the above solutions with software security, control system design, and processing signals. This would be a valuable solution in protecting the use of 3D printing technology for evil.

**Figure 17.4 3D Bioprinter**



Source: (Pavey, 2021)

U.S. Defense Threat Reduction Agency (DTRA) provided the researchers at Wake Forest University with \$24 million to aid their research and development in combating nuclear, chemical, and biological weapons. (Decker, 2013) The WFU lab uses “Body on a Chip” to replicate the cells that function as organs in the human body. With this capability, the scientists can see how the cells act when exposed to specific chemical and biological weapons to find the right treatment for survival.

### **THE RISKS**

Among the wide range of robotics coming of age in the near term, policymakers are most immediately concerned about the use of hobbyist and commercial drones for potential mischief by non-state actors and the development of advanced UAVs by state actors as an asymmetrical capability vis-à-vis high-tech platforms such as fighter jets. Enabling aerial operations, drones can provide unfettered access to targets in ways that terrorists could previously only dream about and security planners have not had to worry about. Airborne

improvised explosive devices (IEDs) could be used to attack people, infrastructure, or aircraft, among many other possible targets, where large destructive power may not be necessary to cause tremendous amounts of damage. Hobbyist drones have limited payloads and ranges but can still be used for disproportionate effects. For example, in September 2013 in Germany, a political protester flew a drone within feet of German Chancellor Angela Merkel and Defense Minister Thomas de Maiziere before it crash-landed next to them. Armed with even a small amount of

explosive fragments or shrapnel could have killed or maimed two members of Germany’s leadership.

In early November 2014, multiple drones were sighted over French nuclear power plants in what was described as a

“provocation of French authorities.” A squadron of drones armed with explosives and detonated in certain positions may be able to cause significant damage to expensive infrastructure. Military aircraft and other high-technology platforms are not immune to this threat. A small number of expendable drones could cause considerable damage to a military aircraft costing hundreds of millions of dollars. The number of drones is scalable, whereas the physical capability of each drone limits explosive capacity.

In 2009, US Airways Flight 1549 had to make an emergency landing on the Hudson River after colliding with a gaggle of Canada geese. Compared to a bird, a drone consisting of metal, hard plastics, batteries, and electronics could do far more damage and potentially take down a passenger jet.

As advances in artificial intelligence are mated with drone technology, drones will begin to perform previously pilot-controlled tasks (navigation, coordination, targeting) autonomously, without the need for input from the primary operator. Multiple drones possessing these autonomous capabilities could “swarm” a target and offer a powerful asymmetric capability to states and non-state actors.

Carrying biological, chemical, or radiological materials, drones offer an extremely agile delivery platform for WMD, even if they are still limited to a small payload. On 24 April 2015, a Japanese man landed a drone containing radioactive material on the roof of Japanese Prime Minister Shinzo Abe’s office to protest Japan’s nuclear energy policy.

In October 2016, ISIS used a drone loaded with explosives for the first time in an attack that killed two soldiers and injured two others. Given the use of chlorine and mustard agents by ISIS, it is conceivable that insurgents might use drones as delivery vehicles for chemical and biological agents shortly.

Drones flown in overcrowded venues or around aircraft at airports do not have to be lethally armed to lead to panicked responses from people, companies, and authorities and, therefore, could be used to instill fear into a target.

## **THE OPPORTUNITIES**

Advanced robotics offer ideal platforms to perform dangerous counter-WMD missions, including surveillance and detection, decontamination, and operations. Cheap, expendable, and often tiny in size, robotics offers a powerful surveillance and detection missions tool. The U.S. Army is developing Micro Autonomous Systems and Technology (MAST). These tiny insect-shaped ground and aerial robots are designed to assist soldiers with rapid and mobile intelligence, surveillance, and reconnaissance missions in high-risk zones.

Microbots can capitalize on their size to move quietly and easily access small spaces. If a unit approaches a building and needs to know what is inside, the soldiers could deploy a reconnaissance team of microbots. The robots could penetrate the building undetected, search the interior, map the layout, and provide data on its occupants and locations.

The U.S. Army also developed the WMD Aerial Collection System, an unmanned capability designed to assess the presence of airborne CBRN material during military operations. The UAV mounted with trackers and collectors can locate, intercept, and collect aerial samples from a CBRN plume for analysis in a laboratory facility. The system allows for in-flight detection reporting.

Enhanced by AI and 3D printing technologies, small teams of MAST robots

are being designed to be autonomous and capable of coordination or “swarming.” These robots are envisioned to support soldiers with improved tactical situational awareness in urban and complex terrain. In the future, the U.S. Army hopes to be able to 3D-print drones while on a mission in less than 24 hours.

Robotics are ideal platforms for detecting the presence of CBRN materials in hostile areas. The U.S. Army partnered with Carnegie Mellon University and Sikorsky Aircraft to design an autonomous ground vehicle delivered by UAV (modified Black Hawk helicopter)

into hostile or inaccessible areas equipped with chemical, biological and radiological sensors for missions in contaminated areas.

Robots can safely operate in hazardous environments and assist in counter-WMD missions, including decontamination and operations. The U.S. Army is working to develop a robot capable of locating, lifting, and carrying wounded soldiers out of dangerous zones to safety for treatment. The Battlefield Extraction-Assist Robot (BEAR) is currently designed to be remote-controlled by combat medics, but developers are working on expanding its capacity to assume semi-autonomous tasks. The BEAR has a “teddy bear” face to reassure injured soldiers and can be used for other missions such as search and rescue, handling hazardous materials, surveillance, reconnaissance, mine inspection, lifting hospital patients, or even warehouse automation.

Leveraging robots’ ability to operate in hazardous environments, the Department of Defense contracted with Boston Dynamics and the Midwest Research Institute to create a robot capable of testing chemical warfare suits called the PETMAN. Once completed, the PETMAN weighed 180 pounds and could run 4.4 mph on smooth surfaces. Tests conducted with these robots ensure that the suits maintain their integrity in a contaminated environment while moving the same way a human would.

The U.S. Navy has developed the Battlespace Preparation Autonomous Underwater Vehicle (BPAUV), a small, fast, autonomous underwater robot, primarily to handle its mine countermeasure mission in shallow water. With its compact size and accurate navigation, the BPAUV can be operated from a ship or boat, function in various weather conditions, and collect high-quality imagery necessary for successful operations. Other applications include unexploded ordnance, anti-submarine warfare, and oceanography.

## **CONCLUSIONS**

Robotics offers powerful and often cheap platforms for

performing various tasks. For non-state actors, drones may serve as a readily available delivery platform for an IED or WMD. For advanced states and militaries, robotics offer significant advantages for operating in hazardous environments on land, the sea, and the air. L.G. Shattuck, "Transitioning to Autonomy: A Humans Systems Integration Perspective," paper presented at the Autonomy Workshop, NASA Ames Conference Center, Moffett Field. As defined by Kadte and Wells.

The Department of Defense defines unmanned aerial vehicles (UAVs) as powered aerial vehicles that do not carry a human operator, use aerodynamic forces to provide vehicle lift, fly autonomously or be piloted remotely, and be expendable or expendable recoverable, and can carry a lethal or nonlethal payload. Noteworthy incidents and insights from failed experiments, the interplay between defensive and offensive innovations, asymmetric mirror-imaging, hobbyist innovation, and enhancements for commercial products would provide additional layers to allow analysts to track better and anticipate relevant changes taking place across an innovation ecosystem comprising terrorist, hobbyist, industry, and state activity. (Rassler & al-'Ubaydi, 2021) Such an approach would help governments better prepare for new, creative, and innovative approaches that terrorists might use tomorrow and in the years ahead. (Rassler & al-'Ubaydi, 2021)

## **Bibliography**

Atherton, K. D. (2016, February 19). *Army Wants Drones On-Demand, 3D-Printed In 24 Hours Or Less*. Retrieved April 11, 2022, from Popular Science: <https://www.popsci.com/army-wants-to-3d-print-drones-in-24-hours/>

Benedict, J. R. (2016, October 1). *Global Power Distribution and Warfighting in the 21st Century*. Retrieved April 11, 2022 from NDU Press: <https://ndupress.ndu.edu/Media/News/Article/969640/global-power-distribution-and-warfighting-in-the-21st-century/>

BLUEFIN Robotics. (2010). *Bluefin-21 BPAUV*. Retrieved April 11,



2022 from Bluefin-21 BPAUV: <https://gdmissionsystems.com/-/media/General-Dynamics/Maritime-and-Strategic-Systems/Bluefin/PDF/Bluefin-21-BPAUV-Product-Sheet.ashx?la=en&hash=DA69EC6FF1F9BA7499D171454DB8CCDC7E6F479>

Brown, M. (2014, September 30). *Extending the Reach of the Warfighter through Robotics (ERWR)*. Retrieved April 11, 2022 from DVIDS: <https://www.dvidshub.net/video/363784/extending-reach-warfighter-through-robotics-erwr>

Crawford, J. (2016, October 20). *Report warns of ISIS developing drones for chemical attacks*. Retrieved April 11, 2022 from CNN: <https://www.cnn.com/2016/10/20/politics/terrorist-groups-and-drones/index.html>

Davis, L. E. (2016, October 11). *Remotely Piloted Innovation*. Retrieved April 11, 2022 from DTIC: <https://ctc.usma.edu/wp-content/uploads/2016/10/Drones-Report.pdf>

Dean, T. R. (2014, May 16). *Researchers consider miniature robots to enhance capabilities* | Article | The United States Army. Retrieved April 11, 2022 from U.S. Army: <https://www.army.mil/article/125337/>

[Researchers\\_consider\\_miniature\\_robots\\_to\\_enhance\\_capabilities/](https://www.army.mil/article/125337/)

Decker, B. (2013, September 30). *Bioprinting to Test Antidotes for Chemical Weapons*. Retrieved April 11, 2022 from Bioprinting World: <http://bioprintingworld.com/bioprinting-to-test-antidotes-for-chemical-weapons/>

Defense Daily Network. (2008, September 30). *DTRA Seeks Info on WMD Aerial Collection System*. Retrieved April 11, 2022 from Defense Daily: <https://www.defensedaily.com/dtra-seeks-info-on-wmd-aerial-collection-system/homeland-security/>

Demonic, M. R., & Mills, M. E. (2021, August 12). 2014 NDIA GROUND VEHICLE SYSTEMS ENGINEERING AND TECHNOLOGY SYMPOSIUM AUGUST 12-14 NOVI, MICHIGAN *Extending the Reach of the Wa*. Retrieved April 11, 2022 from Ground Vehicle Systems Engineering and Technology Symposium (GVSETS) & Advanced

Planning Briefings for Industry (APBI): <http://gvsets.ndia-mich.org/documents/AAIR/2014/>

Extending%20the%20Reach%20of%20the%20Warfighter%20through%20Robotics%20-%20Autonomous%20Execution%20of%20a%20Tactical%20Resupply%20and%20Surveillance%20Mission.pdf

Global Biodefense Staff. (2022, February 25). *Biodefense Headlines – 25 February 2022*. Retrieved April 11, 2022 from Global Biodefense: <https://globalbiodefense.com/2022/02/25/biodefense-headlines-25-february-2022/>

Global Guerrillas. (2012, February 17). *Print Your Own Drone: Free Designs and Tools*. Retrieved April 11, 2022 from Global Guerrillas: <https://globalguerrillas.typepad.com/globalguerrillas/2012/02/print-your-own-drone-free-designs-and-tools.html>

Golson, J. (2014, September 16). *A Military-Grade Drone That Can Be Printed Anywhere*. Retrieved April 11, 2022 from WIRED: <https://www.wired.com/2014/09/military-grade-drone-can-printed-anywhere/>

Hammes, T. X. (2016, January 27). *Technologies Converge and Power Diffuses: The Evolution of Small, Smart, and Cheap Weapons*. Retrieved April 11, 2022 from Cato Institute: <https://www.cato.org/policy-analysis/technologies-converge-power-diffuses-evolution-small-smart-cheap-weapons>

Heine, V. (2013, September 16). *Merkel Campaign Event Visited by Mini Drone*. Retrieved April 11, 2022 from Spiegel: <https://www.spiegel.de/international/germany/merkel-campaign-event-visited-by-mini-drone-a-922495.html>

Kallenborn, Z. (2019, September 9). 174. *A New Age of Terror: The Future of CBRN Terrorism*. Retrieved April 11, 2022 from Mad Scientist Laboratory: <https://madsciblog.tradoc.army.mil/174-a-new-age-of-terror-the-future-of-cbrn-terrorism/>

Koslow, T. (2016, December 6). *Concerns Mount Over ISIS Making 3D Printed Bombs*. Retrieved April 11, 2022 from All3DP: <https://all3dp.com/3d-printed-bombs-isis/>

Lichfield, J. (2014, November 9). *French government on high alert after unexplained drone flights over nuclear power stations | The*

*Independent*. Retrieved April 11, 2022 from The Independent: <https://www.independent.co.uk/news/world/europe/french-government-on-high-alert-after-unexplained-drone-flights-over-nuclear-power-stations-9850138.html>

NDU Press. (2016, April 26). *Cheap Technology Will Challenge US Tactical Dominance – Analysis*. Retrieved April 11, 2022 from Eurasia Review: <https://www.eurasiareview.com/26042016-cheap-technology-will-challenge-us-tactical-dominance-analysis/>

Pavey, A. (2021, March 26). *Bioprinting: a myriad of (t)issues – Science Entrepreneur Club*. Retrieved April 11, 2022 from The Science Entrepreneur Club: <https://www.science-entrepreneur.com/blog-1/bioprinting-a-myrriad-of-tissues>

Quick, D. (2010, November 25). *Battlefield Extraction-Assist Robot to ferry wounded to safety*. Retrieved April 11, 2022 from New Atlas: <https://newatlas.com/battlefield-extraction-assist-robot/17059/>

Rassler, D., & al-‘Ubaydi, M. (2021, December 12). *Anticipating Future Directions of Tech-Enabled Terror*. Retrieved April 11, 2022 from Lawfare Blog: <https://www.lawfareblog.com/anticipating-future-directions-tech-enabled-terror>

RUTGERS UNIVERSITY. (2021, December 10). *New Cyber Protections Against Stealthy “Logic Bombs” Targeting 3D Printed Drones, Prostheses and Medical Devices*. Retrieved April 11, 2022 from SciTechDaily: <https://scitechdaily.com/new-cyber-protections-against-stealthy-logic-bombs-targeting-3d-printed-drones-prostheses-and-medical-devices/>

Shattuck Ph.D., C. G. (2020, March 12). *Transitioning to Autonomy: A Human Systems Integration Perspective*. Retrieved April 11, 2022 from Human Systems Integration Division: <https://human-factors.arc.nasa.gov/workshop/autonomy/download/presentations/Shaddock%20.pdf>

Thomas, A. (2008, June 20). *Army Partners with Academia for Emergence of New Technology*. Retrieved April 11, 2022 from Army.mil: <https://www.army.mil/article/10227/>

army\_partners\_with\_academia\_for\_emergence\_of\_new\_technology

Topolsky, J. (2008, May 4). *Bug-bot video reveals swarming drones, extreme rocking*. Retrieved April 11, 2022 from Engadget: <https://www.engadget.com/2008-05-04-bug-bot-video-reveals-swarming-drones-extreme-rocking.html>

U.S. Department of Defense. (2001, April 12). *Department of Defense Dictionary of Military and Associated Terms*. Retrieved April 11, 2022 from JITC – Homepage: <https://jitc.fhu.disa.mil/>

U.S. NRC. (2011, August 2). *US Airways Case Study 2, US Airways Flight 1549: Forced Landing on Hudson River*. Retrieved April 11, 2022 from Nuclear Regulatory Commission: <https://www.nrc.gov/docs/ML1122/ML11228A218.pdf>

Watkin, H. (2016, July 6). *Crazy Futuristic “Chemputer” Could Grow Drones*. Retrieved April 11, 2022 from All3DP: <https://all3dp.com/chemically-grow-drones-3d-printing/>

Woollaston, V. (2014, March 28). *Researchers successfully build and fly a low-cost DISPOSABLE drone*. Retrieved April 11, 2022 from Daily Mail: <https://www.dailymail.co.uk/sciencetech/article-2591533/Cheap-3D-printed-drones-coming-Researchers-successfully-build-fly-low-cost-DISPOSABLE-aircraft.html>

# 18. Practical Crime Scene Investigation (CSI) Using Autonomous Systems

**By Wayne D. Lonstein Esq. & Dr. Hans C. Mumm**

## **Student Learning Objectives**

The student will gain knowledge of the concepts and framework related to the use of autonomous systems to enhance crime scene investigations.

This chapter will include the challenges of crime scene airspace and the evidentiary collection and accepted use during the prosecution phase of criminal cases.

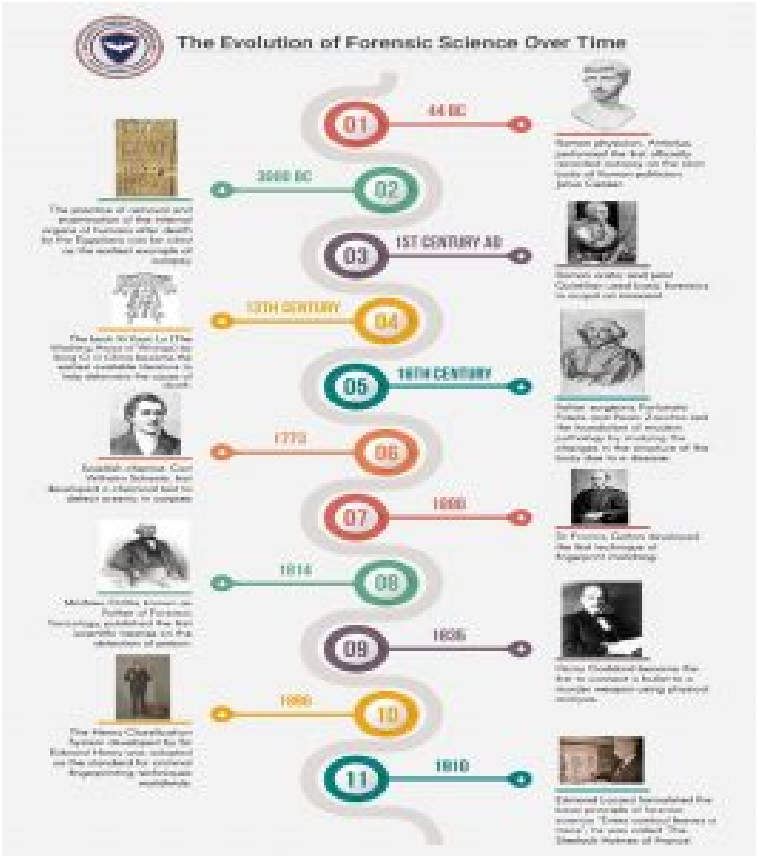
## **A Look Back at the Science of Crime Scene Investigation (CSI)**

It has been said that “modern crime scene investigators combine the logic of fictional detective Sherlock Holmes with advanced scientific techniques in identifying and processing evidence.” (Franklin, 2020)

The historical perspective of CSI starts with an understanding that forensic science is most often associated within the legal system as “the **application of scientific methods and principles to questions of law**. Or, in layman’s terms, forensic science is a discipline used by a forensic investigator to solve crimes.” (Exploring The History Of Forensic Science Through The Ages, 2022)

Antistius, a Roman physician of Julius Caesar, completed the first autopsy. During the 12th Century, the Chinese were credited with “being the first to attempt to define the difference between natural death and Criminal intent.” (Exploring The History Of Forensic Science Through The Ages, 2022)

Figure 18.1. A Timeline of the History of Forensic Science



Source: (Exploring The History Of Forensic Science Through The Ages, 2022)

Today crime scene investigation is an organized activity using the “solid foundation developed over thousands of years of forensic investigation. Modern forensics built upon these technologies and

expanded their application to include computer forensics, DNA forensics, entomological (insect) forensics, and enhanced biological studies. Crime scene investigation continues to experience rapid technological advancements". (Taylor, 2018)

### **Challenges of CSI in Hot Zones-Why Not Use Robots?**

Historically, crime scene evidence collection has been done only by humans; however, with advancing robotics, sensors, and the ability to demonstrate to courts that the evidence was collected to today's standards or higher, why would we not use this technology?

Currently, seven autonomous systems are recognized: unmanned aircraft systems (UAS) (drones), unmanned ground vehicles (UGV), unmanned underwater vehicles (UUV), unmanned surface vessels (USV), humanoids, cyber, and exoskeletons. In light of the past few years of a worldwide pandemic, we now must add "nano biologics" to this list and recognize eight autonomous systems. All can do an incredible amount of good for the human race while recognizing they can all be used in evil ways, creating great harm to humanity, our planet, and our future.

This chapter will narrow the focus to examine the use of UAS (with a USV variant) and USV in CSI CBNRE (chemical, biological, nuclear, radiological, and explosive). The idea behind unmanned systems is to allow these machines to handle dull, dirty, and dangerous situations for humans, contrary to deploying a human, who must be decontaminated after going into a hot zone. Dr. David Cullen summed up the CBNRE threat by stating:

**CBRN(E) weapons are becoming more frequent and increasingly lethal globally. Future military operations are envisioned to be more diverse, contested across all domains, and require rapid decision-making to enable decisive maneuver. Defense forces must sense hazards more rapidly, at a greater speed, increase stand-off distance, and share intelligence faster throughout the formation. (Cullen, 2021)**

In a hot zone, decontamination may not be advised depending on the contaminants in the environment. The disposal of the unmanned system might be a better option, as all of the collected CSI information will have been downloaded, cataloged, and stored. Autonomous systems can be easily sanitized before entering a crime scene, and their movements are recorded and cataloged. In contrast, their movements are more precise throughout a crime scene than a human. This becomes critical as it is “simply impossible for anyone to enter a location without changing it somehow, either by bringing something to it or removing something from it. The latter statement is known as the Locard Exchange Principle.” (Fisher, 2000)

Consider the search for corpses after a CBNRE incident. Autonomous systems can be relatively low cost, allowing for a scene’s saturation and an extensive jurisdiction with minimal manning requirements. These systems are “easy to operate, and can be used in a wider variety of environments and closer proximities, but they are limited in the camera load they can carry. Airspace regulations often restrict them to the line of sight flights.” (Butters, 2021)

Traditional methods of cadaver detection in outdoor environments include manual ground search, cadaver dogs, and manned aerial reconnaissance during daylight. However, these methods have limitations; a potential low-cost alternative may be to employ thermal imaging equipment mounted on an unmanned aerial vehicle (UAV) to detect heat emitted by insects and bacterial activity on the decomposing remains. (Butters, 2021)

The ability of autonomous systems to augment, supplement and assist in CBNRE incidents is just being explored. Multiple autonomous systems can integrate and team to gather evidence in several new, efficient, and effective ways unavailable in years past.

### **Autonomous Systems Technology to Augment Human CSIs**

In May 2017, the Dubai police swore in the first law enforcement robot; the first Robocop model is a citizen-friendly, helpful version.



The follow-on version is more advanced as they are “immune from diseases and viruses; hence, nor can they feel hungry or thirsty. For this reason, they have already proven ideal for rescue missions — already they serve in bomb disposal — or, for example, in radioactive or chemically contaminated areas”. (Robocop becomes real-world: robot law enforcement in Dubai may bring Robocop to a neighborhood near you, 2017)

**Figure 18.2 Law enforcement humanoid in Dubai shopping mall**



Source: (“Robocop becomes real-world: robot law enforcement in Dubai may bring Robocop to a neighborhood near you,” 2017).

**Figure 18.3 Law enforcement humanoid in a public space**



Source: (“Robocop becomes real-world: robot law enforcement in Dubai may bring Robocop to a neighborhood near you,” 2017).

The concept of purpose-built autonomous systems to augment and assist CSIs is a logical next step for law enforcement as crime rates continue to climb and our criminal justice systems are overworked. Autonomous systems can help in reducing unwanted errors from overworked officers.

The importance of CSI has only grown over the years; however, “police handling many cases can find one case blurs into another—a very human reaction,” which offers more reasons for autonomous systems to augment human CSIs. (Fisher, 2000)

Today, CSI is an “umbrella term often used to refer to various methods and techniques applied during a criminal investigation. Focused on discovering, recovering, and processing evidence, crime scene investigation applies reasoned principles to pursue truth”. (Franklin, 2020) Small steps forward, starting with tried-and-true UAVs (with a USV variant) and UGVs, would allow testing of evidence collection, storage, chain of custody, and data integrity without compromising the investigations.

Autonomous systems offer the capabilities that will extend the

range of evidence collection and hopefully assist in higher rates of prosecutions. An autonomous system can have “onboard UAV cognition capabilities for understanding and interacting in environments with imprecise or partial observations, for objects of interest within complex scenes.” (Sandino, 2021) This increase in cognitive depth “allows (s) UAVs to collect more accurate victim coordinates than the baseline planner. Adding the proposed system to UAVs improves robustness against potential false positive readings of detected objects caused by data noise, inaccurate detections, and elevated complexity to navigate time-critical applications.” (Sandino et al., 2021)

### **Virtual Reality-Teaching and Learning in Crime Scene Investigations**

Virtual reality (V.R.) and augmented reality (A.R.) have been used in gaming. This technology is now being implemented in several training environments, from driving, flying, and shooting simulator to law enforcement and military training scenarios. Research has been done in a multi-disciplinary study where a “V.R. crime scene app was designed and implemented, after which both undergraduate student tested it and staff/postgraduate student cohorts...demonstrate(d) that V.R. applications support learning of practical crime scene processing skills.” (Mayne, 2020)

The need to train and hone the skills of experienced CSI and now autonomous systems will benefit from a 3D world whose graphical resolution and frame rates can approach those of ‘real life’ and hence offer an immersive and worthwhile experience...VR-based practical sessions have the potential to add value to forensic science courses through offering cost-effective practical experience (and) the ability to work in isolation and a variety of different scenarios (Mayne, 2020)

### **CBNRE Scenes-Terrorist Attack or Accident-Autonomous Systems Can Help**

Combining air and ground autonomous systems offers new ways

to employ CSI in CBNRE scenes. The ability of the autonomous systems to not only integrate and team together as machines can now be expanded to manned-unmanned teaming arrangements known as MUM-T, with the trust factor being created with a “conceptual architecture for making humans, cyber systems, and physical systems working together in optimal complementarity by taking advantage of the strengths of both human intelligence and machine intelligence.” (Bousdekis, 2020) The idea behind these teams of humans and machines assists in addressing “the challenge of prolonged autonomous navigation within environments, for which a limited amount of information is available before deployment.” (Papachristos, 2014) This concept can be adapted by law enforcement based on the success the United States military is seeing as “Manned-unmanned teaming (MUM-T) operations combine the strengths of each platform to increase situational awareness, allowing the armed forces to conduct operations that include combat support and intelligence, surveillance, and reconnaissance (ISR) missions.” (Iriarte, 2016)

Humans and machines can work in harmony, and an extensive study effort is currently underway to create this harmony which “provides the means to support human-AI symbiosis ecosystem and effectively manage the emerging generation of artificially intelligent partners, offering explainable value through automated reasoning aiming at assisting and facilitating the work of the Operator.” (Bousdekis, 2020)

Most UGVs are equipped with point detection sensors, ready to sample the environment to verify a CBNRE incident and collect evidence. In addition, the next generation of UGVs will offer “Integration and maximum use of stand-off sensing could reduce the potential risk of operators being exposed to CBRN hazards.” (Cullen, 2021).

Autonomous systems offer, in time, the ability to collect needed information without disturbing the crime scene to the extent humans do, no matter how careful humans are as “It is simply impossible for anyone to enter a location without changing it in

some way, either by bringing something to it or removing something from it. The latter statement is known as the Locard Exchange Principle. (Fisher, 2000)

Several variants of UGVs are available on the market; Figure 18.4 shows an example of the FLIR Centaur-medium-sized UGV, which provides a stand-off capability to detect, confirm, identify, and dispose of hazards. (Cullen, 2021)

**Figure 18.4 UGV assisting at an IED site**



Source: (Cullen, 2021)

Over the years, many different types of wireless controlled and wireless controlled UGVs offered bomb disposal units a way to deal with dangerous situations without putting humans at risk. The evolution of sensors, long-life batteries, data links, and advanced programming allows the exploration of using this technology in CBNRE environments to collect CSI data from prosecuting the crime. Table 18.1 below examines the Pros and Cons of using UGVs in CSI environments.

**Table 18.1 Pros & Cons of UGVs supporting CSI environments**

**Pros**

- Long dwell time
- High sensor & carrying capacity
- Ability to carry/drag humans to safety
- Less Disruption to crime scene

**CONs**

- Difficult maneuvering on stairs and complex environments
- Require “mapping” of building layout to function in autonomous mode
- Heavy and difficult to retrieve
- Limited field of view and situation awareness

UAVs offer several advantages at a crime scene. Rapid deployment and a different perspective of crime scenes allow for a more in-depth investigation and lines of inquiry that standard human height perspectives offer. Many police departments are already investigating the use and reliability of these systems, “The Royal Canadian Mounted Police started using Unmanned Aerial Vehicles to help them work on collision and crime scene investigation. It allows the investigations to be conducted under all weather conditions and provides broader views than the traditional procedures.” (UAVs Bring New Dimension In Crime Scene Investigation, 2021)

**Figure 18.5 Investigator using a UAV at a crime scene**  
**Examining UAV use in CSI-Crash Scene Photo Royal Canadian Mounted Police**



Source: (UAVs Bring New Dimension In Crime Scene Investigation, 2021)

Using the combination of image acquisition by UAV and mapping software, the UAV provides “a complete solution to reconstruct accident and crime scenes and solves vital issues not covered by traditional methods.” (“UAVs Bring New Dimension In Crime Scene Investigation,” 2021) Table 2 offers some Pros and Cons of using UAS technology at crime scenes.

**Table 18.2 Pros and Cons of UAS in a CSI environment**

**PROs**

Rapid deployment

Can operate in GPS denied environment

Sensor packages allow for a high level of situation awareness

Ability to easily use in a MUM-T operation and uncouple to return to independent operations

**CONS**

Rotor wash could disrupt crime scene, contaminating collection efforts

A high level of air movement could further disperse CBNRE

Limited weight carrying capacity-limits airtime and payloads

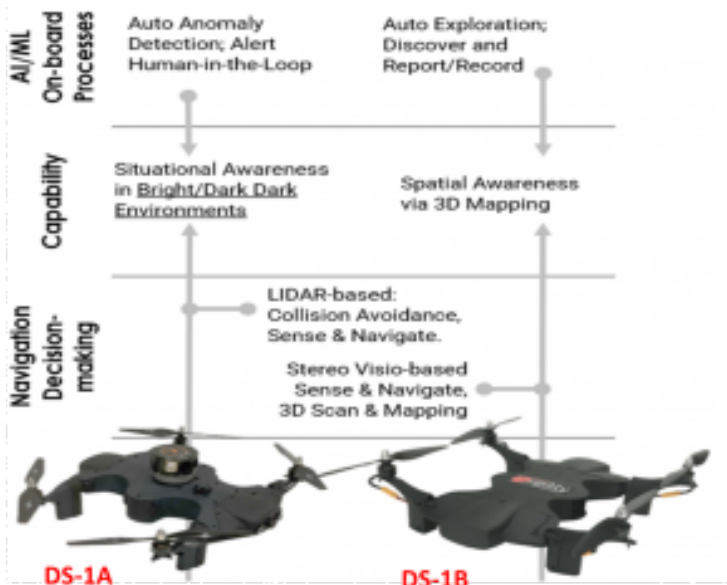
Limited to no ability to assist or move humans from danger

Source: (“UAVs Bring New Dimension In Crime Scene Investigation,” 2021)

Many crime scenes are indoors, commonly known as a GPS-denied environment. Several solutions are being worked on to deal with this limitation. For example, a UAS company, Airgility, in College Park, Maryland, is working on combining A.I. autonomous flight with a series of different size UAS that can operate in GPS-denied areas. This will allow “GPS-denied autonomy in confined spaces such as buildings and silos. As a result of the robotic operations and human-in-the-loop operability, a decision-making advantage is achieved via autonomous robotic workflow and edge-processed analytics.” (Valente, 2022). In addition, the DS-1 series “was developed for Department of Homeland Security (DHS) applications about flight autonomy for confined and harsh environments.” The onboard LIDAR allows the vehicle to understand its surroundings without a GPS signal. The vehicle can transition from GPS flight into a GPS-denied area allowing for greater flexibility in mission planning and use in the uncertainty of a crime scene, providing analytical feedback in real-time.

### **Figure 18.6. Side by Side Comparison of DS-1A and DS-1B UAVs**





Source: (Valente, 2022)

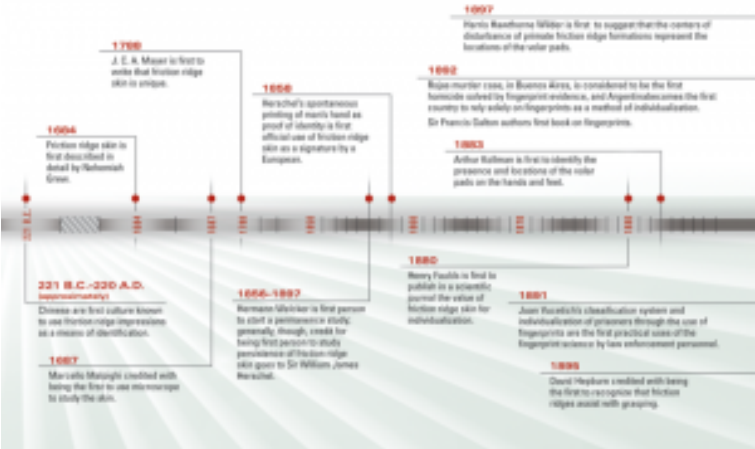
The concept of unmanned robotic teams” consisting of an aerial and a ground vehicle, and a power-tethering physical link between them, and proposes a strategy that addresses their collaborative navigation problem.” (Papachristos, 2014)

The rapid development of autonomous systems for law enforcement is directly related to their ability to be used in CBRNE environments with the expectation of “unmanned aerial vehicles of exceptional capabilities, unmanned ground vehicles as well as marine and hybrid autonomous robots...to exploit the operational advantages of different unmanned vehicle classes.” (Papachristos, 2014) Combining this with human teams and crime scene investigation in a CBNRE environment is the reality that will yield high-fidelity data for use in prosecuting these crimes.

# Legal Considerations for Autonomous Systems Use at a Crime Scene

According to the National Institute of Science and Technology, Forensic Science is “Forensic science is the use of scientific methods or expertise to investigate crimes or examine evidence that might be presented in a court of law.” (NIST, 2022) Since 1902 modern forensic science has embraced new technologies to assist in investigating crime beginning with fingerprints analysis in 1902 to the polygraph, voice, DNA, and widespread use of automated collection and analysis in the 21st Century. Just fingerprint technology alone has evolved from the ancient to the cutting edge and has accelerated by technological automation in the last half-century.

Figure 18.7 A Timeline of Fingerprint Firsts



Source: (Justice, 2014)

While it seems new technology is created for forensics each day, automation needs thorough examination before implementation. In the 1923 decision, *Frye v. the United States*, the United States Circuit Court for the District of Columbia established a rule for admitting expert testimony based upon technology or scientific information. The court wrote:

“When a scientific principle or discovery crosses the line between the experimental

And demonstrable stages are difficult to define. Somewhere in this twilight zone, the evidential force of the principle must be recognized. While courts will go a long way in admitting expert testimony deduced from a well-recognized scientific principle or discovery, the thing from which the deduction is made must be sufficiently established

to have gained general acceptance in the particular field in which it belongs.” (*Frye v. the United States*, 1923)

The intersection of forensic science and automated technology continually requires additional rules regarding the myriad of new and sometimes unproven, being admissible in courts. The Supreme Court of the United States provided an opinion regarding the “General Acceptance” rule established in *Frye*. In *Daubert v. Merrell Dow Pharmaceuticals* (*Daubert v. Merrell Dow Pharmaceuticals*, 1993), the Supreme Court issued new guidance relating to scientific evidence to trial courts. As a result, Federal Rule of Evidence 702 now requires the following factors to be laid as a foundation for scientific evidence:

FRCP 702: a witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:

(a) The expert’s scientific, technical, or other specialized knowledge will help the

the trier of fact to understand the evidence or to determine a fact in issue;

- (b) The testimony is based on sufficient facts or data;
- (c) The testimony is the product of reliable principles and methods, and;
- (d) The expert has reliably applied the principles and methods to the facts of the case. (Federal Rules of Evidence 702, 2000)

While some states still follow Frye's "General Acceptance" standard, most federal courts follow Rule 702. Individuals intending to be forensic examiners or subject matter experts must describe the significance of the evidence, explain how the technology works, and prove the process based upon scientific principles and methods. The forensic witness must show how the technology works and that the technology is considered scientifically reliable. In this particular case, the process, whether a blend of human and technology or solely automated, was conducted according to all established principles for that technology. It is not simply enough to testify about the results; the presenter must also demonstrate how it works and that all technology rules are meticulously followed.

Failure to satisfy these requirements can be devastating to the party relying upon the evidence. In the sensationalized 1994 case of *California vs. Orenthal James Simpson*, forensics took the world stage with multiple types of scientific evidence and expert testimony offered by the parties. (People of the State of California v. Orenthal James Simpson, 1995)

**Figure 18.8. Dr. Henry Lee, examining evidence**



Source: (Court TV, 1994)

Simpson's defense team called Dr. Lee to testify on behalf of Defendant O.J. Simpson. Dr. Lee's testimony created doubt in the jurors' minds that the Los Angeles Police Department failed to comply with foundational crime scene forensic rules, resulting in "untrustworthy" results. The defense called additional experts to testify that both the science was not "reliable" and the process of collecting evidence provided to the technology operator was tainted and therefore not sufficient to prove a case of intentional murder.

**Figure 18.9 Glove demonstration from the Simpson trial. The gloves did not fit.**



Source: (The 1995 Blog, 2020)

**Autonomous Evidence: If You Can't Explain It, Courts Will Not Allow It**

Whether manual, hybrid, or autonomous, forensic evidence collection, analysis, or conclusion; the forensic witness must be able to explain to the court:

1. How the technology works;
2. Establish that the science is reliable and accepted in the scientific community (Daubert v. Merrell Dow Pharmaceuticals, 1993);
3. Explain the requirements for a forensically sound collection of evidence;
4. The Crime Scene Analyst collected per the developer's specification;

5. The technology was tested for proper functioning before, during, and after the analysis; and
6. The results provided were under the normal functioning or process of the technology and acceptable ranges.

**Figure 18.10. Automated Speed Enforcement Technology**



Source: (Missouri Department of Transportation, 2018)

Forensic investigators should be ready to answer questions relating to what they did on a crime scene or what technology they used; they must explain how it functions. One need only look at the 2021 Kyle Rittenhouse murder trial in Kenosha, Wisconsin, as an example. As part of the prosecution's case, technology-enhanced drone video of the shooting was used as evidence. The court struggled to understand whether the technology changed or altered the video.

**Figure 18.11. Scenes from the Rittenhouse courtroom**



Source: (AP, 2021)

Upon questioning the court, the prosecution could not articulate how the technology worked and, more importantly, assure the court that the original content was unaltered instead of highlighted. Although the requirements of *Daubert & Frye* were eventually satisfied, the problem stemmed from the prosecution's inability and its' witnesses' inability to explain how the technology used to create it worked. The fact jeopardized the prosecution case and may have raised doubt in the jurors' minds, eventually acquitted Rittenhouse.

The takeaway is that no matter how well the technology performs, unless it can be explained "how it works" and "why it is reliable," the case can be jeopardized.

## Conclusions



Criminals and terrorists are not bound by any restrictions that hamper law enforcement; they are free to innovate and use technology, CBNRE, and other tactics required to obtain their goal. History dictates what is considered the use of technology “as the Reno gang “invented” train robbery in 1866, and Jesse James pioneered daylight bank robbery a few years later, so modern felons labor nonstop to take full advantage of new technology, seeking more efficient ways to beat the system and avoid detection in the process” (Newton, 2008).

It is time for autonomous systems to augment and integrate into crime scene investigation. The technology has matured to the point of certainty. The laws, policies, and governance should be updated to match the reality of the modern crime scene and the increasing use of CBNRE around the world. It has been said that “High-Tech crimes are defined by their era” (Newton, 2008), and we are living in the next evolution of crime as we seek Justice for crimes committed against our modern societies.

## **Questions**

1. Is there a difference between a human collecting crime scene data and an autonomous system?
2. CSI data is based on science. Do you think autonomous systems are better to augment a human CSI at a scene or replace the human?
3. List three considerations for airspace usage in using a UAV for CSI collection at a crime scene.
4. What legal ramifications could occur with using autonomous systems at a crime scene?
5. Name three ways the law enforcement community and a prosecutor could benefit from using autonomous systems at crime scenes.

## **Bibliography**

Bousdekis, A. A. (2020). A human cyber-physical system framework for operator 4.0 – artificial intelligence symbiosis. *Manufacturing Letters*, pp. 25, 10-15. doi:10.1016/j.mfglet.2020.06.001.

Butters, O. K. (2021). Application of forward-looking infrared (FLIR) imaging from an unmanned aerial platform in the search for decomposing remains. *Journal of Forensic Sciences*, pp. 66(1), 347-355. doi:10.1111/1556.

Cullen, D. (2021). *From A Distance*. Retrieved from [cbnw.co.uk/](https://cbnw.co.uk/): <https://cbnw.co.uk/from-a-distance-flir/>

*Exploring The History Of Forensic Science Through The Ages* . (2022). Retrieved from [//ifflab.org/](https://ifflab.org/): <https://ifflab.org/history-of-forensic-science/>

Fisher, B. A. (2000). *Techniques of crime scene investigation* (6th ed.). CRC Press.

Franklin, C. (2020). *Crime scene investigation*. In: Salem Press. Salem Press.

Iriarte, M. (2016). *MUM-T operations on the U.S. Army's UAS roadmap*. Retrieved from [militaryembedded.com/](https://militaryembedded.com/): <https://militaryembedded.com/unmanned/isr/mum-t-armys-uas-roadmap>

Justice, U. S. (2014). *The Fingerprint Sourcebook*. CreateSpace Independent Publishing Platform.

Mayne, R. &. (2020). Virtual reality for teaching and learning in crime scene investigation. *Science & Justice*, pp. 60(5), 466-472. doi:10.1016/j.scijus.2020.07.006.

Missouri Department of Transportation. (2018). *Automated Enforcement Survey*. Jefferson City, Missouri: Missouri Department of Transportation.

Newton, M. (2008). *The encyclopedia of crime scene investigation: Facts on File*.

NIST. (2022). *Definition of Forensic Science*. NIST / GPO.

Papachristos, C. &. (2014). *The power-tethered UAV-UGV team*:

A collaborative strategy for navigation in partially-mapped environments. Retrieved from 22nd Mediterranean Conference on Control & Automation, 1153-1158. : <https://search.ebscohost.com/1>

Robocop becomes real-world: robot law enforcement in Dubai may bring Robocop to a neighborhood near you. (2017). Retrieved from Robocop becomes real-world: robot law enforcement in Dubai may bring Robocop to a neighborhood near you. (2017). Retrieved from <https://www.ediweekly.com/robocop-becomes-real-world-robot-law-enforcement-dubai-may-bring-robocop-neighborhood-near/>: <https://www.ediweekly.com/robocop-becomes-real-world-robot-law-enforcement-dubai-may-bring-robocop-neighborhood-near/>

Sandino, J. M. (2021). Drone-Based Autonomous Motion Planning System for Outdoor Environments under Object Detection Uncertainty. *Remote Sensing. Remote Sensing*, pp. 13(21), 4481. doi:10.3390/rs13214481.

Taylor, S. (2018). *history-crime-scene-investigation*. Retrieved from [//careertrend.com/](https://careertrend.com/about-5371617-history-crime-scene-investigation.html): <https://careertrend.com/about-5371617-history-crime-scene-investigation.html>

The 1995 Blog. (2020). *Too tight': The botched glove demonstration at O.J.' Trial of the Century' in 1995*. Retrieved from The 1995 Bog: <https://1995blog.com/2020/06/12/recalling-botched-glove-demonstration-at-1995-o-j-simpson-trial-of-the-century/>

UAVs Bring New Dimension In Crime Scene Investigation. (2021). Retrieved from [www.dronethusiast.com](https://www.dronethusiast.com/uavs-bring-new-dimension-crime-scene-investigation/): <https://www.dronethusiast.com/uavs-bring-new-dimension-crime-scene-investigation/>

Valente, E. (2022). *Airgility*. Retrieved from [www.airgility.co/](https://www.airgility.co/): <https://www.airgility.co/>

# 19. Navigation Spoofing and ECD

**By Professor Randall K. Nichols, Kansas State University**

## **STUDENT OBJECTIVES**

Students will understand four concepts:

- 1) That UAS / drones are mobile deployment agents. They are capable of Cyber-Spoofing navigation signals in the air by acting as a rogue access point, HAPs unit, mobile malicious signal generator, or interference medium to the ground control, friendly airborne unit, CBRN asset, or any other mechanism/system requiring localization or position fix via GPS / GNSS,
- 2) That GPS spoofing detection and mitigation for GNSS / GPS systems can be solved using the brilliant ECD algorithm for detection, mitigation, and recovery,
- 3) ADS-B is a subset of the larger receiver localization problem. Solutions that apply to the larger vector space, GNSS / GPS, also are valid for the subset, ADS-B, if computational hardware is available.
- 4) ECD does not effectively handle that indoor or city, or canyon localization

## **NAVIGATION SPOOFING AND ECD**[\[1\]](#)[\[2\]](#)

### **SUMMARY**

GPS spoofing is a reasonably well-researched topic. Many methods have been proposed to detect and mitigate spoofing. The lion's share of the research focuses on detecting spoofing attacks. Methods of spoofing mitigation are often specialized or computational burdensome. Civilian COTS anti-spoofing countermeasures are rare. This chapter highlights the brilliant

value-added research by Dr. Manuel Eichelberger on the mitigation and recovery of GPS spoofing. (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019) ECD implementation and evaluation show that the robustness of collective detection (CD) can be exploited to mitigate spoofing attacks with some modifications. (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019) shows that multiple locations, including the actual one, can be recovered from scenarios in which several signals are present. Experiments based on the TEXTBAT database show that various attacks can be mitigated. In the TEXTBAT scenarios, an attacker can introduce a maximum error of 222 m and a median error under 19 m.[\[3\]](#) This is less than a sixth of the maximum unnoticed location offset reported in previous work that only detects spoofing attacks. (Ranganathan & al., 2016)

ECD does not track signals. It works with signal snapshots. It is suitable for snapshot receivers, which are a new class of low-power GPS receivers. (M.Eichelberger, 2019) (J. Liu & et al., 2012)

ADS-B's high dependency on communication and navigation (GNSS) systems causes the system to inherit the vulnerabilities of those systems. This results in more opportunities (threats) to exploit those vulnerabilities. Advancements in computers, connectivity, storage, hardware, software, and apps are major aids to malicious parties who wish to carry out spoofing and other threats by exploiting the vulnerabilities of ADS-B. Another main vulnerability of ADS-B systems is their broadcast nature without security measures, which can easily be exploited to cause harm.

**Definition: Spoofing – A Cyber-weapon attack that generates false signals to replace valid ones. GPS Spoofing is an attack to provide false information to GPS receivers by broadcasting counterfeit signals similar to the original GPS signal or by recording the original GPS signal captured somewhere else at some other time and then retransmitting the signal. The Spoofing**

**attack causes GPS receivers to provide the wrong information about position and time. (T.E. Humphrees, 2008) (Tippenhauer & et al., 2011) GPS Spoofed UAS / drones may deliver signals against any target ( CBRN assets included) that requires accurate position fix or localization.**

## **INTRODUCTION**

It is important to understand that both GPS (part of the GNSS family) and ADS-B systems are vulnerable to spoofing attacks on both manned and unmanned aircraft. In general, GPS vulnerabilities translate down to the more specific ADS-B subset, which has vulnerabilities in its own right. This report will detail the brilliant work of Dr. Michael Eichelberger on *Robust Global Localization using GPS and Aircraft Signals*. He describes a functional tool known as CD to detect, mitigate and counter spoofing (and jamming) attacks on all stages of GPS. (Eichelberger, *Robust Global Localization using GPS and Aircraft Signals*, 2019)

GPS is ubiquitous and is incorporated into so many applications (aircraft, ship, car /truck navigation; train routing and control; cellular network, stock market, CBRN assets, and power grid synchronization) that it makes a “rich” target for spoofing a receiver perceived location or time. Wrong information in time or space can have severe consequences.

ATC is partially transitioning from radar to a scheme in which aircraft (A/C) transmit their current location twice per second through ADS-B messages. This system has been mandated in Europe and has been well underway in the US since 2020. The A/C determine their location using GPS. If the onboard GPS receiver estimates a wrong location due to spoofing, wrong routing instructions will be delivered due to a wrong reported A/C location, leading to an A/C crash.

Ships depend heavily on GPS. They have few reference points to localize themselves apart from GPS. Wrong location indication can strand a ship, cause a collision, push off course into dangerous waters, ground a ship, or turn a ship into a ghost or a missile. Two

thousand seventeen incidents in the Black Sea and South China Seas have been documented. (Burgess, 2017) (Nichols R. K.-P., 2019)

While planes and ships suffer spoofing attacks in the location domain, an attacker may also try to change the perceived time of a GPS receiver. Cellular networks rely on accurate time synchronization to exchange data packets between ground antennas and mobile handsets in the same network cell. Also, all neighboring network cells need to be time-synchronized for seamless call handoffs of handsets switching cells and coordinating data transmissions in overlapping coverage areas. Since most cellular ground stations get their timing information from GPS, a signal spoofing attacker could decouple cells from the common network time. Overlapping cells might send data simultaneously and frequencies, leading to message collisions and losses. (Anonymous, 2014) Failing communications networks can disrupt emergency services and businesses. (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019)

## **SPOOFING**

Threats and weaknesses show that large damages (even fatal or catastrophic) can be caused by transmitting forged GPS signals. False signal generators may cost only a few hundred dollars of software and hardware.

A GPS receiver computing its location wrongly or even failing to estimate any location can have different causes. Wrong localization solutions come from 1) a low signal-to-noise ratio (SNR) of the signal (examples: inside a building or below trees in a canyon); 2) reflected signals in multipath scenarios, or 3) deliberately spoofed signals. (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019) discusses mitigating low SNR and multipath reflected signals. Signal spoofing (#3) is the most difficult case since the attacker can freely choose each satellite's signal power and delay individually. (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019)

*Before discussing ECD – Collective detection maximum likelihood*

*localization approach* (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019), it is best to step back and briefly discuss GPS signals, classical GPS receivers, A-GPS, and snapshot receivers. Then the ECD approach to spoofing will show some real power by comparison. Power is defined as both enhanced spoofing detection and mitigation capabilities. [4]

## **GPS SIGNAL**

The GPS system consists of a control segment, space segment, and user segment. The space segment contains 24 orbiting satellites. The network monitor stations, GCS, and antennas comprise the control segment. The third and most important are the receivers who make up the user segment. (USGPO, 2021)

Satellites transmit signals in different frequency bands. These include the L1 and L2 frequency bands at 1.57542 GHz and 1.2276 GHz. (DoD, 2008) Using code division multiple access protocols, signals from different satellites may be distinguished and extracted from background noise (CDMA). (DoD, 2008) Each satellite has a unique course/acquisition code (C/A) of 1023 bits. The C/A codes are PRN sequences transmitted at 10.23 MHz, which repeats every millisecond. The C /A code is merged using an XOR before being with the L1 or L2 carrier. The data broadcast has a timestamp called HOW, which is used to compute the location of the satellite when the packet was transmitted. The receiver needs accurate orbital information ( aka ephemeris) about the satellite, which changes over time. The timestamp is broadcast every six seconds; the ephemeris data can only be received if the receiver can decode at least 30 seconds of the signal.[5] (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019)

## **CLASSIC RECEIVERS**

Classical GPS receivers use three stages when obtaining a location fix. They are Acquisition, Tracking, and localization.

Acquisition. The relative speed between satellite and receiver introduces a significant Doppler shift to the carrier frequency.



[6] GPS receiver locates the set of available satellites. This is achieved by correlating the received signal with satellites' known C/A codes. Since satellites move at considerable speeds. The signal frequency is affected by a Doppler shift. So, the receiver must correlate the received signal with C/A codes with different Doppler shifts. (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019)

Tracking. After a set of satellites has been acquired, the data contained in the broadcast signal is decoded. Doppler shifts and C/A code phase are tracked using tracking loops. After the receiver obtains the ephemeris data and HOW timestamps from at least four satellites, it can compute its location. (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019)

Localization. Localization in GPS is achieved using signal time of flight (ToF) measurements. TVs are the difference between the arrival times of the HOW timestamps decoded in the tracking stage of the receiver and those signal transmission timestamps themselves. [7] The local time at the receiver is unknown, and the localization is done using pseudo ranges. The receiver location is usually found using least-squares optimization. (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019) (Wikipedia, 2021)

A main disadvantage of GPS is the low bit rate of the navigation data encoded in the signals transmitted by the satellites. The minimal data necessary to compute a location fix, which includes the ephemerides of the satellites, repeats only every 30 seconds. [8]

### **A-GPS (ASSISTED GPS) – REDUCING THE STARTUP TIME**

Assisted GPS (A-GPS) drastically reduces the startup time by fetching the navigation data over the Internet, commonly connecting via a cellular network. Data transmission over cellular networks is faster than decoding the GPS signals and normally only takes a few seconds. The ephemeris data is valid for 30 minutes. The acquisition time can be reduced using that data since the available satellites, and their expected Doppler shifts can be estimated. The

receiver still needs to extract the HOW timestamps from the signal with A-GPS. However, these timestamps are transmitted every six seconds, which translates to how long the A-GPS receiver takes to compute a location fix. (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019)

## **COURSE - TIME NAVIGATION**

Course-Time Navigation (CTN) is an A-GPS technique that drops the requirement to decode the HOW timestamps from the GPS signals. (Diggelen, 2009) The only information used from the GPS signals is the phases of the C/A code sequences detected by a matched filter. Those C/A code arrival times are unambiguously related to the sub-milliseconds; the deviation may be no more than 150 km from the correct values. [9] [10] Since the PRN sequences repeat every millisecond, without considering navigation data flips in the signal, CTN can, in theory, compute a location from one millisecond of the sampled signal. [11] Noise can be an issue with such short signal recordings because it cannot be filtered out the same way with longer recordings of several seconds. The big advantage is that signal processing is fast and power-efficient and reduces the latency of the first fix. Since no metadata is extracted from the GPS signal, CTN can often compute a location even in the presence of noise or attenuation. (Diggelen, 2009)

## **SNAPSHOT RECEIVERS**

Snapshot receivers aim at the remaining latency that results from the transmission of timestamps from satellites every six seconds. Snapshot receivers can determine the satellite modulo 1 ms ranges, which corresponds to 300 km.

## **COLLECTIVE DETECTION**

**Collective Detection (CD)** is a maximum likelihood snapshot receiver localization method, which does not determine the arrival time for each satellite but rather combines all the available information and decides only at the end of the computation. [12]

This technique is critical to the (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019) invention to mitigate spoofing attacks on GPS or ADS-B. CD can tolerate a few low-quality satellite signals and is more robust than CTN. CD requires a lot of computational power. CD can be sped up by a branch and bound approach, which reduces the computational power per location fix to the order of one second even for uncertainties of 100 km and a minute. CD improvements and research has been plentiful. (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019) (J.Liu & et.al., 2012) (Axelrod & al, 2011) (P. Bissag, 2017)

### ECD

Returning to the spoofing attack discussion, Dr. Manuel Eichelberger's CD – *Collective detection maximum likelihood localization approach*, **his method not only can detect spoofing attacks but also mitigate them!** The ECD approach is a robust algorithm to mitigate spoofing. ECD can differentiate closer differences between the correct and spoofed locations than previously known approaches. (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019) COTS has little spoofing integrated defenses. Military receivers use symmetrically encrypted GPS signals, subject to a “replay” attack with a small delay to confuse receivers.

ECD solves even the toughest type of GPS spoofing attack, consisting of spoofed signals with power levels similar to the authentic signals. (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019) ECD achieves median errors under 19 m on the TEXBAT dataset, the de-facto reference dataset for testing GPS anti-spoofing algorithms. (Ranganathan & al., 2016) (Wesson, 2014) The ECD approach uses only a few milliseconds worth of raw GPS signals, so-called snapshots, for each location fix. This enables offloading of the computation into the Cloud, allowing knowledge of observed attacks. [13] Existing spoofing mitigation methods require a constant stream of GPS signals and tracking those signals over

time. Computational load increases because fake signals must be detected, removed, or bypassed. (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019)

## **RESEARCH TO 2016: SURVEY OF EFFECTIVE GPS SPOOFING COUNTERMEASURES**

Researchers have been trying to find a complete solution to meet the spoofing threat because of the overwhelming dependence on GPS in every sector, ranging from civilian to military. To understand that ECD ( following sections) is a brilliant departure from past efforts, briefly covering the prevailing common wisdom is necessary. Haider and Khalid 2016 published an adequate survey of spoofing countermeasures up through 2016. (Haider & Khalid, 2016)

### **Spoofing Techniques**

According to (Haider & Khalid, 2016), there are three common GPS Spoofing techniques with different sophistication levels. They are simplistic, intermediate, and sophisticated. (Humphreys & al., 2008)

The *simplistic spoofing attack* is the most commonly used technique to spoof GPS receivers. It only requires a COTS GPS signal simulator, amplifier, and antenna to broadcast signals to the GPS receiver. It was performed successfully by Los Alamos National Laboratory in 2002. (Warner & Johnson, 2002) Simplistic spoofing attacks can be expensive as the GPS simulator can run \$400K and is heavy (not mobile). The available GPS signal does not synchronize simulator signals, and detection is easy.

In the *intermediate spoofing attack*, the spoofing component consists of a GPS receiver to receive a genuine GPS signal and a spoofing device to transmit a fake GPS signal. The idea is to estimate the target receiver antenna position and velocity and then broadcast a fake signal relative to the genuine GPS signal. This type of spoofing attack is difficult to detect and can be partially prevented by using an IMU. (Humphreys & al., 2008)

In sophisticated spoofing attacks, multiple receiver-spoofers target the GPS receiver from different angles and directions. The angle-of-attack defense against GPS spoofing in

which the angle of reception is monitored to detect spoofing fails in this scenario. The only known defense successful against such an attack is cryptographic authentication. (Humphreys & al., 2008) [14]

Note that prior research on spoofing was to *exclude* the fake signals and focus on a single satellite. ECD ( next section) *includes* the fake signal on a minimum of four satellites and then progressively / selectively eliminates their effect until the real *weaker* GPS signals become apparent. (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019)

According to (Haider & Khalid, 2016), six innovative research papers cover spoofing countermeasures.

1. Multi-test Detection and Protection Algorithm against Spoofing Attacks on GNSS Receivers (Jovanovic & Botteron, 2014)

The CM presented in this paper relies on statistical properties of the GPS signal, signal power level, Doppler frequency offset, and carrier to noise ratio. [15] The method monitors the above statistical properties and checks for inconsistencies to detect the presence of a GPS spoofer signal. The test results show that the proposed CMs can successfully detect the presence of the GPS fake signal with a low probability of false alarm. Once the spoofed signal is detected, the method offers a protection module ( once the spoofed signal is detected). The tracking history is further evaluated to re-establish the lock on the correct signal. This method only works against simplistic spoofer attacks. However, it is cost-effective as it requires only changes to the classic GNSS receiver, not the whole GPS infrastructure. (Jovanovic & Botteron, 2014)

#### **GPS Spoofing Countermeasures (Warner & Johnston, 2003)**

This paper is good for anyone interested in learning about GPS spoofing CMs, but the techniques discussed were general, not specific. The effectiveness of the approaches and strategies to defend against spoofing mentioned cannot be measured because no tests were performed to evaluate the methods presented. None of

the presented methods were implemented in the field. The majority of strategies discussed were based on the monitoring of signal properties. (Haider & Khalid, 2016)

#### **An Asymmetric Security Mechanism for Navigation Signals (Kuhn, 2015)**

The method described in Kuhn is based on cross-correlation and short-term information processing.[\[16\]](#) It is proposed that each satellite transmitter will transmit a signal known as a hidden mark signal at regular intervals of time with a power level lower than the receiver noise level. After each mark signal transmission, a signed ( encrypted) data signal is transmitted with a power level above the receiver noise level. GPS receivers can only assess the hidden mark signal after receiving the signed data signal. This approach is best for a spoofed-replayed attack. The crystal oscillators inside classic GPS receivers can easily measure the delay between the data signal and the hidden mark signal despite being less than accurate compared to the satellite's onboard atomic clocks. The method fails for multiple spoofer antennas. (Kuhn, 2015)

#### **A Cross-layer defense mechanism against GPS spoofing attacks on PMUs in Smart Grid (Fan & al., 2015)**

The CM described a method to protect the electrical grid PMUs from possible GPS spoofing attacks. The protection method consists of cross-layer protection. The first layer (physical) receives signals from hybrid antennas and then measures the AOA of the signals of all the GPS receivers. AOA will be the same as a GPS receiver if sourced at the same satellite. Spoofed signals will have a different AOA. The second layer ( upper layer) receives input from the physical layer and then uses state-based estimation techniques to detect bad data. The technique is feasible and only requires an additional GPS receiver and antenna. The method works against simple and intermediate attacks. (Fan & al., 2015)

#### **Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing (Magiera & Katulski, 2015)**

This paper focuses on a CM that uses spatial processing. It tests

well for both detection and reducing the impact of spoofed receivers. The method uses multiple antennas for reception and combines with the AOA approach. The phase delay measurement is used to distinguish the fake and authentic signals. The accuracy of the CM was tested when 4–8 spoofed signals were in play. Accuracy prediction was 99% when carrier to noise ratio was at least 46 dB Hz. (Magiera & Katulski, 2015)

#### **GPS Spoofing Detection via Dual-Receiver Correlation of Military Signals(Psiaki & al., 2013)**

The authors proposed a cross-layer detection mechanism to detect multiple spoofing attacks against the smart grid. In the physical layer, an AOA-based mechanism is employed. The distribution of the normal to spoofed standard deviation of the difference of the C/No from different antennas is calculated. The prior probability of spoofing is calculated and fed into the upper layer for further detection. In the upper layer, a Kalman filter is applied to estimate the state of the power system and use the measurement error to calculate the trustworthiness value of being spoofed. The information is all combined and correlated / integrated into the cross-layer mechanism. Results have been posted well, but computation time is high. (Psiaki & al., 2013)

#### **A-F ANALYSIS (Haider & Khalid, 2016)**

Table 19.1, reprinted from (Haider & Khalid, 2016), shows the criteria used to evaluate each technique to find the most effective GPS spoofing CM. Table 19.2, reprinted from (Haider & Khalid, 2016), presents an A-F analysis concerning the criteria outlined in Table 19.1.

From Table 19.2, we can discern that almost all the techniques can offer protection against a simplistic spoofing attack (Kuhn, 2015) (Jovanovic & Botteron, 2014) (Fan & al., 2015) (Magiera & Katulski, 2015) (Psiaki & al., 2013). Only two techniques can offer protection against sophisticated types of attacks (Kuhn, 2015) (Psiaki & al., 2013). This represents a reasonable look at the state-of-the-art GPS spoofing CMs in 2016.

Then along comes Dr. Manuel Eichelberger and ECD!

Table 19.1& 19.2 Effectiveness Criteria

| TABLE I: Effectiveness Criteria             |  |   |  |  |  |  |  |  |                 |  |  |
|---|--|---|--|--|--|--|--|--|-----------------|--|--|
| Criteria                                    |  | Description   |  |  |  |  |  |  | Possible Values |  |  |
| Quick Implementation                        |  | Ability to apply the technique quickly and in an extensible manner          |  |  |  |  |  |  | Yes/No          |  |  |
| Cost effective                              |  | Cost effective for small-scale or large number of operations                |  |  |  |  |  |  | Yes/No          |  |  |
| Resistant to Simple Attacks                 |  | Ability to detect simple attacks  |  |  |  |  |  |  | Yes/No          |  |  |
| Resistant to Intermediate Attacks           |  | Ability to detect intermediate types of attacks                             |  |  |  |  |  |  | Yes/No          |  |  |
| Resistant to Sophisticated Attacks          |  | Ability to detect sophisticated and advanced types of attacks               |  |  |  |  |  |  | Yes/No          |  |  |
| Requires Changes to existing infrastructure |  | Requires changes to existing infrastructure for implementation of technique |  |  |  |  |  |  | Yes/No          |  |  |
| Requires changes to existing hardware       |  | Requires changes to hardware for implementation of technique                |  |  |  |  |  |  | Yes/No          |  |  |
| Requires changes to existing software       |  | Requires changes to software for implementation of technique                |  |  |  |  |  |  | Yes/No          |  |  |
| Requires changes to existing network        |  | Requires changes to network for implementation of technique                 |  |  |  |  |  |  | Yes/No          |  |  |
| Requires changes to existing system         |  | Requires changes to system for implementation of technique                  |  |  |  |  |  |  | Yes/No          |  |  |

| TABLE II: Analysis of spoofing techniques (A-F) in effectiveness criteria |  |                        |                |                             |                                   |                                    |   |                                       |                                       |                                      |                                     |
|---|--|------------------------|----------------|-----------------------------|-----------------------------------|------------------------------------|---|---------------------------------------|---------------------------------------|--------------------------------------|-------------------------------------|
| A/F   | Technique  | Effectiveness Criteria |                |                             |                                   |                                    |   |                                       |                                       |                                      |                                     |
|   |  | Quick Implementation   | Cost effective | Resistant to Simple Attacks | Resistant to Intermediate Attacks | Resistant to Sophisticated Attacks | Requires Changes to existing infrastructure | Requires changes to existing hardware | Requires changes to existing software | Requires changes to existing network | Requires changes to existing system |
| 1   | Multi-sensor Detection and Prediction Algorithm against Spoofing Attacks on GPS Datastream | Yes                    | Yes            | Yes                         | No                                | No                                 | No  | Yes                                   | No                                    | Yes                                  | No                                  |
| 2   | An Adaptive Security Mechanism for Navigation Signals                                      | No                     | No             | Yes                         | Yes                               | Yes                                | Yes   | Yes                                   | No                                    | No                                   | No                                  |
| 3   | A Cross-Layer Defense Mechanism against GPS Spoofing Attacks on PNT in Urban Area          | Yes                    | Yes            | Yes                         | Yes                               | No                                 | No  | No                                    | No                                    | No                                   | Yes                                 |
| 4   | Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing                 | No                     | Yes            | Yes                         | Yes                               | No                                 | No  | No                                    | Yes                                   | Yes                                  | Yes                                 |
| 5   | GPS Spoofing Detection via Dual Receiver Correlation of Military Signals                   | No                     | No             | Yes                         | Yes                               | Yes                                | No  | No                                    | Yes                                   | No                                   | Yes                                 |

Source: Courtesy of (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019) Table 19.1, reprinted from Table I (Haider & Khalid, 2016), shows the criteria used to evaluate each technique to find the most effective GPS spoofing CM. Table 19.2, reprinted from Table II (Haider & Khalid, 2016), presents an A-F analysis concerning the criteria outlined in Table 19.1.

GPS SPOOFING RESEARCH: OUT OF THE BOX BRILLIANCE TO ECD DEFENSE

Three research tracks are most relevant to ECD / CD: Maximum Likelihood Localization, Spoofing Mitigation algorithms, and Successive Signal Interference Cancellation (SIC). Note that historical spoofing research focuses primarily on detecting singular



SPS source attacks. The focus on mitigation, correction, and recovery attending to multiple spoofing signals on multiple satellite attack surfaces is the hallmark of ECD.

### **Maximum Likelihood Localization**

CD is a maximum likelihood GPS localization technique. It was proposed in 1996 but considered computationally infeasible at that time. (Spilker, 1996) CD was first implemented by Axelrad et al. in 2011. (Axelrod & al, 2011) The search space contained millions or more location hypotheses. Improvements in the computational burden were found using various heuristics. (Cheong & al., 2011) (Jia, 2016) A breakthrough came with the proposal of a branch-and-bound algorithm that finds the optimal solution within ten seconds running on a single CPU thread. (P. Bissag, 2017)

### **Spoofing Mitigation**

GPS spoofing defenses have intensively been studied. Most of them focus on detecting spoofing attacks. There is a paucity of prior research for spoofing mitigation and recovering from successful attacks by finding and authenticating the correct signals. (M.L. Psiaki & Humphreys, 2016) In contrast to the extensive research on GPS spoofing, there is a lack of commercial, civil receivers with anti-spoofing capabilities. (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019) ECD inherently mitigates spoofing attacks.

Spoofing hardware performing a *sophisticated, seamless satellite-lock takeover* attack has been built. (Humphreys & al., 2008) Challenges associated with spoofing are matching the spoofed and accurate signals' amplitudes at the receiver, which might not be in LOS and moving. (Schmidt & al, 2016)

It is practically feasible for a spoofer to erase the authentic signals at a 180-degree phase offset. (M.L. Psiaki & Humphreys, 2016) This is one of the strongest attacks that can only be detected with multiple receiver antennas or a moving receiver. (M.L. Psiaki & Humphreys, 2016) The spoofer needs to know the receiver location more

accurately than the GPS L1 wavelength, 19 cm, for signal erasure to be feasible. Receivers with only a single antenna cannot withstand such an erasure attack. ECD targets single-antenna receivers and does not deal with signal erasure. (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019) The original signals are still present in all other spoofing attacks, including signal replay and multiple transmission antenna implementations, and ECD remains robust. (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019) Detecting multi-antenna receivers and differentiating signal timing consistencies are covered in (Tippenhauer & et al., 2011)

The GPS anti-spoofing work most relevant to ECD is based on the joint processing of satellite signals and the maximum likelihood of localization. One method can mitigate a limited number of spoofed signals by vector tracking of all satellite signals. (Jafarnia-Jahromi & al., 2012) A similar technique is shown to be robust against jamming and signal replay. (Y. Ng & Gao, 2016)

### **Successive Signal Interference Cancellation [17]**

ECD uses an iterative signal damping technique with spoofing signals similar to SIC. SIC removes the strongest received signals to find the weaker signals and has been used with GPS signals before. (G. Lopez-Risueno & Seco-Granados, 2005) (Madhani & al., 2003) That work is based on a classical receiver architecture which only keeps a signal's timing, amplitude, and phase. The ECD has its own snapshot receiver based on CD, which directly operates in the localization domain and does not identify individual signals in an intermediate stage. It is impossible to differentiate between authentic and spoofed signals, *a priori*, ECD does not remove signals from the sample data. Otherwise, the localization algorithm might lose the information from authentic signals/ Instead, ECD dampens strong signals by 60% to reveal weaker signals. This can reveal localization solutions with lower CD likelihood. (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019)

## **GPS Signal Jamming**

The easiest way to prevent a receiver from finding a GPS location is by jamming the GPS frequency band. GPS signals are weak and require sophisticated processing to be found. Satellite signal jamming considerably worsens the satellite signal acquisition results' signal-to-noise ratio (SNR). ECD algorithms achieve a better SNR than classical receivers and tolerate more noise or stronger jamming. (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019)

A jammed receiver is less likely to detect spoofing since the original signals cannot be accurately determined. The receiver tries to acquire any satellite signals it can find. The attacker only needs to send a set of valid GPS satellite signals stronger than the noise floor without synchronizing with authentic signals. [18] (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019)

There is a more powerful and subtle attack on top of the jammed signal. The spoofer can send a set of satellite signals with adjusted power levels and synchronize to the authentic signals to successfully spoof the receiver. (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019) So even if the receiver has countermeasures to differentiate the jamming, the spoofer signals will be accepted as authentic. (Nichols R. K., 2020)

## **Two Robust GPS Signal Spoofing Attacks and ECD**

Two of the most powerful GPS signal spoofing attacks are Seamless Satellite-Lock Takeover (SSLT) and Navigation Data Modification (NDM). How does ECD perform against these?

### **Seamless Satellite-Lock Takeover (SSLT)**

The most powerful attack is a *seamless satellite-lock takeover*. The original and counterfeit signals are nearly identical in such an attack concerning the satellite code, navigation data, code phase, transmission frequency, and received power. This requires the attacker to know the location of the spoofed device precisely so that ToF and power losses over a distance can be factored in. After

matching the spoofed signals with the authentic ones, the spoofer can send its signals with a small power advantage to trick the receiver into tracking those instead of the authentic signals. A classical receiver without spoofing countermeasures, like tracking multiple peaks, cannot mitigate or detect the SSLT attack, and there is no indication of interruption of the receiver's signal tracking. (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019)

### **Navigation Data Modification (NDM)**

An attacker has two attack vectors: modifying the signal's code phase or *altering the navigation data*—the former changes the signal arrival time measurements. The latter affects the perceived satellite locations. Both influence the calculated receiver location. ECD works with snapshot GPS receivers and is not vulnerable to NDM changes as they fetch information from other sources like the Internet. ECD deals with modified, wireless GPS signals.

### **ECD ALGORITHM DESIGN**

ECD is aimed at single-antenna receivers. Its spoofing mitigation algorithm object is to identify all likely localization solutions. It is based on CD because 1) CD has improved noise tolerance compared to classical receivers, 2) CD is suitable for snapshot receivers, 3) CD is not susceptible to navigation data modifications, and 4) CD computes a location likelihood distribution which can reveal all likely receiver locations including the actual location, independent of the number of spoofed and multipath signals. ECD avoids spoofing pitfalls and signal selection problems by joining and transforming all signals into a location likelihood distribution. Therefore, it defeats the top two GPS spoofing signal attacks. (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019)

Relating to the 4th point, spoofing and multipath signals are similar from a receiver's perspective. Both result in several observed signals from the same satellite. The difference is that multipath

signals have a delay-dependent on the environment, while spoofing signals can be crafted to yield consistent localization solutions at the receiver. Classical receivers can be modified to track an arbitrary number of signals per satellite instead of only one to detect spoofing and multipath signals. (S.A.Shaukat & al., 2016) The set of authentic signals – one signal from each satellite – would have to be correctly identified in such a receiver. Any selection of signals can be checked for consistency by verifying that the resulting residual error of the localization algorithm is very small. This is a combinatorically difficult problem. For  $n$  satellites and  $m$  transmitted sets of spoofed signals, there are  $(m+1)^n$  possibilities for the receiver to select a set of signals. Only  $m+1$  of those will result in a consistent localization solution representing the actual location and  $m$  spoofed locations. ECD avoids this signal selection problem by joining and transforming all signals into a location likelihood distribution. (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019)

ECD only shows consistent signals since just a few signals overlapping (synced) for some location hypotheses do not significantly accumulate. All plausible receiver locations – given the observed signals – have a high likelihood. Finding these locations in four dimensions, space and time, is computationally expensive. (Bissig & Wattenhoffer, 2017)

### **Branch and Bound**

A fast CD leveraging branch and bound algorithm is employed to reduce the computational load compared to exhaustively enumerating all the location hypotheses in the search space. (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019) describes the modifications to the B&B algorithm for ECD in copious detail in chapter 6. Eichelberger also discusses acquisition, receiver implementation, and experiments using the TEXBAT database. [\[19\]](#) [\[20\]](#)

One of the key points under the receiver implementation concerns the correlation of C/A codes. [\[21\]](#)

The highest correlation is theoretically achieved when the C/A code in the received signal is aligned with the reference C/A code. Due to the pseudo-random nature of the C/A codes, a shift larger than one code chip from the correct location results in a low correlation value. Since one code chip has a duration of 1/1023 ms, the width of the peaks found in the acquisition vector is less than 2% of the total vector size. ECD reduces the maximum peak by 60% in each vector. A detection for partially overlapping peaks prevents changes to those peaks. Reducing the signal rather than eliminating it has a little negative impact on the accuracy. Before using these vectors in the next iteration of the algorithm, the acquisition result vectors are normalized again. This reduces the search space based on the prior iteration. (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019)

### **ADS-B SECURITY**

We next move into the subset problem, namely ADS-B systems on aircraft, both manned and unmanned. ADS-B ubiquitously uses GPS location and signal receiver technologies. ADS-B has a very high dependency on communication and navigation (GNSS) systems. This is a fundamental cause of insecurity in the ADS-B system. It inherits the vulnerabilities of those systems and results in increased Risk and additional threats. (Nichols R. K., 2020) (Nichols R. K.-P., 2019)[\[22\]](#) Another vulnerability of the ADS-B system is its broadcast nature without security measures. These can easily be exploited to cause other threats such as eavesdropping on aircraft movement with the intention to harm, message deletion, and modification. The systems dependency on the onboard transponder is also considered a major vulnerability shared by the SSR. Aircraft hijackers can exploit this vulnerability to make the aircraft movements invisible. (Busyairah, 2019)

### **ADS-B Standards**

ICAO has stressed including provisions for protecting critical

information and communication technology systems against cyberattacks and interference, as stated in the Aviation Security Manual Document 8973/8. (ICAO, 2021) This was further emphasized in ATM Security Manual Document 9985 AN/492 to protect ATMs against cyberattacks. (ICAO, 2021)

### **ADS-B Security Requirements [23]**

Strohmeier et al. (Strohmeier, 2015) and Nichols et al. (Nichols R. K.-P., 2019) have outlined a set of security requirements for piloted aircraft and unmanned aircraft. Here are the combined security requirements for the ADS-B system in sync with the standard information security paradigm of the CIA:

- Data integrity [24]

The system security should ensure that ADS-B data received by the ground station or other aircraft (a/c) or UAS (if equipped) are the exact messages transmitted by the a/c. It should also detect any malicious modification to the data during the broadcast.

- Source integrity

The system security should verify that the ADS-B message received is sent by the message's actual owner (correct a/c).

- Data origin (location / position fix) authentication

The system security should verify that the positioning information in the ADS-B message received is the original position of the a/c at the time of transmission.

- Low impact on current operations

The system security hardware/software should be compatible with the current ADS-B installation and standards.

- *Sufficiently quick and correct detection of incidents*
- *Secure against DOS attacks against computing power*
- *System security functions need to be scalable irrespective of traffic density.*
- *Robustness to packet loss*

### **Vulnerabilities in ADS-B system**

Vulnerability in this section refers to the Ryan Nichols (RN) equations for information Risk determination. A vulnerability is a weakness in the system that makes it susceptible to exploitation via a threat or various types of threats. (Nichols R. K.-P., 2019) ADS-B system is vulnerable to security threats.

### **Broadcast Nature of RF Communications**

ADS-B principle of operation, system components, integration, and operational environment are adequately discussed in Chapter 4 (Busyairah, 2019). The ADS-B system broadcasts ADS-B messages containing a/c state vector and identity information via RF communication links such as 1090ES, UAT, or VDL Mode 4. The broadcast nature of the wireless networks without additional security measures is the main vulnerability in the system. (R.K. Nichols & Lekkas, 2002) [\[25\]](#)

### **No Cryptographic Mechanisms**

The sender encrypts neither ADS-B messages at the point of origin nor the transmission links. There are no authentication mechanisms based on robust cryptographic security protocols. The ICAO (Airport's authority of India 2014) has verified no cryptographic mechanism was implemented in the ADS-B protocol. (Airports Authority of India, 2014) [\[26\]](#)



## **ADS-B COTS**

ADS-B receivers are available in COTS at affordable prices. The receiver can be used to track ADS-B capable a/c flying within a specific receiver range. The number of ADS-B tracking gadgets for all media is growing every year. They can be used to hack the systems on UAS. (Nichols R. K.-P., 2019)

## **Shared Data**

As a result of COTS availability of ADS-B receivers, various parties, both private and public, are sharing real-time air traffic information on a/c on the Internet. Several websites on the Internet provide digitized live ADS-B traffic data to the public, e.g., flightradar24.com, radarvirtuel.com, and FlightAware. The availability of the data and the capability to track individual a/c movements open the door to malicious parties to perform undesired acts that may have safety implications. (Busyairah, 2019)

## **ASTERIX Data Format**

All-purpose Structured EUROCONTROL Surveillance Information eXchange (ASTERIX) is a binary format for information exchange in aviation. (EUROCONTROL, 2016) ADS-B data is encoded into ASTERIX CAT 21 format and transmitted by ADS-B equipped a/c to ADS\_B ground stations. And they are decoded into a usable form for ATC use. The ASTERIX format decoding guidance, source code, and tools are widely available in the public domain. (Busyairah, 2019)

## **Dependency On The On-Board Transponder**

ADS-B encoding and broadcast are performed by either the transponder (for 1090ES) or an emitter (for UAT/ VDL Mode 4) onboard the a/c. Therefore, the ADS-B aircraft surveillance is dependent on the onboard equipment. There is a vulnerability (not cyber or spoofing) whereby the transponder or emitter can be turned off inside the cockpit. The a/c becomes invisible, and SSR and TCAS operation integrity is affected.

## **Complex System Architecture and Passthrough Of GNSS Vulnerabilities**

ADS-B is an integrated system dependent on an onboard navigation system to obtain information about the state of the a/c and a communication data link to broadcast the information to ATC on the ground and other ADS-B-equipped a/c. The system interacts with external elements such as humans (controllers and pilots) and environmental factors. *The integrated nature of the system increases the system's vulnerability.* **The system inherited the vulnerabilities of the GNSS on which the system relies to obtain a/c positioning information!** The ADS-B system also inherits vulnerabilities of the communications links. (Busyairah, 2019) (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019) (The Royal Academy of Engineering, 2011)

### **Threats to ADS-B system**

Threats in this section refer to the Ryan Nichols (RN) equations for information Risk determination. A Threat is an action exploiting a vulnerability in the system to cause damage or harm specifically to a/c and generally to the Air Traffic Services (ATS), intentionally or unintentionally. (Nichols R. K.-P., 2019) ADS-B system is vulnerable to security threats.

### **Eavesdropping**

The broadcast nature of ADS-B RF communication links without additional security measures (cryptographic mechanisms) enables the act of eavesdropping on the transmission. Eavesdropping can lead to serious threats such as targeting specific a/c movement information to harm the a/c. This can be done with more sophisticated traffic and signal analysis using available sources such as Mode S and ADS-B capable open-source GNU Radio modules or SDR. Eavesdropping is a violation of confidentiality and compromises system security. (Busyairah, 2019)

### **Data-Link Jamming**

Datalink jamming is an act of deliberate / non-deliberate

blocking, jamming, or causing interference in wireless communications. (R.K. Nichols & Lekkas, 2002) Deliberate jamming aims to disrupt information flow ( message sending /receiving) between users within a wireless network using a radio jammer device. Jammer devices can be easily obtained as COTS devices. (Strohmeier, 2015) (R.K. Nichols & Lekkas, 2002) Using the Ryan Nichols equations, the impact is severe in aviation due to the large coverage area (airspace), which is impossible to control. It involves safety-critical data; hence the computed Risk/lethality level is high. (R.K. Nichols & Lekkas, 2002) (Busyairah, 2019) The INFOSEC quality affected is availability because jamming stops the a/c or ground stations or multiple users within a specific area from communicating. On Air Traffic Control

Jamming is performed on ADS-B frequencies, e.g., 1090MHz. The targeted jamming attack would disable ATS at any airport using ATCC. Jamming a moving a/c is difficult but feasible. (Strohmeier, 2015)

ADS-B system transmitting on 1090ES is prone to unintentional signal jamming due to the use of the same frequency (Mode S 1090 MHz) by many systems such as SSR, TCAS, MLAT, and ADS-B, particularly in dense space. (Busyairah, 2019) [27] Not only is ADS-B prone to jamming, but so is SSR. (Adamy, 2001)[28]

### **Two Types of Jamming Threats for ADS-B**

Apart from GNSS (positioning source for ADS-B) jamming, the main jamming threats for the ADS-B system include GS Flood Denial and A/C Flood Denial.

#### **Ground Station Flood Denial (GSFD)**

The GSFD blocks 1090 MHz transmissions at the ADS-B ground station. There is no difficulty in gaining close proximity to a ground station. Jamming can be performed using a low-power jamming device to block ADS-B signals from A/C to the ground station. The threat does not target individual a/c. It blocks ADS-B signals from all A/C within the ground station range.

#### **Aircraft Flood Denial (A/C FD)**

A/CFD blocks signal transmission to the a/c. This threat disables the reception of ADS-B IN messages, TCAS, and interrogation from WAM/MLAT and SSR. It is very difficult to gain close proximity to a moving A/C. The attacker needs to use a high-powered jamming device. According to (D. McCallie, 2011), these devices are not easy to obtain. MAYBE (see author note).[\[29\]](#) What is true is that the jamming function will be ineffective as soon as the A/C moves out of the specific range of the jamming device. Better attempts can be made from within the A/C. [\[30\]](#)

### **ADS-B SIGNAL SPOOFING**

ADS-B signal spoofing attempts to deceive an ADS-B receiver by broadcasting fake ADS-B signals that resemble a set of normal ADS-B signals or by re-broadcasting genuine signals captured elsewhere or at a different time. Spoofing an ADS-B system is also known as message injection because fake (ghost) a/c is introduced into the air traffic. The system's vulnerability – having no authentication measures implemented at the systems data link layer – enables this threat. Spoofing is a hit on the security goal of Integrity. This leads to undesired operational decisions by controllers or surveillance operations in the air or on the ground. The threat affects both ADS-B IN and OUT systems. (Busyairah, 2019) Spoofing threats are two basic varieties: Ground Station Target Ghost Injection / Flooding and Ground Station Target Ghost Injection / Flooding.

#### **Ground Station Target Ghost Injection / Flooding**

Ground Station Target Ghost Injection / Flooding is performed by injecting ADS-B signals from a single a/c or multiple fakes (ghost) a/c into a ground station. This will cause single /multiple fake (ghost) a/c to appear on the controller's working position (radar screen). [\[31\]](#)

#### **Aircraft Target Ghost Injection / Flooding**

Aircraft Target Ghost Injection / Flooding is performed by injecting ADS-B signals from a single a/c or multiple fake (ghost) a/c into an airplane in flight. This will cause ghost a/c to appear on

the TCAS and CDTI screens in the cockpit to go haywire. Making the mess worse, the fake data will also be used by airborne operations such as ACAS, ATSAW, ITP, and others for aiding a/c navigation operations. (Busyairah, 2019)

### **ADS-B message deletion**

An a/c can look like it has vanished from the ADS-B-based air traffic by deleting the ADS-B message broadcast from the a/c. This can be done by two methods: destructive interference and constructive interference. Destructive interference is performed by transmitting an inverse of an actual ADS-B signal to an ADS-B receiver. Constructive interference is performed by transmitting a duplicate of the ADS-B signal and adding the two signal waves (original and duplicate). The two signal waves must be of the same frequency phase and traveling in the same direction. Both approaches will result in being discarded by the ADS-B receiver as corrupt. (Busyairah, 2019)

### **ADS-B message modification**

ADS-B message modification is feasible on the physical layer during transmission via datalinks using two methods: Signal Overshadowing and Bit-flipping. Signal overshadowing is done by sending a stronger signal to the ADS-B receiver, whereby only the stronger of the two colliding signals is received. This method will replace either the whole target message or part of it. Bit flipping is an algorithmic manipulation of bits. The attacker changes bits from 1 to 0 or vice versa. This will modify the ADS-B message and is a clear violation of the security goal of Integrity. (Strohmeier, 2015) This attack will disrupt ATC operations or a/c navigation.

### **Circling back to ECD**

The ADS-B vulnerabilities and threats above are amenable to ECD mitigation if sufficient computing horsepower is available. For an a/c or ground station, this condition bodes well. For a UAS or sUAS, not necessarily so.

## INDOOR LOCALIZATION WITH AIRCRAFT SIGNALS USING ECD VS COMPETITIVE TECHNOLOGIES

GPS does not work well indoors due to the low signal strength. GPS satellite gets its energy from a dual solar array, which generates about 400-2900 W of power (depending on the satellite generation).[\[32\]](#) With an altitude of about 12,427 miles, this relatively weak signal barely makes it to earth. (Accuracy, 2021) The free space path loss is on the order of 180 dB. (anonymous, 2021) (Eichelberger & Tanner, Indoor Localization with Aircraft Signals, 2017)

Airplanes and other aircraft fly at an altitude below 8.5 miles. They also have ample power leaving for communications.[\[33\]](#) For safety reasons, airplanes and helicopters repeatedly transmit their location ( like GPS satellites). These ADS-B signals are strong enough to be received indoors, even with cheap hardware. But are these air traffic control signals (ATC) *precise* enough to locate the aircraft and *any* mobile device? ATC signals have not been designed for indoor localization. Three challenges present: (Eichelberger & Tanner, Indoor Localization with Aircraft Signals, 2017)

- 1) Aircraft do not fly in orbit. Aircraft do not have accurate predetermined flight paths, and unexpected changes to their route are always possible (i.e., holding pattern, weather, crowded airport)
- 2) Aircraft are not uniformly distributed in the sky. GPS satellites cover the sky in a regular pattern to maximize use position fixing ( localization).
- 3) Aircraft position signals are not precise. An aircraft has an unpredictable delay between learning its position from the GPS satellites and retransmitting this position. (Cornell – LII, 2021) [\[34\]](#) Unlike GPS satellites with their atomic clocks, aircraft transmissions may not include complete time information; some aircraft do not even include precise position information.

There are key differences in “accuracy” and “precision” and “absolute” and “relative” accuracy when it comes to discussions of GNSS/ GPS position fixing, mapping, and surveying. Schaefer devotes Chapter 19 Accuracy and Precision of GNSS in the field in his book, *GPS and GNSS Technology in Geosciences* (2021). (Schaefer & Pearson, 2021)

Eichelberger points out a few mitigating factors. Aircraft do not fly in orbits, but passengers and crew certainly do not appreciate abrupt flight path changes. Aircraft positions are not optimized for ground user-localization but rather for air traffic safety. In urban areas, there are more aircraft available than satellites. This increases the number of signals and reduces statistical uncertainty in position estimation from noisy measurements (item 3 above). (Eichelberger & Tanner, *Indoor Localization with Aircraft Signals*, 2017) However, at night, the frequency of received A/C signals is substantially lower than during the daytime.

Do the mitigations above outweigh the communications issues using just aircraft signals to retransmit the GPS signals to ground stations and users? No. Eichelberger presents an infrastructure-free indoor localization method using ECD. It requires only a network of receivers, [ground stations]; a receiver whose position should be determined [handset]; and a server that connects the handset. There is no silver bullet here. His entire approach, mathematics, field tests, and conclusions may be found in (Eichelberger & Tanner, *Indoor Localization with Aircraft Signals*, 2017).

#### **ECD vs. minimum US government GPS standards**

***The GPS Performance Standard, the US government, currently lists a worse-case horizontal accuracy of better than 17 meters (~55.8 ft) in 95% of all cases. (USGPO, 2020) Depending on the receiver's quality and available correction methods, the horizontal can be substantially better, on the order of 3-7 meters (~9.8 – 23 ft).[\[35\]](#) Usually, indoor localization methods attempt to be more accurate, such as military targeting or user in a large mall.***

**ECD cannot compete with other indoor localization methods. ECD prototype implementation has a median error of about 25 m (82 ft). ECD works very well outdoors and marginally for indoor localization on the plus side. ECD does not report well for indoor localization operations.** Rather than describe the indoor ECD implementation, prototype methods, simulations, and detailed results, the reader is guided to the primary paper for further discussion. (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019)

### **Related Work**

Much research on indoor localization focuses on providing accurate position fixes (localization), for instance, room level or sub-meter accuracy. The cost factors to get so accurate are **ITE**:

1. Installation of dedicated infrastructure like beacons in each building or room (ex., hospital neo-natal or heart surgery recovery),
2. Training or initialization phase to gather data, which is necessary for subsequent localization,
3. Usage of **E**xpensive user equipment.(Eichelberger & Tanner, Indoor Localization with Aircraft Signals, 2017)

Most methods do not suffer all three drawbacks. But less cost is a trade-off for less accuracy. Liu et al. provide an overview of indoor localization methods. They differ by fundamental measurements, which are received signal strength (RSS), time of arrival (TOA), time difference of arrival (TDOA),[\[36\]](#) or angle of arrival (AOA). (Liu & al, 2007) Below are briefly listed the main ECD competitors with ITE drawbacks in brackets.

### **WiFi [T]**

WiFi signals are popular for indoor localization because of the wide use of WiFi hotspots. No dedicated infrastructure like beacons is needed. WiFi-based approaches generally have an accuracy of a few meters ( “few” x 3.280 = ft). WiFi localization methods require



a training phase in which positions or fingerprints of the access points are determined at different locations. Infrastructure changes must be detected, and the database needs to be updated regularly. (Liu & al, 2007)

### **Ultrasound [I]**

Ultrasound-based methods require dedicated hardware—cheap equipment with excellent results. Ultrasound systems have proven to be very accurate, achieving centimeter-level accuracy. (1 cm= 0.393 in) The drawbacks are limited effective distance prone to ambient noise. (Oberholzer & et.al, 2011)

### **Light [T,E]**

The most accurate results are achieved by laser- and camera-based methods. The best system in 2016 achieved an accuracy of 5 cm (1.968 in) using two lasers and multi high-end cameras. It costs a quarter-million dollars. (Microsoft, 2016) LEDs and miniaturization have opened up the visible light spectrum to communication and localization techniques. Pathak et al. give an extensive overview of current methods. (Pathak & al, 2015)

### **Bluetooth [T, I]**

Bluetooth, like WiFi, uses a 2.4 GHz frequency band. WiFi may take tens of seconds to identify base stations; faster response times can be achieved with Bluetooth. (Mair, 2012) Bluetooth pairing presents a delay before users can exchange information. The accuracy of Bluetooth methods approaches 3 m (9 ft).

### **RFID [I]**

RFID systems are either active or passive. They have limited capacity energy and require many units to communicate over short distances. Bouet and Dos Santos explore RFID localization systems. (Bouet, 2008)

### **Sensor Fusion**

Sensor-assisted localization methods are favored in smartphone applications because all these devices feature an inertial measurement unit (IMU) comprising an accelerometer, a gyroscope,

and a compass. (Ye & al, 2012) Accuracy ranges are dependent on local conditions, tower availability, and 4 or 5G / LTE available networks.

### **HAPS**

Of special interest to this reviewer is the possibility of using High Altitude UAS Platforms for wireless communications (HAPS) to replace the aircraft in retransmitting GPS signals and acting as the primary agent for indoor and outdoor localization procedures. Two important references detail the advantages and disadvantages of HAPS for communication systems and localization use. (Alejandro Aragon-Zavala, 2008) Nichols et al. provide an especially strong analysis of HAPS capabilities compared to terrestrial and satellite systems for telecommunications; HAPS platform advanced telecommunications services in various stages of engineering and development, HAPS link budgets, and characteristics of terrestrial, satellite, and haps systems. (Nichols R. K.-P., 2019)

### **Security of GNSS (Shrivastava, 2021) (Ochin & Lemieszewski, 2021)**

In 2021 (Ochin & Lemieszewski, 2021), Ochinn & Lemieszewski penned an excellent update on the spoofing threat covering air, land, and sea operations in Europe and Asia. Some interesting topics covered were self-spoofing or limpet spoofing technologies; DIY GNSS spoofer's; [37] GNSS interference modalities; complementary countermeasures like INS; [38] GNSS jamming techniques, GNSS meaconing, and detailed sections on cloud-based GNSS positioning. Modern satellite navigation is based on the use of NO-Request range measurements between the navigation satellite and the user. It means that the information about the coordinates of the satellites given to the user is included in the navigation signal. The range measurement is based on calculating the receiving signal time delay compared with the signals generated by the user's equipment. (Ochin & Lemieszewski, 2021) Chapter 3 divides Cloud-based spoofing detection into four classes and mathematically defines the antenna distances and navigation modes based on those classes.

These detection modes are based on a single antenna spoofer and do not consider mitigation and recovery steps. This is compared to ECD, which does all three steps in the security solution.

Ochin & Lemieszewski (Ochin & Lemieszewski, 2021) present a fascinating picture of the history of anti-spoofing from 1942 patent to fight the American radio-controlled sea-based torpedoes with a radio jamming of German boats and submarines. (US Patent No. 2,292,387, 1942) They continue with a European view of security measures for the six satellite constellations. They conclude with a Postscript on the drama behind the taking by Iran of the US RQ-170 Sentinel and how they did it! (Goward, April 21, 2020) The Ochin & Lemieszewski chapter supports the risk opinions presented earlier. "The Risk of losing GNSS signal (to spoofing) is growing every day. The accessories necessary for the manufacture of systems for GNSS "jamming" and/or "spoofing" are now widely available, and this type of attack can be taken advantage of by not only the military but also by terrorists." (Ochin & Lemieszewski, 2021)

## CONCLUSIONS

The purposes of this chapter were to introduce the problem of Navigation Cyber-Spoofing; to recognize that GNSS / GPS / ADS-B systems, including CBRN mobile assets, are susceptible to Cyber Spoofing; that research has focused on detection rather than mitigation and recovery efforts; and finally, that ECD is a brilliant solution to part of the Cyber Spoofing problem as it does not exclude false signals but encompasses them into the algorithm.

## Bibliography

Accuracy, G. G.-G. (2021, July 16). *Official U.S. government information about the Global Positioning System (GPS) and related topics*. Retrieved from <https://www.gps.gov/systems/gps/performance/accuracy/#problems>

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

Airports Authority of India. (2014). *Security Issues of ADS-B Operations*. ICAO. Hong Kong, China: ICAO.

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

Ali, e. a. (2014). ADS-B system failure modes and models. *The Journal of Navigation*, 67: 995-1017.

anonymous. (2021, July 16). GPS newsgroup. Retrieved from <http://gpsinformation.net/main/gpspower.htm>:  
<http://gpsinformation.net/main/gpspower.htm>

Anonymous. (2014). *Timing & Synchronization for LTE-TDD & LTE-Advanced Mobile Networks*; Technical Report, Microsemi. Retrieved from [www.microsemi.com](http://www.microsemi.com): [https://www.microsemi.com/document-portal/doc\\_download/133615-timing-sync-for-lte-tdd-lte-a-mobile-networks](https://www.microsemi.com/document-portal/doc_download/133615-timing-sync-for-lte-tdd-lte-a-mobile-networks)

Axelrod, P., & al, e. (2011). Collective Detection and Direct Positioning Using Multiple GNSS Satellites. *Navigation*, pp. 58(4): 305-321.

Bissig, P., & Wattenhoffer, M. E. (2017). Fast & Robust GPS Fix using 1 millisecond of data. 16 *ACM / IEEE Int Conf on Information Processing in Sensor Networks* (pp. 223-234). Pittsburgh, PA: IPSN.

Bouet, M. & (2008). RFID Tags: Position Principles and localization techniques. *IEEE 1st IFIP Wireless Days*, pp. 1-5.

Burgess, M. (2017, September 21). *When a Tanker Vanishes, all evidence points to Russia*. Retrieved from <https://www.wired.co.uk/>: <https://www.wired.co.uk/article/black-sea-ship-hacking-russia>

Busyairah, S. A. (2019). *Aircraft Surveillance Systems: Radar Limitations and the Advent of the Automatic Dependent Surveillance-Broadcast*. New York: Routledge.

Cheong, J., & al., e. (2011). Efficient Implementation of Collective Action. In *IGNSS Symposium*, 15-17.

Closas, P., & al., e. (2007). Maximum likelihood estimation of position in GNSS. *IEEE Signal Processing Letters* (pp. 14(5): 359-362). IEEE.

Cornell – LII. (2021, July 16). ADS-B law. Retrieved from <https://www.law.cornell.edu/>: <https://www.law.cornell.edu/cfr/text/14/91.227#e>

87. McCallie, e. a. (2011). Security analysis of the ADS-B Implementation in the NEXT generation Air transport system. *Inter J. of Critical Infrastructure Protection*, 4: 78–87.

Diggelen, F. V. (2009). *A-GPS: Assisted GPS, GNSS, and SBAS*. NYC: Artech House.

DoD. (2008). *Global Positioning System Performance Standard 4th edition (GPS SPS PS)*. Washington, DC: DoD.

Eichelberger, M. (2019). *Robust Global Localization using GPS and Aircraft Signals*. Zurich, Switzerland: Free Space Publishing, DISS. ETH No 26089.

Eichelberger, M., & Tanner, S. L. (2017). *Indoor Localization with Aircraft Signals*. ACM -Sen Sys -17, ISBN: 978-1-4503-5459-2.

EUROCONTROL. (2016, June). *part\_1\_-\_eurocontrol\_specification\_asterix\_spec-149*. Retrieved from <https://www.eurocontrol.int/sites/>: [https://www.eurocontrol.int/sites/default/files/2019-06/part\\_1\\_-\\_eurocontrol\\_specification\\_asterix\\_spec-149\\_ed\\_2.4.pdf](https://www.eurocontrol.int/sites/default/files/2019-06/part_1_-_eurocontrol_specification_asterix_spec-149_ed_2.4.pdf)

Fan, Y., & al., e. (2015). A Cross-layer defense mechanism against GPS spoofing attacks on PMUs in Smart Grid. *IEEE Trans on Smart Grid*, Vol 6. No. 6 November.

2628. Lopez-Risueno & Seco-Granados, G. (2005). Cn/sub 0/ estimation and near-far mitigation for GNSS indoor receivers. In *2005 IEEE 61st Vehicular Technology Conf.*, V4: 2624–2628.

Goward, D. (April 21, 2020). GPS circle spoofing was discovered in Iran. *GPS World*.

Haider, Z., & Khalid, & S. (2016). Survey of Effective GPS Spoofing

Countermeasures. *6th Intern. Ann Conf on Innovative Computing Technology* (INTECH 2016) (pp. 573-577). IEEE 978-1-5090-3/16.

Humphreys, T., & al., e. (2008). Assessing the spoofing threat: Development of a portable GPS civilian spoofer. In *Radionavigation Laboratory Conf. Proc.*

ICAO. (2021, June 2). *atm\_security\_manual* 9985. Retrieved from <http://www.aviationchief.com/>: [http://www.aviationchief.com/uploads/9/2/0/9/92098238/icao\\_doc\\_9985\\_-\\_atm\\_security\\_manual\\_-\\_restricted\\_and\\_unedited\\_-\\_not\\_published\\_1.pdf](http://www.aviationchief.com/uploads/9/2/0/9/92098238/icao_doc_9985_-_atm_security_manual_-_restricted_and_unedited_-_not_published_1.pdf)

ICAO. (2021, June 2). *Aviation Security Manual Document 8973/8*. Retrieved from <https://www.icao.int/Security/>: <https://www.icao.int/Security/SFP/Pages/SecurityManual.aspx>

IS-GPS-200G. (2013, September 24). IS-GPS-200H, GLOBAL POSITIONING SYSTEMS DIRECTORATE SYSTEMS ENGINEERING & INTEGRATION: INTERFACE SPECIFICATION IS-GPS-200 - NAVSTAR GPS SPACE SEGMENT/NAVIGATION USER INTERFACES (24-SEP-2013). Retrieved from <http://everyspec.com/>: [http://everyspec.com/MISC/IS-GPS-200H\\_53530/](http://everyspec.com/MISC/IS-GPS-200H_53530/)

J.Liu, & et.al. (2012, November). Energy Efficient GPS Sensing with Cloud Offloading. *Proceedings of 10 ACM Conference on Embedded Networked Sensor Signals (SenSys)*, pp. 85-89.

Jafarnia-Jahromi, A., & al., e. (2012). Detection and mitigation of spoofing attacks on a vector-based tracking GPS receiver. *ION ITM*.

Jia, Z. (2016). A Type of Collective Detection scheme with improved pigeon-inspired optimization. *Inter. J. of Intelligent Computing and Cybernetics*, 9(1):105-123.

Jovanovic, A., & Botteron, C. (2014). Multi-test Detection and Protection Algorithm against Spoofing Attacks on GNSS Receivers. *PLANS IEEE/ION Position, Location and Navigation Symposium* (pp. 5-8 May). Monterey, CA 5-8 May: IEEE/ION.

Kuhn, M. G. (2015). An Asymmetric Security Mechanism for Navigation Signals. *6th Info Hiding Workshop*. Toronto, CA: Univ of Cambridge. Retrieved from <https://www.cl.cam.ac.uk/~mgk25/ih2004-navsec.pdf>

Liu, H., & al, e. (2007). Survey of wireless indoor positioning techniques and systems. *IEEE TX on systems, man and cybernetics, Part C ((applications & reviews)*, pp. 37, 6: 1067-1080.

M.Eichelberger, v. H. (2019). Multi-year GPS tracking using a coin cell. In *Proc. of 20th Inter.Workshop on Mobile Computing Systems & Applications ACM*, 141-146.

M.L. Psiaki & Humphreys, T. (2016). GNSS Spoofing and Detection. *Proc. of the IEEE*, 104(6): 1258-1270.

Madhani, P., & al., e. (2003). Application of successive interference cancellation to the GPS pseudolite near-far problem. *IEEE Trans, on Aerospace & Elect. Systems*, 39(2):481-488.

Magiera, J., & Katulski, & R. (2015). Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing. *J. of Applied Research & Technology*, Vol 13. pp 45-47.

Mair, N. & (2012). A collaborative Bluetooth- based approach to localization of mobile devices. *IEEE 8th Inter Conf. on Collaborative Computing: Networking, Applications, and work sharing*, pp. 363-371.

Microsoft. (2016). *Microsoft Indoor Localization Competition*. Retrieved from [www.microsoft.com](http://www.microsoft.com): <https://www.microsoft.com/en-us/research/event/microsoft-indoor-localization-competition-ispn-2016/#official-results>

Nichols, R. K. (2020). *Counter Unmanned Aircraft Systems Technologies & Operations*. Manhattan, KS: [www.newprairiepress.org/ebooks/31](http://www.newprairiepress.org/ebooks/31).

Nichols, R. K.-P. (2019). *Unmanned Aircraft Systems in the Cyber Domain, 2nd Edition*. Manhattan, KS: [www.newprairiepress.org/ebooks/27](http://www.newprairiepress.org/ebooks/27).

Nichols, R., & al., e. (2020). *Unmanned Vehicle Systems and Operations on Air, Sea, and Land*. Manhattan, KS: New Prairie Press #35.

Oberholzer, & et.al. (2011). Spiderbait: Augmenting wireless sensor networks with distance and angle information. *Proc of 10th ACM/ IEEE Int Conf on Information Processing in Sensor Networks*, pp. 211-222.

Ochin, E., & Lemieszewski, & L. (2021). Chapter 3 Security of

GNSS. In G. P. PETROPOULOS, & P. SRIVASTAVA, *GPS and GNSS Technology in the Geosciences* (51-73). NYC: Elsevier.

234. Bissag, E. M. (2017, April). Fast and Robust GPS Fix Using One Millisecond of Data. *Proc of the 16th ACM /IEEE International Conference on Information Processing in IPSN*, 223-234.

Pathak, H. P., & al, e. (2015). Visible light communication, networking, and sensing: a survey, potential, and challenges. *IEEE Communications Surveys & Tutorials*, pp. 17, 4: 2047-2077.

Psiaki, M., & al, e. (2013). GPS Spoofing Detection via Dual-Receiver Correlation of Military Signals. *IEEE Tran of Aerospace & Electrical systems*, vol 49, issue 4, pp. 2250-2260.

R.K. Nichols & Lekkas, P. (2002). *Wireless Security; Threats, Models & Solutions*. NYC: McGraw Hill.

R.K. Nichols, e. a. (2020). *Unmanned Vehicle Systems & Operations on Air, Sea & Land*. Manhattan, KS: New Prairie Press #35.

Ranganathan, A., & al, e. (2016). SPREE: A Spoofing Resistant GPS Receiver. *Proc. of the 22nd ann Inter Conf. on Mobile Computing and Networking*, ACM, pp. 348-360.

S.A.Shaukat, & al, e. (2016). Robust vehicle localization with GPS dropouts. *6th ann Inter Conf on Intelligent and advanced systems* (pp. 1-6). IEEE.

Schaefer, M., & Pearson, A. (2021). *GPS and GNSS Technology in Geosciences*. NYC: Elsevier.

Schmidt, D., & al, e. (2016). A Survey and Analysis of GNSS Spoofing Threat and Countermeasures. *ACM Computing Surveys (CSUR)*, 48(4).

Shrivastava, G. P. (2021). *GPS and GNSS Technology in the Geosciences*. NYC: Elsevier.

Spilker, J. (1996). Fundamentals of Signal Tracking Theory. *Prog in Astronautics & Aeronautics*, 163:245-328.

Strohmeier, M. (2015). On the security of the automatic dependent surveillance-broadcast protocol. *IEEE Communications Surveys & Tutorials*, 17:1066-1087.



The system, H. K. (1942). US Patent No. 2,292,387.

T.E. Humphrees, e. (2008). Assessing the Spoofing Threat: Development of a portable GPS Spoofing Civilian Spoofer. ION (pp. Sept 16-19). Savana, GA: ION.

The Royal Academy of Engineering. (2011). *Global Navigation Space Systems: Reliance and Vulnerabilities*. London: The Royal Academy of Engineering.

Tippenhauer, N., & et.al. (2011). On the requirements for successful spoofing attacks. *Proc. of the 18th ACM Conf. on Computing and communications security (CCS)*, 75-86.

Tsui, J. B. (2000). *Fundamentals of Global Positioning Systems Receivers – A Software Approach*. NYC: John Wiley & Sons.

USGPO. (2020, April). *Global Positioning System (GPS) Standard Positioning Service (SPS) 5th ed.* Retrieved from <https://www.gps.gov/technical/ps/>: <https://www.gps.gov/technical/ps/2020-SPS-performance-standard.pdf>

USGPO. (2021, June 14). What is GPS? Retrieved from [Gps.gov: www.gps.gov/systems/gps](https://www.gps.gov/systems/gps)

Warner, J. S., & Johnston, R. (2003). GPS Spoofing Countermeasures. *Journal of Security Administration*. Retrieved from <https://www.semanticscholar.org/paper/GPS-Spoofing-Countermeasures-Warner-Johnston/36e1f723bff8d429aca4714abe54500a9edaa49>

Warner, J., & Johnson, & R. (2002). A Simple Demonstration that the system (GPS) is vulnerable to spoofing. *J. of Security Administration*. Retrieved from <https://the-eye.eu/public/Books/Electronic%20Archive/GPS-Spoofing-2002-2003.pdf>

Wesson, K. (2014, May). *Secure Navigation and Timing without Local Storage of Secret Keys*. Ph.D. Thesis.

Wikipedia. (2021, June 2). *Global Positioning System*. Retrieved from <https://en.wikipedia.org/wiki/>: [https://en.wikipedia.org/wiki/Global\\_Positioning\\_System](https://en.wikipedia.org/wiki/Global_Positioning_System)

1026. Ng & Gao, G. (2016). Mitigating jamming & meaconing attacks using direct GPS positioning. In *Position, Location & Navigation*

Symposium (PLANS) IEEE/ION, 1021-1026.

Ye, H., & al, e. (2012). track: Infrastructure-free floor localization via mobile phone sensing. *IEEE Inter Conf. on Pervasive computing and communications*, pp. 2-10.

## Endnotes

[1] **ECD** – Dr. Manuel Eichelberger’s advanced implementation of CD to detect and mitigate spoofing attacks on GPS or ADS-B signals (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019)

[2] The detailed ECD Navigation model and supporting equations are found in the primary reference (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019)

[3] The results are defined and graphically presented in (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019) p87-ff.

[4] The author has nicknamed it to Honor Dr. Manuel Eichelberger’s brilliant doctoral research, ECD. ECD is Dr. Manuel Eichelberger’s advanced implementation of CD to detect and mitigate spoofing attacks on GPS or ADS-B signals

[5] This is a key point. CD reduces this timestamping process significantly.

[6] Data is sent on a carrier frequency of 1575.42 MHz. (IS-GPS-200G, 2013)

[7] GPS satellites operate on atomic frequency standards; the receivers are not synchronized to GPS time.

[8] Because the receiver must decode all that data, it must continuously track and process the satellite signals, which translates to high energy consumption. Furthermore, the TTFF on startup costs the user both latency and power.

[9] The deviation is defined as the time offset multiplied by the speed of light plus the location distance.

[10] For those who insist on SI / metric,  $1 \text{ km} = \sim 0.62 \text{ mi (miles)}$

[11] Data bit flips can happen. The normal practice is 2 milliseconds of sample time.

[12] The vector/tensor mathematics for localization are reasonably complex and can be found in Chapter 5.3 of (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019)

[13] Cloud offloading also makes ECD suitable for energy-constrained sensors.

[14] (Nichols & al., 2020) have argued the case for cryptographic authentication on civilian UAS /UUV and expanded the INFOSEC requirements.

[15] To evaluate the performance of the (Jovanovic & Botteron, 2014) CM, an attack was performed on a GNSS receiver through a GSS8000 full constellation simulator attached to a rooftop antenna.

[16] This cross-correlation portion of this CM method syncs well as a forerunner of ECD.

[17] This is a key section to understanding the beauty of ECD. The entire SIC algorithm and ECD implications are found in detail in (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019) p81-ff.

[18] This is what makes jamming a lesser attack. The jamming is

detectable by observing the noise floor, in-band power levels, and loss of signal-lock takeover.

[19] See (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019) Sections 6.5 – 6.7 pages 84-94.

[20] See (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019) Sections 5.34 – 5.5 for extended discussions on space discretization, satellite visible set  $\mathbf{V}$ , time discretization, averaging over likely hypotheses, hypothesis  $\mathbf{h}$ , coding, efficient implementation of the B&B, local oscillator bias, criteria and test evaluations of ECD, computational considerations, and conclusions. (Closas & al., 2007)(J. Liu & et.al., 2012) (Diggelen, 2009)

[21] This is accomplished in the acquisition stage of a GPS receiver. The received signals are correlated with the C/A codes.

[22] (Nichols R. K., 2020) presents a model of Risk as a function of Threats, Vulnerabilities, Impact, and Countermeasures known as the Ryan- Nichols equations, that models the qualitative effects of information flow through the communications and navigation systems in UAS. The model is based on the brilliant INFOSEC work of Dr. Julie J.C.H. Ryan and Dr. Daniel J. Ryan, described in many of the authors' NPP books.

[23] These INFOSEC goals are admirable but considering that most GPS and UAS COTS do not have sufficient GPS spoofing countermeasures or cybersecurity protections (most are legacy), the list is more of a wish list. [Author opinion]

[24] Please note the word “should.” Hackers just love this word.

[25] Wireless networks present few obstacles to access and can easily be attacked by open-source software. (R.K. Nichols, 2020)

[26] This is still true in legacy systems. Newer implementations have

additional protections. UAS systems are notoriously weak in terms of security.

[27] Ali et al. identified that jamming of GPS transmissions from the satellite affected the ADS-B system. (Ali, 2014) This is a rather obvious statement of research considering that we have also established that the vulnerabilities of GNSS/GPS pass down to ADS-B systems because they are a subset of the larger problem.

[28] Dave Adamy is the leading global expert in EW. He teaches it is more difficult to jam a PSR due to its rotating antenna and higher transmission power. (Adamy, 2001)

[29] This might have been true in 2011, a decade of change, growth, cost-effective COTS, and state-sponsored hackers. Say this observation is severely dated. (Author comment)

[30] Author comment based on experience. Jamming devices are as small as your cell phone and more powerful than computers available in 2011. (Nichols R. K., 2020)

[31] This is a headache. Consider a SWARM of 100 + UAS bursting onto the controller's screen at a busy airport.

[32] This is about the consumption of a GSM base station.

[33] A Boeing 747 has an average power consumption of 140 MW, leaving power to spare for GPS communications.

[34] Uncompensated latency of up to 0.6 s. (Cornell – LII, 2021)

[35] 1 m = 3.280 ft

[36] TDOA is also called multilateration.

[37] DIY – Do it yourself

[38] INS- an inertial navigation system is composed of motion

sensors (accelerometer, gyrometer, and magnetometer), allowing the determination of the absolute movement of a platform. Using this information and knowledge of the last position, it is possible to use dead reckoning to estimate the platform's position, velocity, and time after spoofing or jamming detection.

PART IV

# SECTION 4: SOCIAL NETWORKS AND TOOLS OF THE TRADE





# 20. Social Network Implications for WMDD

**By Wayne D. Lonstein, Esq.**

## **STUDENT LEARNING OBJECTIVES**

The student will gain knowledge of the emergence of social media networks such as Twitter, Facebook, Tik Tok, and YouTube as delivery methods for various types of WMDD. (Figure 20.1) By highlighting the ubiquitous availability and acceptance of these networks globally, they serve as uniquely effective methods of delivering information globally and instantly. They are capable of causing mass casualties or death by seeding panic, false narratives, or even serving as a messaging or command and control tool for combatants, terrorists, or other NGO actors globally.

## **SOCIAL MEDIA NETWORKS AS A WEAPON OF MASS DESTRUCTION, DISTRACTION, AND DIVISION**

In 1980, famed Holocaust survivor and Nazi hunter Simon Wiesenthal was asked by a college student if the Holocaust could happen again. Wiesenthal responded; “If the technology available to Adolf Hitler had been available in 1492, no Jew would have survived in Spain, no Catholic in England, and no Protestant in France.” (Heir, 2019) Although Hitler had no shortage of apologists in the Western media, such as the New York Times, radio was still limited in its reach, and television was in its formative years. (Frankel, 2001) The concept of the instant digital transmission of information globally was primarily a concept reserved for those who wore tinfoil hats.

**Figure 20.1 A Third of Tik Tok users in the U.S. may be 14 or under, raising safety concerns.**

## ***A Third of TikTok's U.S. Users May Be 14 or Under, Raising Safety Questions***

Three current and former employees expressed concerns about the Chinese-owned app's safeguards for preteen children.

Give this article



21



Young users of TikTok in Elizabeth, N.J. TikTok classified more than a third of its 49 million daily users in July in the United States as being 14 years old or younger, according to internal documents. Taylor Johnson for The New York Times.

Source: (Courtesy New York Times) (Johnson, 2020)

In a 2015 article, “Are We Experiencing a Digital Spring?” this author examines how social media help fuel the Arab Spring. (Lonstein, Are We Experiencing a Digital Spring? 2015) The governments of Tunisia, Egypt, Libya, and Yemen fell with never-before-seen speed, in part helped by the instant viral spread of

social media videos and posts. The power of social media and streaming was far greater than the viral spread of a populist movement may well have been far more nuanced than initially thought.

In 2017, Jon Herrmann wrote an article entitled “Nine Links in the Chain: The Weaponized Narrative, Sun Tzu, and the Essence of War.” Herrmann examines how weaponized narratives disseminate. He wrote; “a narrative can now deploy in a rapid-fire series of mutually reinforcing stories that are hard for people to disregard and reach a global audience in seconds at a minimal cost.” (Herrmann, 2017)

In 2016, the Chinese technology company Byte Dance launched the social media app Tik Tok. The platform formally took hold in 2018, going from obscurity to **2.5 billion installs in just three years** with a projected social media user’s market share of **over 20% by 2024**, trailing only the Meta-owned Facebook and Instagram in **popularity worldwide**. While many have been strongly critical of the content moderation and de-platforming activities of the US-based social media companies, one crucial difference exists between those companies and Tik Tok: state control of or access to user data. While that may insignificant, a careful examination of its Privacy Policy reads: *“We may collect biometric identifiers and biometric information as defined under U.S. laws, such as faceprints and voiceprints, from your User Content. Where required by law, we will seek any required permissions from you before any such collection.”* (Perez, 2021) 2021)

According to Bryan Cunningham, Executive Director of the Cybersecurity Policy Research Institute at U.C. Irvine, “If the legal authorities in China or their parent company demand the data, users have already given them the legal right to turn it over.” William Evanina, former Director of the National Counterintelligence and Security Center, warned, “When you are going to download Tik Tok ... and you click on that ‘I agree to terms’ – what is in that is critical” (Rodriguez, 2021)

In the age of deep fakes, A.I., machine learning, and all those technologies encompass, all of the users of Tik Tok, no matter their

age or nationality, may have already provided the Rosetta stone of information to the hostile governments, terrorist, or their proxies.

Students must be aware of the risks social media can present as a tool of information mining, information warfare, and live, global command and control; they should consider that it can in and of itself be considered a Weapon of Mass Destruction. During the COVID-19 Pandemic, Carnegie Mellon University studied over 200 million tweets discussing the pandemic. The findings were proof positive of how Social Media is a force multiplier when it comes to information warfare. “Of the top 50 influential re-tweeters, 82% are bots, they found. Of the top 1,000 re-tweeters, 62% are bots.” (Young, 2020) Some like Sarah Jacobs Gamberini believe that Social Media can also serve as a Bioweapon, especially during a time such as the current pandemic. “Russia’s present leaders fear that U.S. advantages in information technology allow Washington and its allies to undermine Russian social, cultural, and political institutions as part of its broader campaign to ensure Western geopolitical dominance. The Kremlin sees information as a new type of weapon and views all forms of information, across all platforms, as potential sources of power to be weaponized.” (Gamberini, 2020) Bots on social media platforms have been documented to help amplify division and misinformation, especially when there is a heated debate, in this case, vaccinations. (Broniatowski, 2018)

### **CONSUMER AND COMMERCIAL DRONE TECHNOLOGY IS ALSO A TOOL FOR ESPIONAGE AND EVEN OFFENSIVE KINETIC ATTACKS**

Consumer technology risk does not end with information harvesting. It extends to another vector of delivery for weaponized narratives. In 2016, Zhu Ling, editor-in-chief of China Daily, said: “We have always attached great importance to ‘borrowing a mouth to speak’ and used international friends to carry out foreign propaganda.” (Australian Strategic Policy Institute, 2021)

Considering China’s ability to acquire such a broad swath of users’ biometric and personal data and its potential weaponization, it

takes little imagination to conclude that Tik Tok presents a clear and present danger to people worldwide. Just imagine multiple “A.I.” generated deep fake accounts of influencers spreading propaganda or worse to the fifty million daily users of Tik Tok in the United States and one billion users monthly across the globe? The prospect of mining the images and biometric information of children using social media apps without understanding the consequence of their actions or the legal ability to sign a binding contract is even more troubling. Imagine a Tik Tok or V.K. user becoming the Prime Minister of the United Kingdom. Upon assuming office, a hostile nation attempts to blackmail or extort them based upon biometric, or other personal information mined years before. The risk does not end with social media. SZ DJI Technology Co., the world’s largest producer of unmanned aerial vehicles, has been in the cross-hairs of many Western national security agencies for years. The primary concern is that DJI drones are in the hands of consumers, and companies are serving as passive listening and information harvesting tools for the Chinese military-industrial juggernaut. (Figure 20.2) According to FCC Commissioner Brendan Carr, DJI drones “vast amounts of sensitive data,” and Carr warned DJI might be a “Huawei on Wings” in an FCC statement. (Commission, 2021)

**Figure 20.2 Drone operator flying over rooftops**



Source: (Courtesy Wayne Lonstein) (Lonstein, Photo, 2022)

In June of 2021, a “leaked” report summary from The Hill claimed that the “Pentagon report clears use of drones made by top Chinese Manufacturer.” (Rodrigo, 2021) Whether a trial balloon or mistake, The Hill report resulted in a strong response from the Department of Defense in July 2021 which issued a statement countering conflicting information being “not approved for release by the DOD. (Defense, 2021)

Unfortunately, governmental prohibitions on DJI products and investment in the company do little to address the risk posed by DJI products in consumer markets. It is not a giant leap to see how consumer technology has become a tool of terror and war. In a recent report in FT, Marine Corps General Frank McKenzie identified the risk by calling these products “Costco Drones” the new “IED Movement.” (Manson, 2022)

The 2022 Russian invasion of Ukraine is an ongoing conflict as of the writing of this text. Numerous accounts about the highly effective use of weaponized consumer drones have surfaced, and

their effect on the Russian troops appears to be significant. (Figure 20.3) Consumer drones with infrared cameras locate Russian troops, and modified drones deliver explosive payloads. (Hambling, 2022) According to the website [dronedj.com](http://dronedj.com) “A local U.A. company developing a way to drop payloads onto Russian vehicles simply from COTS drones; here an F-1 grenade is dropped from a DJI Phantom 4 onto a car from 100m,” @CalibreObscura’s [tweet](#) reads. “Note that this is civilians developing this for defense, not the Ukrainian Army.” (Crumley, 2022)

**Figure 20.3 Grenade launched from DJI Phantom 4**



Source: Courtesy Dronedj.com (Crumley, 2022)

Over the last decade, the emerging technologies of live streaming social media and drones have been the source of many improvements to the day-to-day lives of billions of people globally. While the positives have primarily outweighed the negatives, a concern exists that the marriage of the two technologies can provide bad actors with a command-and-control capability never before available. Students must remain mindful of the rapidly emerging threats posed by consumer products. Whether it is

mining information for children or unsuspecting users of social media apps, or information obtained from connected technology used in our daily lives, the prospect of misuse of this information remains significant.

The risks posed by exploiting social media platforms go far beyond misinformation, unrest, and recruitment. Consumer technology such as drones can be coupled with social media to allow for the remote operation of UAVs from anywhere in the world. FPV technology is a game-changer. “FPV stands for first-person view. So, when it comes to flying an FPV drone, pilots of FPV drones see what the drone sees. Traditional drones differ from this as they are piloted through the pilot’s perspective on the ground. With FPV, it is instead piloted through the drone’s perspective, not the pilot, via an onboard camera. (Figure 20.4) A drone’s eye view, if you will.” (Dean, 2021)

**Figure 20.4 DJI Operator**



Source: Courtesy DJI

FPV drones have become wildly popular. Their target market is



the hobbyist or drone racing consumer. It was not a giant leap to see how using FPV drones could be an effective tool of warfare where the operator can remotely operate the drone through remote virtual display goggles for missions of up to 7.5 kilometers or more with modification.

Such inexpensive and effective technology is not lost on NGOs and Terror groups when waging asymmetric warfare. The Islamic State took advantage of inexpensive consumer drones in Iraq and Syria, easily modified to carry and deliver ordnance to attack United States forces. “They used them when we were closing in on Mosul,” Lt. Gen. Mark Nowland, deputy chief of staff for operations for the Air Force, told a small group of reporters following Thursday’s event. “There were some operations where they dropped a grenade essentially, so it was essentially a piece of artillery that was falling on some forces.” (Pomerleau, 2018)

Students should consider what happens when inexpensive consumer technology and social media live streaming meet? This prospect is no longer a hypothetical exercise; instead, it is a troubling reality. Imagine the propaganda value of a terror group live-streaming an attack or nation-state combatants’ live streaming combat drone activities to propagandize a narrative about the success of operations. The troubling marriage of technology, social media live to stream, and warfare is a new reality that may confront students sooner than they think. Add to that the private ownership of Social Media or, in the case of nations such as China, direct control over platforms such as Tik Tok, and the issue of access or bandwidth could become a deciding factor on the information warfare narrative battlefield.

## **QUESTIONS FOR STUDENTS TO CONSIDER**

1. Should consumer technology companies and social media networks be subject to government oversight in times of war?
2. Since they operate globally, how can social media companies in multiple countries navigate the conflicting interests of two nations at war?
3. Should consumer product companies such as drone manufacturers be responsible for harm caused when their technology is used in terror operations or other harmful manners resulting in mass casualties to civilians?
4. What uses of social media and consumer electronics can you foresee shortly which will need to be addressed? How would you remediate the threat?
5. What is the best method to address the battlefield or terroristic use of modified consumer drones and technology without harming the development of these groundbreaking technologies?

### Bibliography

Australian Strategic Policy Institute. (2021, December 10). *Borrowing mouths to speak on Xinjiang*. Retrieved from Australian Strategic Policy Institute: <https://www.aspi.org.au/report/borrowing-mouths-speak-xinjiang>

Broniatowski, D. A. (2018, September 12). *Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate*. Retrieved from American Journal of Public Health: <https://ajph.aphapublications.org/doi/full/10.2105/AJPH.2018.304567>

Commission, F. C. (2021, October 19). *Carr Calls for Review of DJI, Citing National Security Risks*. Retrieved from FCC.GOV: <https://www.fcc.gov/document/carr-calls-review-dji-citing-national-security-risks>

Crumley, B. (2022, March 2022). *Drone video shows purported DJI drone in spot-on Ukraine grenade drop*. Retrieved from Dronedj: <https://dronedj.com/2022/03/21/drone-video-shows-purported-dji-drone-in-spot-on-ukraine-grenade-drop/>

Dean, G. (2021, October 20). *What are FPV drones?* Retrieved from Space: <https://www.space.com/what-are-fpv-drones>

Defense, U. D. (2021, July 23). *Department Statement on DJI Systems*. Retrieved from Defense.gov: <https://www.defense.gov/News/Releases/Release/Article/2706082/department-statement-on-dji-systems/>

Frankel, M. (2001, November 14). *150th Anniversary: 1851-2001; Turning Away From the Holocaust*. Retrieved from New York Times.

Gamberini, S. J. (2020, November 19). *Social Media Weaponization: The Biohazard of Russian Disinformation Campaigns*. Retrieved from Center For The Study Of Weapons Of Mass Destruction: <https://wmdcenter.ndu.edu/Publications/Publication-View/Article/2422660/social-media-weaponization-the-biohazard-of-russian-disinformation-campaigns/>

Hambling, D. (2022, March 8). *How Small Drones Could Win The Fight In Ukraine's Cities (And The Truth About That Anti-Drone Pickle Jar Story)*. Retrieved from Forbes: <https://www.forbes.com/sites/davidhambling/2022/03/08/how-small-drones-could-win-the-fight-in-ukraines-cities-and-the-truth-about-that-anti-drone-pickle-jar-story/?sh=2b6ee625641e>

Heir, M. C. (2019, January 4). *Op-Ed: Hitler would have loved social media*. Retrieved from Los Angeles Times.

Hermann, J. (2017, July 27). *Nine Links in the Chain: The Weaponized Narrative, Sun Tzu, and the Essence of War*. Retrieved from The Strategy Bridge: <https://thestrategybridge.org/the-bridge/2017/7/27/nine-links-in-the-chain-the-weaponized-narrative-sun-tzu-and-the-essence-of-war>

Johnson, T. (2020, August 14). *A Third of TikTok's U.S. Users May Be 14 or Under, Raising Safety Questions*. Retrieved from New York Times: <https://www.nytimes.com/2020/08/14/technology/tiktok-underage-users-ftc.html>

Lonstein, W. (2015, September 8). *Are We Experiencing a Digital Spring?* Retrieved from LinkedIn: <https://www.linkedin.com/pulse/we-experiencing-digital-spring-wayne-lonstein/>

Lonstein, W. (2022). Photo. New York: Envato Elements.

Manson, K. (2022, January 5). *Low-cost warfare: U.S. military battles with 'Costco drones.'* Retrieved from F.T.: <https://www.ft.com/content/aef5901e-4b9c-4561-a559-a6b7197baf61>

Perez, S. (2021, June 21). *TikTok just permitted itself to collect biometric data on U.S. users, including 'faceprints and voiceprints.'* Retrieved from Tech Crunch: <https://techcrunch.com/2021/06/03/tiktok-just-gave-itself-permission-to-collect-biometric-data-on-u-s-users-including-faceprints-and-voiceprints/>

Pomerleau, M. (2018, January 5). *How \$650 drones are creating problems in Iraq and Syria*. Retrieved from C4ISRNET: <https://www.c4isrnet.com/unmanned/uas/2018/01/05/how-650-drones-are-creating-problems-in-iraq-and-syria/>

Rodrigo, C. M. (2021, June 1). *Pentagon report clears use of drones made by the top Chinese manufacturer*. Retrieved from The Hill: <https://thehill.com/policy/defense/556370-pentagon-report-clears-use-of-drones-made-by-top-chinese-manufacturer?rl=1>

Rodriguez, S. (2021, June 25). *TikTok insiders say Chinese parent ByteDance tightly controls social media companies*. Retrieved from CNBC: <https://www.cnbc.com/2021/06/25/tiktok-insiders-say-chinese-parent-bytedance-in-control.html>

Young, V. A. (2020, May 27). *Nearly half of the Twitter Accounts*

*Discussing 'Reopening America' May Be Bots.* Retrieved from Carnegie Mellon University: <https://www.cmu.edu/news/stories/archives/2020/may/twitter-bot-campaign.html>

## 2I. Tools of the Trade

By Mike Monnik, Arison Neo [\[1\]](#)

### STUDENT OBJECTIVES

- 1) Why the Threat Intelligence matters for UAS
- 2) How to collect UAS Threat Intelligence
- 3) Using tools for historical and current Intelligence Collection
- 4) Using tools for current and future Intelligence Collection

### Introduction

This chapter will observe several tools that can aid in the observation, prevention, and attribution of adversary use of drones. Identifying what tactics, techniques, and procedures an adversary might use can be useful in replicating their mindset. To replicate their mindset, it is important to catalog as many data points as possible of historical incidents or activities where the threat actor was involved. Intelligence-led is defined as applying criminal intelligence analysis as a rigorous decision-making tool to facilitate crime reduction and prevention through effective (policing) strategies. (Intelligence-Led Policing, 2020)

Drones are Cyber-Physical systems. This means that they operate via digital links, protocols, and on technology stacks that would represent that of a computer system. However, they are kinetic and can operate in physical space indoors, outdoors, near people, and at high altitudes near airplanes. As a result, tracking the malicious use of UAS requires a Cyber-Physical approach merging both traditional cybersecurity and threat intelligence aspects with Hostile Vehicle Mitigation (HVM). The era of mass tracking airplanes and even ships has grown rapidly over time, with websites like FlightRadar24 (flightradar24, 2022) and FleetMon (fleetmon – tracking the seven seas, 2022). However, these asset classes are expensive, rarely

change callsigns (albeit due to regulation and international standards), and have identification technology to make this task more approachable. On the other hand, drones can be purchased for as little as USD 50 but could be positioned at the same altitude and geolocation as the planes mentioned above and ships. As of March 2022, there are currently 1000 drones in the air for every passenger aircraft, demonstrating the sheer volume and task of tracking and managing drones.

There are some attempts to standardize and legislate Remote Identification (RID) for drones to manage them, similar to vehicle license and registration. However, these technologies are still in their infancy. Clear distinguishing between International Friend or Foe (IFF) is still very difficult. As observed in the Ukraine-Russia conflict, it can be hard to compare a drone in the air to friendly forces, a journalist, a civilian, or an adversary. As a result, tracking all drones is not yet possible – most commercial drone detection or counter-drone (C-UAS) systems provide hyperlocal (2-10 km range) tracking capabilities, with military systems more than 100km, but usually with a focus on those with larger cross-body sections. However, it is important to track malicious drone incidents, the threat actors behind them, and the Tactics, Techniques, and Procedures (TTPs) they employ. By tracking specific scenarios, the equipment used, and the data behind them, a team can create mock scenarios to test the effectiveness of C-UAS against realistic incidents and flight profiles.

There are three main varieties of Test & Evaluation practices for assessing the effectiveness of a drone mitigation system. The first is a Table-Top exercise, otherwise referred to as a “War Room,” which brings all relevant stakeholders into a room to theorize an incident, practice their response and evaluate lessons learned. This is a largely theoretical activity but has the ability for anyone to participate, including management, legal, security, marketing, and more. The key outcome of a tabletop exercise is to identify key roles

and responsibilities, playbooks for following during an incident, and gaps that can be improved upon in communication. These exercises are best suited to organizations that have started thinking about protecting their assets. They might want to evaluate the best defense mechanism, whether people, processes, or technology (e.g., Counter-UAS).

An Aerial Threat Simulation focuses on the practical, pitting a mock adversary “Red Team or OPFOR” against the defense “Blue Team or BLUFOR.” In these exercises, usually at a live deployment or test facility, both teams know and agree on various scenarios, equipment, and flight profiles. These are then executed against the system involved, and its response is studied carefully in each category – such as Detect, Identify, Track, Mitigate and Recover. There are no surprises, but the objective is to evaluate if the system does what it says on the box and the extent of the variance. These exercises are best suited to organizations that have completed a Table-Top exercise and are looking to validate a vendor’s claims or refine their Blue Team doctrine.

A Red Team exercise is kept confidential to upper management only, and the BLUFOR team is not informed that a test might occur, how, or when. This is the upper echelon of C-UAS Test & Evaluation and focuses on the end-to-end solution and the team’s capability to detect and mitigate unknown, unexpected threats. The Red team uses various equipment, including fixed-wing, quadcopters, and multi-copters of varying make, model, color, size, and speed. Various flight profiles are also used, including fast, slow, First-Person View (FPV), Beyond-Visual-Line-of-Sight (BVLOS), One-to-Many (swarms), and by direction (such as the nape of the earth, directly above, zigzag, and extremely high altitudes). A variety of ranges might include launching extremely close or very far from the target perimeter. The Red Team may employ a variety of payloads, such as delivered by payload dropping mechanisms, kamikaze



(loitering munitions) where the drone ferries the payload into the target, or remote trigger Improvised Explosive Devices (IEDs).

Obfuscation and anti-attribution techniques such as automated and semi-automated flights, GPS or RF 'dark' systems, and protocols such as GSM or custom Software Defined Radio (SDR) frequencies may be used. In some cases, the Red Team also does not know what capability the BLUEFOR team possesses, which allows them creativity and realism in selecting their equipment and attack techniques. The objective of the exercise is to mimic a real-world threat actor by budget, technology closely, and technique, catching the BLUEFOR team by surprise and effectively evaluating their (and the technology's) response. These exercises are best suited to organizations that have completed multiple Tabletop exercises and Aerial Threat Simulations and want assurance on their defensive playbook, people, technology, communication, and reaction.

By gathering UAS threat intelligence data of known incidents, threat actors, and their TTPs, we can design comprehensive and accurate scenarios for use within the Test mentioned above & Evaluation activities. The collection of UAS incident data should be categorized by type, equipment, and geolocation so that the Red Team's actions are relevant. There is little benefit in testing a narcotics payload delivery against a critical infrastructure asset that faces explosive or surveillance threats. Most drone threat actors can be differentiated between the clueless, the careless, the criminal, and the terrorist. Most incidents can be categorized into the following: Intrusion (Trespass, ISR), Aviation (Near-miss, Sighting), Collision (Building, vehicle, asset), Contraband (Narcotics, Equipment, Arms), Weaponization (payload, IED, loitering munition), or Mitigation (jamming, spoofing, counter-UAS). The drone may be a fixed-wing system, quadcopter, or multicopter, of different make and models.

Most counter-UAS vendors, and many pro-active security teams today, have a UAS threat intelligence partner or organization which

captures, analyses, and disseminates intelligence to them, replacing the need for, and skilling up, a dedicated human resource. This information can be separated into three key categories – alerts, analysis, and information. Alerts are actionable, time-critical alerts that may trigger a response by the receiver, usually calculated by the analyst as being high impact or priority. The analysis is an in-depth assessment of an event, threat actor, or technology that can provide useful insights to inform product development lifecycles or Standard Operating Procedures (SOPs). Information about where incidents are occurring and how often can be further extrapolated to understand important information such as threats in geographic regions, frequency, and enough data, to be used by AI/ML to identify and mitigate threats automatically.

Before data extraction can take place, it's important to remember these key aspects of information processing:

**Accuracy:**

- Is there other intelligence or sources to support the event?

**Reliability:**

- How credible (or historically reputable) is the source?

**Timeliness:**

- When was this observed? Is it new, or does it include old/stock media?

In some cases, a random tweet by a civilian on Twitter may not be able to be corroborated – yet might contain timely and important information regarding an emerging threat. In this case, the information could be reported as “unvetted” – giving the relevant customers awareness but a caveat that the information may not

be true or entirely complete. This is especially important in times where a flurry of social media posts might indicate an occurring terrorist attack before other sources have been able to confirm

### **Tools for UAS Threat Intelligence**

Any intelligence analyst tasked with gathering UAS threat and incident data will eventually need to automate, aggregate, triage, analyze and then disseminate the produced information. This section introduces both free and paid, open and closed-source tools that can do this. Intelligence can be strategic or tactical, ranging in type and frequency. These include monthly trends, weekly briefs, daily 'presidential' style updates, or common operating pictures (COP) filtered by region, equipment type, threat actor, or incident kind. Different customers will require unique intelligence use-cases depending on their environment and risk appetite.

For example:

- Airports might require detection of all drones within a 10km radius of the airport
- Prisons might require threat actor TTPs and incidents occurring within their country
- Ports might require online chatter or sentiment regarding pirates using drones to disrupt shipping

Lastly, intelligence with enough identification of trends, patterns, and attributes of threat actors can be used to highlight the vulnerabilities that could be used to exploit and mitigate them.

**Figure 21.1 A typical UAS Threat COP over one month.**



**Source: DroneSec (DRONESEC, 2022)**

### **Open-Source Tools**

Open-source tools collect data from the internet that does not require authorization to access. These can be both free and paid. Examples include:

- Aviation Authorities
- AIRPROX
- Law Enforcement
- Ministry of Defense
- Social Media (Twitter (twitter, 2022), Facebook(Facebook , 2022), Instagram (Instagram, 2022), TikTok (tiktok, 2022), Snapchat)
- Open Chat Groups (Telegram (telegram, 2022), Discord (Discord, 2022), Slack (Slack, 2022))
- Internet forums
- News
- Media (YouTube (youtube, 2022), LiveLeak (Wikipedia, 2022))
- Livestreams
- Search Engines (surface and open TOR (torproject, 2022)/Dark

Web (whats-the-dark-web-how-to-access-it-in-3-easy-steps, 2022))

- Threat Intelligence feeds (DroneSec, (DRONESEC, 2022)  
LiveUAMap (liveuamap, 2022))

### **Closed-Source Tools**

Closed source tools often require payment to access but can draw on open-source information. The medium itself may be a closed source, requiring authorization.

- Counter-UAS detection feeds
- Closed Social Media groups, Chat groups (Signal (signal.org, 2022)), and Forums
- Closed TOR/Dark Web sources
- Curated Threat Intelligence feeds (e.g., DroneSec (DRONESEC NOTIFY, 2022), Dataminr (Dataminr, 2022))
- Journalists, Word-of-Mouth

### **Collection data types**

When collecting information about a drone incident, it is important to log the event's context or metadata.

Common but important data points for collection include:

#### **Table 21.1 Important Data Points for Collection**

| <b>Type</b>                                      | <b>Example</b>   |
|--|--|
| Geographic Location (General, Exact Coordinates) | <i>Melbourne, Australia (-37.7837, 144.9618)</i>         |
| Date, and Time (UTC)                             | 31/03/2022 14:37:21                                      |
| Make, Model, Sub-Model                           | DJI Mavic 3 Professional                                 |
| Location Category                                | Mass Assembly  |
| Activity Category                                | Intrusion  |
| Activity Result                                  | Sporting game paused for 20 minutes                      |
| Seizure of the drone                             | No   |
| Apprehension of the operator                     | No   |
| Visuals  | Yes (pictures, videos)                                   |
| Payload  | Ukrainian Flag attached by string to landing gear        |
| Size   | sUAS   |
| Color  | Painted sky blue   |
| Serial Number                                    | Unknown  |
| Other system components (e.g., controllers)      | Unknown  |
| Known hardware mods                              | Appeared to have extended battery pack known known known |
| Known software mods                              | Unknown  |
| Threat Actor Group                               | Local activists  |
| Detection type                                   | Civilian visual observation, social media (links)        |
| C-UAS Detection                                  | No   |
| C-UAS Mitigation                                 | No   |

Source: DroneSec (DRONESEC, 2022)

By collecting as much data as possible, post-event forensics can be performed and cross-referenced with other detection systems, CCTV, visual observations, or law enforcement records are possible. Further activities include using AI/ML to learn from these datasets

to perform on-the-fly risk-based decision modeling and prediction capabilities.

By gathering this unique data, trends and patterns can emerge, and data-drive questions can be answered, such as the following examples:

- Are we seeing an increase in narcotics-style incidents within the country of Ethiopia?
- Are C-UAS implementations or new legislation working, given our data on seizures or apprehension?
- Is the increase in DJI Mavic 3 drones in Afghanistan due to a supply chain from Israel?
- What is the most dangerous or most expected UAS threat right now?

### **Tools for historical and current UAS threat intelligence**

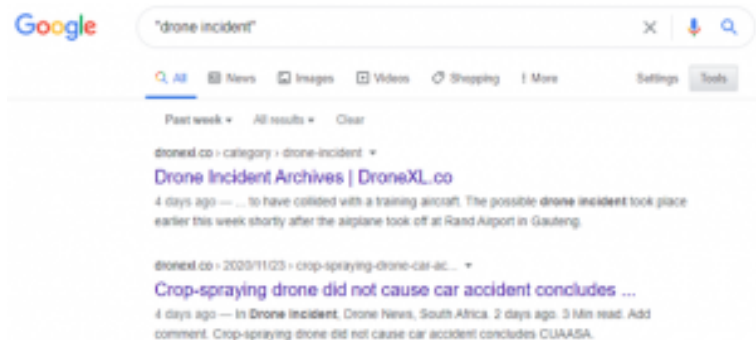
#### **Configuring Google (Open-Source, free)**

However, search engines are a powerful tool for locating data regarding drone incidents and can provide a significant signal-to-noise ratio. The analyst must have a specific direction in their collection to focus on key filters, such as sources, timelines, or information types. For example, the query “drone incident” may produce thousands of results; however, filtering it to items in the last seven days or appending a specific country will provide significantly more valuable and relevant results. It is highly recommended that users study “Google Dorks” (Google Dorks Primer, 2022) to make the best use of the search engine’s advanced search and filter capabilities.

To refine the query “drone incident” in Google to the past 24 hours:

1. Click on the “Tools” tab
2. Click on “Past 24 hours.”

**Figure 21.2 Using search engines to list incident events in the past seven days.**



Source: DroneSec (DRONESEC, 2022)

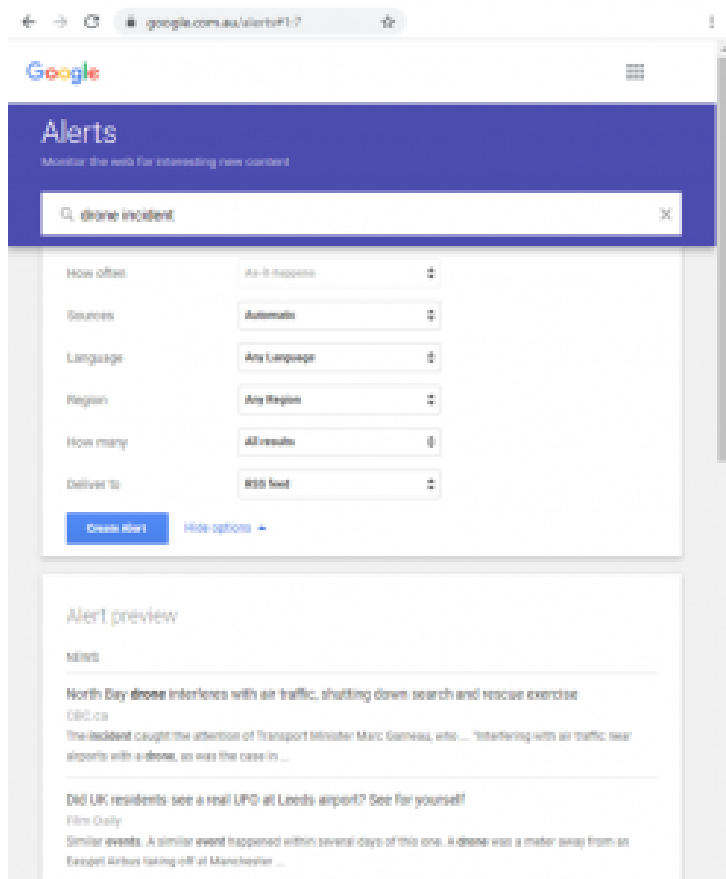
This process can be repeated in an automated fashion with the word “drone” being replaced by “UAS,” “UAV,” “RPAS,” “quadcopter,” “multicopter,” or even “fixed-wing.” Keep in mind that each country has nuances regarding the way they designate drones – for example, in the USA, a small drone might be referenced by “UAS” and “C-UAS,” In contrast, in Australia, the terminology is often “RPAS” and “C-RPAS,” respectively.

Alternatively, users can set up ‘keyword alerts’ in Google to receive alerts via email or RSS. This can be done via the web URL <https://www.google.com.au/alerts>. Users may want to stack their queries, such as having the keywords: *drone incident*, *drone collision*, *drone terrorist*, *drone airport*. ([google.com.au/alerts](https://www.google.com.au/alerts), 2022)

This methodology can be applied to most search engines with various customization options available.

**Figure 21.3 Google.com au/ alerts**





Source: (google.com.au/alerts, 2022)

### Configuring LiveUAMap (Open-Source, paid)

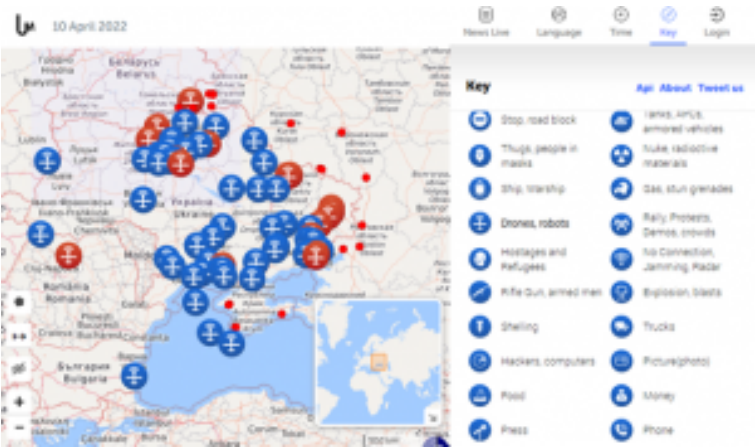
Live Universal Awareness Map (LiveUAMap) is a global news and information site related to factual reporting of incidents and events. The system covers various categories, not just aerial drones – but can be filtered to demonstrate just drone threats. The system has a free version but is limited in what it can show. The system generally retrieves tweets from Twitter, often the fastest reporting source for

events occurring in real-time around the world. (liveuamap, 2022)  
Analysts should always use multiple tools for incident collection, to cross-reference and verify reports and increase their list of sources  
– LiveUAMap only covers twitter but does so very well.

To configure LiveUAMap for a COP view:

1. Select the geographic region “world” or navigate to <https://world.liveuamap.com/>
2. Select the tab “Time” and highlight the specified time/date
3. Select the tab “Key” and select the category “drones, robots,” and press Apply

**Figure 21.4 A global view of tweeted drone incidents**



**Source:** LiveUAMap (liveuamap, 2022)

### **Tools for current and future UAS threat intelligence**

To gather intelligence that might pertain to future incidents and malicious use of UAS, analysts need to gather data that might be best represented in the discussion or planning of an event in the

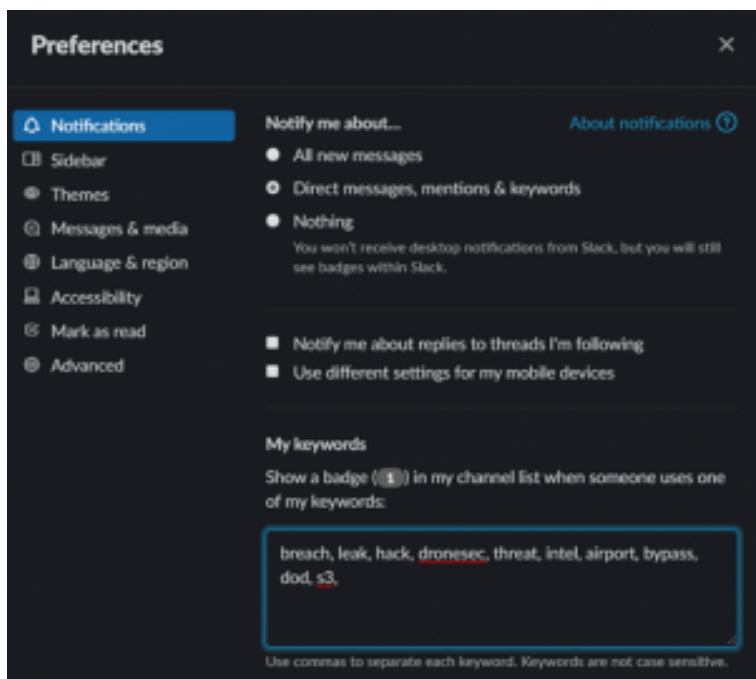
future. While social media can support this, authorization or invitation is often required to join underground or closed groups that share detailed information. Payment is required for advanced UAS Threat Intelligence gathering platforms as their operatives or technology actively participate in and, as a result, gather information relating to potential malicious use of UAS. This section will cover free and paid mechanisms for gaining closed-source information to support UAS threat intelligence collection.

### **Configuring Slack (Closed-Source, free)**

Slack can be configured with silent keyword alerts so that any time the word is mentioned, you receive a notification. This can be useful for groups that actively plan malicious UAS use for predicting future events. Slack is a closed-source tool as you are required to join that group to monitor it, of which others can observe your presence. It is highly recommended to use incognito sock-puppet accounts when joining any source that requires authorization.

1. Go to Profile -> Preferences -> Notifications
2. Change to “Direct messages, mentions & keywords.”
3. Paste a word list into the “My keywords” section

**Figure 21.5 A collection of words for slack.**



**Source: DroneSec (DRONESEC, 2022)**

Your wordlist is a collection of terms that match what you might be looking for. These can be hundreds or thousands of keywords in volume and use Natural Language Processing (NLP) for other language translations in advanced intelligence-gathering operations.

This will notify you (or a selected webhook) when your keyword matches any public message in any channel. Similar yet alternative options are available for Discord, Skype, Telegram, and Signal.

### **DroneSec Notify (Open/Closed-Source, free/paid)**

DroneSec is the premier UAS security incident tracking organization globally. DroneSec has other capabilities in drone

security and counter-drone training (training – dronesec, 2022), tooling and intelligence that support Law Enforcement, Military, Government, and Private Industry, and runs the largest drone security conference (Global Drone Security Network) in the world. The DroneSec Notify UAS Threat Intelligence Platform (TIP) automatically crawls the internet (open and closed sources) and reports on UAS incidents. Rather than a static physical detection system, the platform acts as a COP, providing data fusion between hundreds of open and closed sources. The organization produces both a free weekly intelligence brief (dronesec-notify (pages), 2022) and a paid subscription (dronesec-notify (pages), 2022), which provides 24/7 real-time threat alerts, notifications, and a database.

The Notify system is highlighted in this chapter as it is the only dedicated Threat Intelligence Platform designed for UAS threat and incident collection, analysis, and dissemination. It was developed (Neo, 2022) for analysts, security teams, and counter-drone systems to monitor, share and report events on a global scale. The system includes the following functions:

- – **Dashboard** COP for a collection of recent incidents, visual map, and visual statistics
- – **Search** for querying the database of over 4000+ drone incidents by various filters and categories
- – **Artefacts** for viewing Medium and Low priority drone incidents and events
- – **Reports** for viewing High priority incidents and contextual analysis
- – **Tracked Assets** for setting up alerts and notifications when a query match is found
- – **Knowledge Base** for a collection of tailored Reports, Whitepapers, Guidelines, and Research on the topics of drone security, counter-drone, drone cybersecurity, regulations, and more
- – **Statistics** for viewing the number of artifacts over time, by

various categories, trends, and types

Interpreting the free weekly summary includes the following incident categories:

- Non-conflict-zone
- Conflict-zone
- Cyber and data security
- Social media
- Whitepapers, Publications, and Regulations
- Counter-Drone Systems
- UTM Systems
- Informational
- Technology

**Figure 21.6 The free, weekly UAS Threat Intelligence brief**  
**Source**



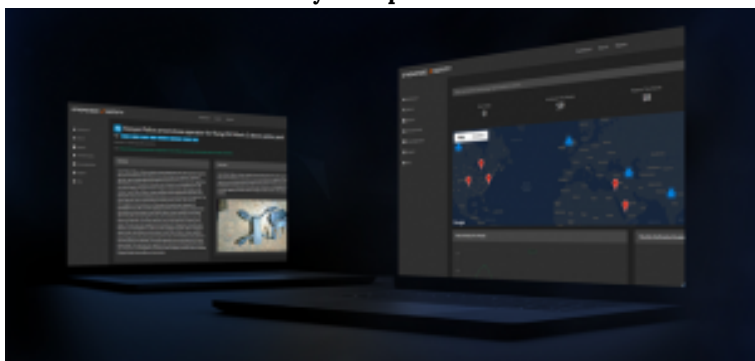
Source: (DRONESEC, 2022)

This provides a holistic view of physical and cyber threats, incident actors, mitigations, and threats to swarms and connected nodes.

The system provides:

- Monitoring and tracking keywords, geographic locations, trends, statistics, and curated analysis
- Access to intelligence on cyber vulnerabilities, exploits, and modeling tools
- Access to a detailed UAS Threat Actor Glossary, including tactics, techniques, and procedures (TTPs)

**Figure 21.7 The UAS TIP provides global incident tracking and analysis capabilities.**



Source: (DRONESEC, 2022)

To configure Notify, users access the dashboard, where they are presented with a global view of incidents in the past two weeks. Multiple incidents occurring within close proximity to each other are grouped and can be individually viewed. Additional filters include events occurring in the past 72 hours, artifacts and high-priority reports over the past 30 days, and documents within the knowledge base.

**Figure 21.8 The DroneSec Notify UAS TIP Dashboard**

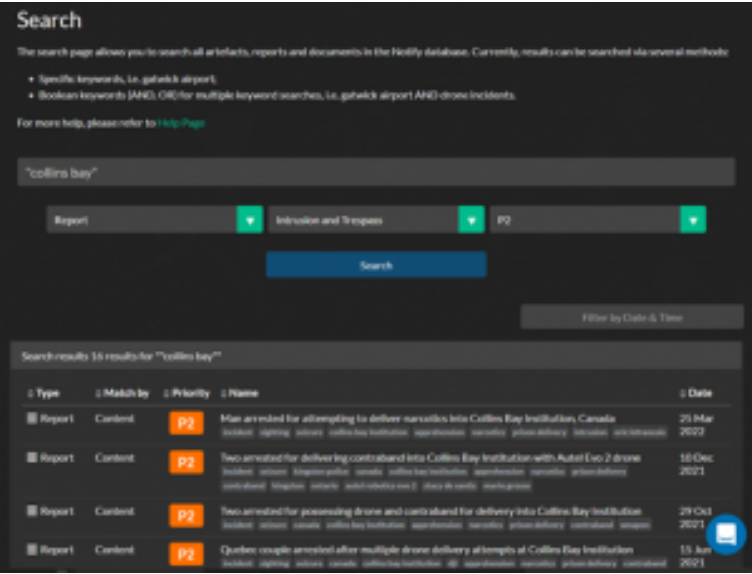


Source: (DRONESEC, 2022)

Searching the database is easy and based on keywords. These keywords can be exact, inclusive of, or supporting Boolean operations such as the use of “AND,” “OR” operators for refining results. Users can also click and include tags that provide thousands of possibilities based on country, make, model, incident type, payload, or even specific threat actors.

**Figure 21.9 Performing a search for a specific prison Source**





Source: (DRONESEC, 2022)

Reports are curated incidents that are critical-to-high priority items that will most likely trigger an alert or constitute in-depth analysis by UAS Threat Intelligence Analysts. These reports can range from P1 (Critical) to P2 (High) and usually result in a successful contraband drop, violence or death caused by a payload, or significant events such as aviation near-misses and airport intrusions. The Reports page provides a user with a running list of the most recent and important UAS events globally.

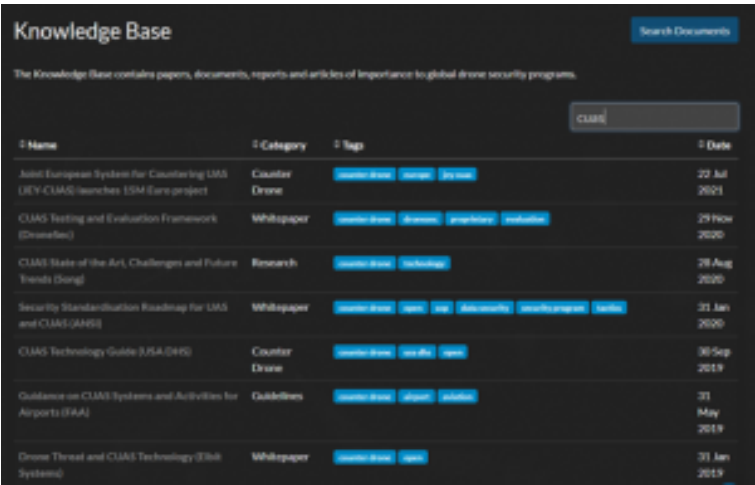
**Figure 21.10 Viewing a running list of recent high-priority reports.**



Source: (DRONESEC, 2022)

The platform also contains a Knowledge Base, a central repository for all drone physical, cyber, and countermeasure security documentation. The space was intended to be a data lake for SOPs, frameworks, guidelines, and research relating to the area. This allows teams to speed up their creation of a drone security program, red team, or conduct comprehensive literature reviews in a central place. The Knowledge Base also includes all DroneSec-generated content, such as Special Reports, cybersecurity databases, and counter-drone test & evaluation frameworks.

**Figure 21.12 A search for C-UAS related content in the Knowledge Base**



| Name  | Category      | Tags  | Date        |
|---|---------------|---|-------------|
| Joint European System for Countering UAS (JECUAS) launches ESF-Euro project | Counter Drone | <a href="#">counter-drone</a> <a href="#">drone</a> <a href="#">jrc</a>   | 22 Jul 2021 |
| CUAS Testing and Evaluation Framework (Dronedec)                            | Whitepaper    | <a href="#">counter-drone</a> <a href="#">drone</a> <a href="#">guidelines</a> <a href="#">test-eval</a>  | 29 Nov 2020 |
| CUAS State of the Art, Challenges and Future Trends (Dronedec)              | Research      | <a href="#">counter-drone</a> <a href="#">technology</a>  | 28 Aug 2020 |
| Security Standardisation Roadmap for UAS and CUAS (ANSSI)                   | Whitepaper    | <a href="#">counter-drone</a> <a href="#">cyber</a> <a href="#">info</a> <a href="#">security</a> <a href="#">security</a> <a href="#">security</a> | 31 Jan 2020 |
| CUAS Technology Guide (USA DHS)   | Counter Drone | <a href="#">counter-drone</a> <a href="#">cyber</a> <a href="#">info</a>  | 30 Sep 2019 |
| Guidance on CUAS Systems and Activities for Airports (FAA)                  | Guidelines    | <a href="#">counter-drone</a> <a href="#">drone</a> <a href="#">guidelines</a>  | 31 May 2019 |
| Drone Threat and CUAS Technology (Eilat Systems)                            | Whitepaper    | <a href="#">counter-drone</a> <a href="#">info</a>  | 31 Jan 2019 |

Source: (DRONESEC, 2022)

Finally, the system contains a documented UAS Threat Actor Glossary, centralizing all known threat information about the group and its technology, tactics, techniques, and procedures. It also links users to previous events attributed to the group and potential future capabilities. Lastly, the statistics page is useful for analysts to understand the trends involved in drone incidents from a number's

perspective, giving them insight into resource allocation and potential predictions of future UAS misuse. DroneSec Notify is an important tool in any analyst, first responder, or Law Enforcement Agent's kit for staying at the bleeding edge of malicious use of UAS by threat actors.

### **Stolen Drone Info (Open/Closed-Source, free/paid)**

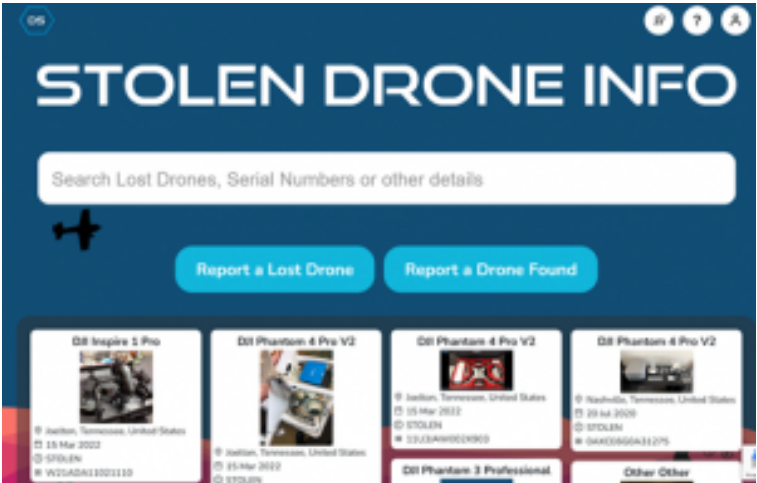
Intelligence demonstrates that a large percentage of the drones used by criminals for crimes such as dropping contraband into prisons or across borders are stolen. Drone operators and retailers have reported their homes, cars, and shops being burglarized with their drones stolen; these drones are usually resold on the black market, used for illegal payload delivery drops, or even contribute to the procurement and supply of drones to terrorist entities. The primary reason crime groups seek to use stolen drones is to mask their identity to reduce the risk of capture. (Crime Facts Info, 2022) This is because the original drone operator's identity is linked to the system given a variety of attributional factors:

- – The original operator's financial information was linked to the purchase
- – Store accounts, CCTV, or receipt tracking may link to the operator
- – The operator's drone account was linked to the drone, controller, or device
- – The operator had registered the drone's serial number with the manufacturer or aviation authority
- – The operator's digital media and/or GPS telemetry may still exist within the drone's storage

Stolen Drone Info is an online database that can be used by drone operators, drone detection systems, agencies, and organizations to report and detect drones that have been stolen. The tool can aid

in tracking drones, connecting users back to their merchandise, and keeping the skies safe from stolen ones. Additionally, the tool decodes serial numbers, letting users know if the drone they are purchasing is legitimate or stolen. Being an automated system, the tool can crawl open-source locations to determine if entries match the database of stolen systems up for sale. If already sold or used by malicious individuals, a network of drone detection nodes can match entries in the database with drones in the air.

**Figure 21.13 The Stolen Drone Info tool dashboard**



Source: (DRONESEC, 2022)

Open-source data can be trawled from the internet and social media such as Facebook and Craigslist, where marketplace and chat forums exist. Serial numbers are usually mentioned in these places, and users try to engage the mass media to search for the owner of the drone found or in hopes that someone would have found their lost or stolen drone. These avenues usually result in low success rates as the finder and the seeker may not be in the same forums, chat rooms, or marketplaces. With a consolidated registry that

combines these avenues and links, everyone increases the chances of matching the drone to its rightful owner.

Connecting drone detection systems and law enforcement agencies are critical in providing real-time threat intelligence and enhancing decision-making abilities. Drone detection systems can detect drones operating in an area and automatically retrieve their data, including make, model, serial number, and location. In some systems, the operator's location can be detected as well. This data can be automatically mapped to the registry's database and alert the relevant authorities when a stolen drone's serial number appears in the detection system. Additionally, counter-drone systems often perform several decisions based on data available to them to ascertain if the drone is malicious or not. The drone is stolen at the point of detection tolen provides a more confident data source for the counter-drone operator's decision tree.

**Figure 21.14 Example of a stolen drone reported on the SDI**



distinguishing one from another. The same number is read by detection systems (or physically) by the drones transmitting links. Certain brands' serial numbers have data embedded within the drone's manufacture date, make, and model that can be decoded easily. In contrast, others may only have the batch number or location of assembly and distribution. This information may be important in determining the origins of the drone, such as where it was purchased from and possibly linking out the supply chain to the drone operator or threat actor. Other information such as distinctive features or accessories helps differentiate one similar model from another, which adds to the identifiability of the drone.

The Stolen Drone Info tool is a useful component in reducing the anonymity of threat actors using stolen drones and increasing the chances of detecting such drones by detection systems. It can aid analysts in observing geographic hot spots, specific make and models of drones, and even reunite drones with their original owners.

## **Conclusions**

To be aware of potential threats and understanding the threat is required. This can be extracted from strategic and tactical Threat Intelligence using various tools discussed in this chapter. The theory of unmanned system tracking is still early, and its application will continue to apply to the underwater, surface-based, ground, and even satellite-based systems. Cyber-physical systems have close linkages to both cybersecurity and physical security intelligence operations. Data fusion is a requirement to provide an accurate, timely operating picture of the threats posed and how to counter them. Historical context can aid the creation of trends and patterns that can be observed for unique items, leading to future predictions and safer skies.

## **Bibliography**



Crime Facts Info. (2022, 03 01). Retrieved from Australian Institute of Criminology: <https://www.aic.gov.au/sites/default/files/2020-05/cfi055.pdf>

Dataminr. (2022, April 10). Retrieved from [www.dataminr.com](http://www.dataminr.com): <https://www.dataminr.com/>

Discord. (2022, April 10). Retrieved from [discord.com](https://discord.com): <https://discord.com/>

DRONESEC. (2022, April 10). Retrieved from [dronesec.com](https://dronesec.com): <https://dronesec.com/>

DRONESEC NOTIFY. (2022, April 10). Retrieved from [dronesec.com/pages/notify](https://dronesec.com/pages/notify): <https://dronesec.com/pages/notify>

*dronesec-notify* (pages). (2022, April 10). Retrieved from [dronesec.com/pages/dronesec-notify](https://dronesec.com/pages/dronesec-notify) : <https://dronesec.com/pages/dronesec-notify>

Facebook . (2022, April 10). Retrieved from [www.facebook.com](https://www.facebook.com): <https://www.facebook.com/>

FleetMon – tracking the seven seas. (2022, April 10). Retrieved from [www.fleetmon.com](https://www.fleetmon.com): <https://www.fleetmon.com/>

flightradar24. (2022, April 10). Retrieved from [www.flightradar24.com](https://www.flightradar24.com): <https://www.flightradar24.com/>

Google Dorks Primer. (2022, April 10). Retrieved from [www.secjuice.com/osint-engagement-101](https://www.secjuice.com/osint-engagement-101):

<https://www.secjuice.com/osint-engagement-101/> Video: <https://www.youtube.com/watch?v=Cz2bgvEzbuo>

[google.com.au/alerts](https://www.google.com.au/alerts). (2022, April 10). Retrieved from [www.google.com.au/alerts](https://www.google.com.au/alerts): <https://www.google.com.au/alerts>

Instagram. (2022, April 10). Retrieved from [www.instagram.com](https://www.instagram.com): <https://www.instagram.com/>

Intelligence-Led Policing. (2020, May). Retrieved from <https://www.aic.gov.au/sites/default/files/2020-05/cfi055.pdf>:

<https://www.aic.gov.au/sites/default/files/2020-05/cfi055.pdf>

liveuamap. (2022, April 10). Retrieved from [liveuamap.com](https://liveuamap.com): <https://liveuamap.com/>

Neo, A. (2022, April 10). *why-we-created-threat-intelligence-platform-drones*. Retrieved from [www.linkedin.com/pulse/](https://www.linkedin.com/pulse/)

<https://www.linkedin.com/pulse/why-we-created-threat-intelligence-platform-drones-arison-neo/signal.org>. (2022, April 10). Retrieved from signal.org: <https://signal.org/>  
 Slack. (2022, April 10). Retrieved from slack.com: <https://slack.com/>  
 snapchat. (2022, April 10). Retrieved from www.snapchat.com: <https://www.snapchat.com/>  
 telegram. (2022, April 10). Retrieved from telegram.org: <https://telegram.org/>  
 TikTok. (2022, April 10). Retrieved from www.tiktok.com: <https://www.tiktok.com/>  
 torproject. (2022, April 10). Retrieved from www.torproject.org: <https://www.torproject.org/>  
 training - dronesec. (2022, April 10). Retrieved from training.dronesec.com: <https://training.dronesec.com/>  
 twitter. (2022, April 10). Retrieved from twitter.com: <https://twitter.com/>  
 whats-the-dark-web-how-to-access-it-in-3-easy-steps. (2022, April 10). Retrieved from www.vpnmentor.com: [https://www.vpnmentor.com/popular/whats-the-dark-web-how-to-access-it-in-3-easy-steps/?keyword=dark%20web&geo=95821&device=&cq\\_src=google\\_ads&cq\\_cmp=367844759&cq\\_term=dark%20web&cq\\_plac=&cq\\_net=s&cq\\_plt=gp&keyword=dark%20web&campaignID=367844759&matchtype](https://www.vpnmentor.com/popular/whats-the-dark-web-how-to-access-it-in-3-easy-steps/?keyword=dark%20web&geo=95821&device=&cq_src=google_ads&cq_cmp=367844759&cq_term=dark%20web&cq_plac=&cq_net=s&cq_plt=gp&keyword=dark%20web&campaignID=367844759&matchtype)  
 Wikipedia. (2022, April 10). Retrieved from en.wikipedia.org/wiki/LiveLeak: <https://en.wikipedia.org/wiki/LiveLeak>  
 Youtube. (2022, April 10). Retrieved from www.youtube.com: <https://www.youtube.com/>

[\[1\]](#) DRONESEC© is the copyrighted name for the Australian – based company. Reference to its product line and company name is both

authorized by the company and requested by the authors as representative of the best of breed tools of the trade. In the Managing Editors' opinion, DRONESEC© represents one of the strongest drone monitoring services in the world. However, officially the authors under the current CC, KSU policies, and publisher – New Prairie Press, are not permitted to endorse any product by any company.