2022

Space Systems: Emerging Technologies and Operations

Randall K. Nichols
Kansas State University - Polytechnic Campus

Candice M. Carter

John-Paul Hood

Mark J. Jackson

Siny M. J. Joseph

See next page for additional authors

Recommended Citation

Nichols, Randall K.; Carter, Candice M.; Hood, John-Paul; Jackson, Mark J.; Joseph, Siny M. J.; Larson, Haley; Lonstein, Wayne D.; Mai, Randall; McCreight, Robert; Mumm, Hans C.; Oetken, Michael L.; Pritchard, Michael J.; Ryan, Julie J. H. C.; Sincavage, Suzanne E.; and Slofer, William, "Space Systems: Emerging Technologies and Operations" (2022). *NPP eBooks*. 47.
https://newprairiepress.org/ebooks/47

Authors

Randall K. Nichols, Candice M. Carter, John-Paul Hood, Mark J. Jackson, Siny M. J. Joseph, Haley Larson, Wayne D. Lonstein, Randall Mai, Robert McCreight, Hans C. Mumm, Michael L. Oetken, Michael J. Pritchard, Julie J. H. C. Ryan, Suzanne E. Sincavage, and William Slofer

Space Systems:
Emerging Technologies
and Operations

New Prairie Press,
Kansas State University Libraries
Manhattan, Kansas

Cover design by Dr. Suzanne E. Sincavage and Prof. Candice M. Carter

Electronic edition available online at: http://newprairiepress.org/ebooks/47/

ISBN: 978-1-944548-48-3

NEW prairie PRESS
open access scholarly publishing

SPACE SYSTEMS: EMERGING TECHNOLOGIES AND OPERATIONS

PROF. RANDALL K. NICHOLS; CANDICE M. CARTER; JOHN PAUL HOOD; MARK J. JACKSON; SINY JOSEPH; HALEY LARSON; WAYNE D. LONSTEIN; RANDALL MAI; ROBERT MCCREIGHT; HANS C. MUMM; MICHAEL OETKEN; MICHAEL J. PRITCHARD; JULIE J.C.H. RYAN; SUZANNE E. SINCAVAGE; AND WILLIAM SLOFER

New Prairie Press
Manhattan, KS

CONTENTS

Part I. SECTION 1: C4ISR AND EMERGING SPACE TECHNOLOGIES

Part II. SECTION 2: SPACE CHALLENGES AND OPERATIONS

Part III. SECTION 3: HUMANITARIAN USE OF SPACE TECHNOLOGIES

TITLE PAGE

SPACE SYSTEMS: EMERGING TECHNOLOGIES AND OPERATIONS

By

Nichols; Carter, Hood, Jackson, Joseph, Larson, Lonstein, Mai,
McCreight, Mumm, Oetken, Pritchard, Ryan, Sincavage, Slofer

A PDF version of this book will be available in Fall 2022 at [https://www.newprairiepress.org/ebooks/47/]

The Pressbooks edition is live and available at https://kstatelibraries.pressbooks.pub/spacesystems/

Cover design by (Dr. Suzanne Sincavage and Candice Carter)

Courtesy of

New Prairie Press

Kansas State University Libraries

Manhattan, Kansas

Pressbooks ISBN: 978-1-944548-48-3

Cover Art

SPACE SYSTEMS: EMERGING TECHNOLOGIES AND OPERATIONS

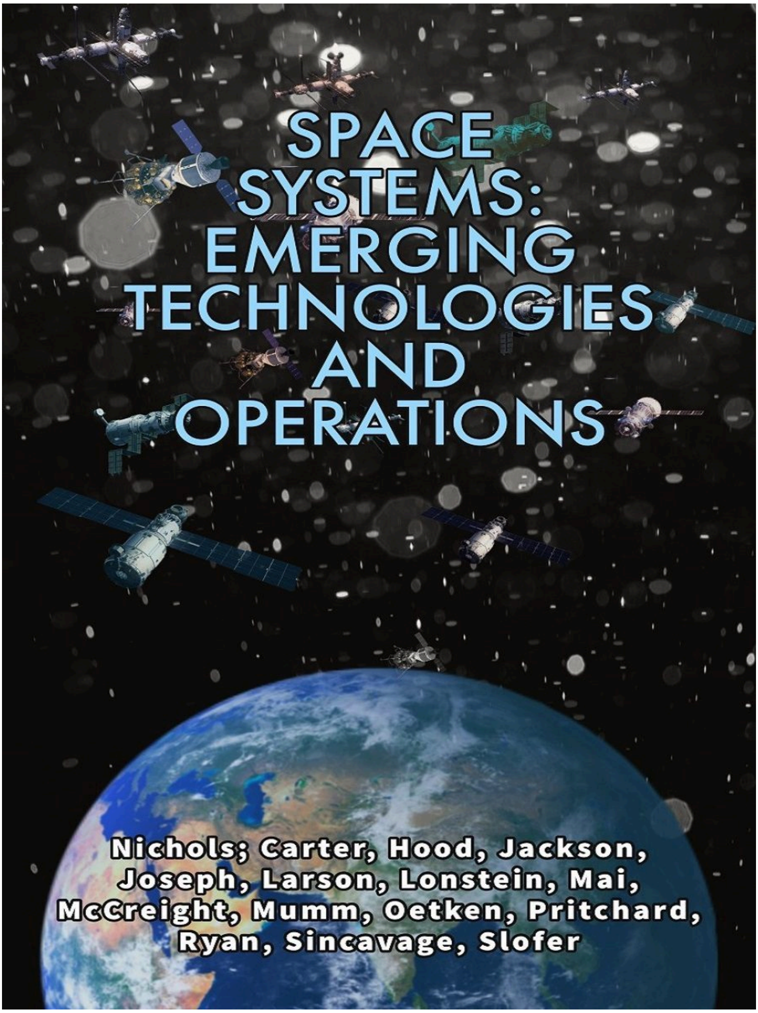
Nichols; Carter, Hood, Jackson, Joseph, Larson, Lonstein, Mai, McCreight, Mumm, Oetken, Pritchard, Ryan, Sincavage, Slofer

Source: Created by: (Sincavage & Carter)

Bibliography

Sincavage, & Carter, &. (2022.). Final Cover for Book 7 Nichols (Ed). *SPACE SYSTEMS: EMERGING TECHNOLOGIES AND OPERATIONS.* KSU – NPP, Los Angeles, CA.

COVER ART


SPACE SYSTEMS: EMERGING TECHNOLOGIES AND OPERATIONS
Nichols; Carter, Hood, Jackson, Joseph, Larson, Lonstein, Mai, McCreight, Mumm, Oetken, Pritchard, Ryan, Sincavage, Slofer

Source: Created by: (Sincavage & Carter)

Bibliography

Sincavage, & Carter, &. (2022.). Final Cover for Book 7 Nichols (Ed). *SPACE SYSTEMS: EMERGING TECHNOLOGIES AND OPERATIONS.* KSU – NPP, Los Angeles, CA.

COPYRIGHT / PUBLICATION PAGE

COPYRIGHT PAGE

A PDF version of this book will be available in Fall 2022 at [https://www.newprairiepress.org/ebooks/47/]

The Pressbooks edition is live and available at https://kstatelibraries.pressbooks.pub/spacesystems/

Cover design by (Dr. Suzanne E. Sincavage & Prof. Candice M. Carter)

Cover image:

Courtesy of (Sincavage & Carter, 2022)

New Prairie Press
Kansas State University Libraries
Manhattan, Kansas #TBD

Pressbooks ISBN: 978-1-944548-48-3

Bibliography

Sincavage, & Carter. (2022). Final Cover for Book 7 Nichols (Ed). *Space Systems: Emerging Technologies and Operations.* KSU – NPP, Manhattan, KS.

BOOKS ALSO BY PROFESSOR RANDALL K. NICHOLS AND THE KSU WILDCAT TEAM

BOOKS ALSO BY PROFESSOR RANDALL K. NICHOLS AND THE WILDCAT WRITING 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 TechnologiesWith 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; 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

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 52 years ~10,000 Dragons / Dragonesses in the field) who are securing the 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 regarding 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 and their families 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 all. 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 Michelle Jackson, a long-time friend, who introduced me to the managing Dragon.

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, Esq.

I dedicate this work to my wife and best friend Julie, my sons Ethan, Ari, and 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 Professor Candice Carter

I dedicate this work to an exceptional leader, mentor, and master of *Bushido*, Professor Randall K. Nichols. His commitment to training dragons to succeed in asymmetric warfare and life is unprecedented. For Dr. Suzanne Sincavage, co-author, a guiding mentor for biodefense research and life. To Treadstone71 for being a guiding light through the dark parts of the web. Finally, to the Los Libros, I love you immensely my shining stars.

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 Dr. 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 Dr. 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 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

The Endless Parade of questions that 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.

From: Professor Michael L. Oetken

I dedicate this work to my loving wife Dr. Jeridy Oetken, my children, Emily, Bethany, and Chase, and my parents Dellane and Carolyn. You have all given me the strength, courage, and determination to pursue my goals and aspirations throughout my career in industry and academia. Jeridy, my wife of over 25 years, you are my foundation and compass in life. Thank you for being my co-pilot in all our adventures together.

From: Dr. Siny Joseph

I would like to dedicate this book chapter to my parents Colonel A. V. Joseph (retired) and Lisa Joseph, without their sacrifices and dedication, I would never be what I am, my best friend and brother George Aikara, who inspires and amazes me every single day, my mentors on whose giant shoulders I stand, my students who motivate me to give my best, my biggest cheerleading twin daughters Sanya and Tanya Namboodiri who breathe life into me and make it all meaningful, and lastly, my husband Dr. Vinod Namboodiri, who challenges, pushes and enables me to do and be better, and takes greater pride in my achievements than his own!

From Dr. Haley Larson

I dedicate this work to my loving husband Cody – your support of my spirited pursuit of knowledge makes efforts like this possible. To my children Owen, Everett, Luke and Kate – I hope you are inspired to pursue a lifetime of learning, as you never know where your knowledge may lead you.

From Dr. Michael J. Pritchard

To Heidi, Sydney & Zander: I'm Mr. Meeseeks, look at me!

DISCLAIMERS (LONSTEIN)

DISCLAIMERS

Information contained in this work has been obtained by the authors from sources believed to be accurate and reliable. However, New Prairie Press, Professor Randall K. Nichols (Managing Editor / Publisher), Kansas State University, U.S. Army, and any of its contributors guarantee the information's accuracy or completeness. None of the parties mentioned above, nor its authors or contributors or their organizations 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 / Space Systems, Space Emerging Technologies and Operations; 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 concern 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 to be actual occurrences.

The authors, publishers, and associated institutions, U.S. Army 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.

Reviewed by Wayne Lonstein, Attorney at Law

FOREWORD BY JERRY DREW

Foreword

Jerry Drew, Military Space Operations Expert and Theorist

While the casual observer may not have noticed the elevation of United States Cyber Command to an independent combatant command in 2018 or the establishment (or rather, the reestablishment) of United States Space Command in 2019, these changes within the Department of Defense carried profound significance. The new organizational structures, each headed by a four-star general directly reporting to the Secretary of Defense, reflected a deeper realization that had been percolating in national security circles for a long time: the U.S. military, although cripplingly dependent on satellites and computer networks, needed to advance its thinking and its practice in these areas in order to field a joint force capable of fighting and winning in the twenty-first century.

Such advances, however, are incremental, especially in a military as large as that of the United States. To further compound the challenges of change, many military practitioners and civilian security experts still consider space and cyber as esoteric disciplines. Activities in these domains clearly enable land, air, and maritime operations but in a way that is often difficult to understand and often more difficult to explain. And although the national security space community has been engaged in an effort to provide these explanations since its inception, military space forces are now in the position of not just enabling operations in other domains but of playing an expanded role in integrated military operations with the rest of the joint force.

Under the direction of Professor Randall Nichols, Kansas State University has published a series of six textbooks that significantly contributes to the goal of explaining modern, multi-domain security activities. To date, the series has garnered more than 50,000 downloads and is averaging about 1,000 new downloads each month. In this installment, a group of fifteen dedicated experts advances the series into the realm of space operations—a discipline within the larger field of security studies that has consumed the past twelve years of my professional life. I could not be more grateful for their efforts. It is hard to imagine more experienced and dedicated professionals than the ones who have spent the past two years of their lives putting together this textbook, yet I know that similar groups are working around the world on problems of equal value to our nation, and the timing could not be better. Indeed, with China's rapid military expansion and Russia's invasion of Ukraine last spring, the sense of urgency among the security community seems to have reached a level only surpassed in recent memory by the tragedy of September 11, 2001.

But the times have changed over the past twenty years. As the Biden administration's Interim National Security Strategic guidance makes clear, the United States is no longer an undisputed world power, transregional problems abound, and "America's fate is inextricably linked to events beyond our shores."[1] To prepare for these challenges, graduate-level students and researchers require an in-depth treatment of the most technical aspects of modern, multi-domain warfare, including orbital warfare, cyber operations, unmanned aerial systems, unmanned underwater vehicles, hypersonic weapons, and how these capabilities shape the contemporary security environment. Indeed, if the phrase "Rise of the Machines" may still ring a bit histrionic, the on-going conflict in Ukraine provides at least some insight into what the conflicts of the future will entail: rapidly evolving drone warfare, mesh network communications, the criticality of the information environment—all underpinned by satellites, servers, and the electromagnetic spectrum. Perhaps more than any other nation, the United States military depends upon the technological advantages achieved by such systems. To deter our adversaries, and to defeat them, if necessary, technology is indispensable, but the knowledge of how to employ that technology is vital. War is still a human endeavor, and humans must carry the necessary knowledge.

In writing of the German General Heinz Guderian, British historian B.H. Liddell Hart observed that in the annals of military history, “Innovators have rarely had the chance to put into practice themselves the theories they have expounded.”[2] In the modern world, however, rapid innovation and implementation, underpinned by soundly developed theory, will be critical for future battlefield success. Because of the availability of advanced technologies like drones, the fluidity of the cyber and electromagnetic environments, and the hyper-transparency offered by space systems, the innovators must, at all possible times, be prepared to apply what they have learned as expeditiously as possible. The side that innovates with more creativity and at the proper level of complexity will achieve marked advantages. It is to that end that this textbook—and this entire series of textbooks—aims to contribute, and it is your responsibility, dear reader, to advance your particular fields by building upon the knowledge and experience of others. The military establishment needs your help, and such contributions could not be more important for the future of the free world.

As the authors of this text ably demonstrate, however, the future is not all (or possibly not even mostly) one of conflict. Warfare happens to be the artistic medium of greatest concern to me, but the same technologies that are vital to our security also provide new opportunities to advance agricultural sciences, to mitigate the effects of natural disasters and climate change, and to build a cislunar economy that promises abundant economic benefits and lays the cornerstone of humankind's expansion across the solar system. In other words, like radios, rockets, satellites, and cell phones, the technologies described in this series are often dual-use, and when the time is appropriate, they must be used appropriately. Just as our forebearers have often wished to beat their swords into plowshares, it is my sincere hope that our children will turn their hyperspectral cameras away from the enemy and use the very same reconnaissance drones to determine the most efficient placement of synthetic fertilizers. The future is always scary, but as I write this, the Artemis I launch is pending, and there is good reason to hope for a future built more on cooperation than on conflict. Good luck out there!

Jerry Drew
September 3, 2022

[1] The White House, *Interim National Security Strategic Guidance* (Washington, DC: 2021), 6.

[2] B.H. Liddell Hart, foreword to *Panzer Leader*, by Heinz Guderian (New York: Da Capo, 2002), 15.

PREFACE - PURVIEW OF DREAMERS (NICHOLS)

PREFACE – ***PURVIEW OF DREAMERS***

SPACE SYSTEMS: EMERGING TECHNOLOGIES AND OPERATIONS is our seventh textbook in a series covering the world of UASs / CUAS/ UUVs. Other textbooks in our series are ***Drone Delivery of CBNRECy – DEW Weapons: Emerging Threats of Mini-Weapons of Mass Destruction and Disruption (WMDD); 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 six titles have received considerable global recognition in the field. (Nichols & Carter, 2022) (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 seventh title takes on a new purview of **Space**. Let's think of space as divided into four regions. Planets, solar systems, and the great dark void fall into the purview of astronomers and astrophysics. The earth, from a measurement standpoint, is the baseline of space. It is the purview of geographers, engineers, scientists, politicians, and romantics. Flying high above the earth are Satellites. Their purview is governed by military and commercial organizations. The lowest altitude at which air resistance is low enough to permit a single complete, unpowered orbit is approximately 80 miles (125 km) above the earth's surface. Normal LEO satellite launches range between 99 miles (160 km) to 155 miles (250 km). Satellites in higher orbits experience less drag and can remain in space longer in service. Geosynchronous orbit is around 22,000 miles (35,000 km). However, orbits can be even higher. The Russians claim they placed a radio astronomy satellite in a long elliptical orbit that carries it nearly as far as the moon. (Hardwick, 2022) UASs (Drones) have a maximum altitude of about 33,000 ft (10 km) because rotating rotors become physically limiting. (Nichols R. , et al., 2019) Recreational drones fly at or below 400 ft in controlled airspace (Class B, C, D, E) and are permitted with prior authorization by using a LAANC or DroneZone. Recreational drones are permitted to fly at or below 400 ft in Class G (uncontrolled) airspace. (FAA, 2022) ***However, between 400 ft and 33,000 ft is in the purview of DREAMERS.***

In the DREAMERS region, space has its most interesting technological emergence. We see emerging technologies and operations that may have profound effects on humanity. This is the mission our book addresses. We look at the Dreamer region from three perspectives: a military view where intelligence, jamming, spoofing, advanced materials, and hypersonics are in play. An exploration of the challenges in the Dreamer region follows. These include space-based platform vulnerabilities, trash, disaster recovery management, AI, manufacturing, and extended reality. Lastly, we dramatically shift to the humanitarian use of space technologies. This includes precision agriculture wildlife tracking, fire risk zone identification, and improving the global food supply and cattle management.

State-of-the-Art research by a team of fifteen SMEs is incorporated into our book. We trust you will enjoy reading it as much as we have in its writing. There is hope for the future.

Randall K Nichols
Professor of Practice
Director, GC Aerospace Cyber Operations
UAS / UUV Series Managing Editor / Co-Author
Kansas State University Aerospace & Technologies Campus
Professor Emeritus – Cybersecurity, Utica College

Bibliography

Barrie, D. (2021, July 1). *irans-drone-fleet.* Retrieved from 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/

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

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

FAA. (2022, June 22). *Recreational Flyers & Modeler Community-Based Organizations -14 CFR Part 107.* Retrieved from FAA.gov: www.faa.gov

Facon, I. (2016, May). *A-Perspective-on-Russia-Proliferated-Drones.* Retrieved from http://drones.cnas.org/: http://drones.cnas.org/wp-content/uploads/2016/05/A-Perspective-on-Russia-Proliferated-Drones.pdf

Hardwick, C. S. (2022, June 22). *How high are satellites?* . Retrieved from Quora.com: www.quora.com

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, & Carter, H. J. (2022). *Drone Delivery of CBNRECy – DEW Weapons: Emerging Threats of Mini-Weapons of Mass Destruction and Disruption (WMDD).* Manhattan, KS: New Prairie Press #46.

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 #21.

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, #38.

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#: https://en.wikipedia.org/wiki/Emerging_technologies#:~:text=Emerging%20technologies%20are%20technologies%20whose,background%20of%20nonexistence%20or%20obscurity.

[1] NPP metrics as of 09/06/2022: 43,242 downloads (with additional files) for commercial, military, educational, government, NGOs, Libraries, and small business organizations, 1,540 institutions, 164 countries, 11,852 metadata pages, 9,560 abstract views, 47 social media, 31,541 usage, and 363 referrers! Our books are averaging ~1,000 + downloads /month. These figures do not include Amazon sales, Kindle, or tablet versions.

ACKNOWLEDGEMENTS

ACKNOWLEDGEMENTS

Books such as this are the products of contributions by many people, not just the authors' musings. **SPACE SYSTEMS: EMERGING TECHNOLOGIES AND OPERATIONS** (Nichols & Carter, 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: Dr. Richard Linton, KSU current President; Dr. Richard Myers, retired 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 KSUAT; 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. Carolyn S. Jackson and Dr. Emily Finch at New Prairie Press and Pressbooks, Joel Anderson, KSU OVPR and Research Director.

We had some wonderful outside SMEs to bounce ideas off and get our heads straight. They include Dr. Donald Rebovich, Professor Emeritus, and SME in Fraud and Identity Theft, 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 current Wildcat author; and Dr. Dan J. Ryan, experienced SME / lawyer in intelligence, cryptography, and global defenses.

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 my KSU Wildcat team produced between 2018-2022. *DRONE DELIVERY OF CBNRECy – DEW WEAPONS, Emerging Threats of Mini-Weapons of Mass Destruction and Disruption (WMDD*); (Nichols & Sincavage, DRONE DELIVERY OF CBNRECy – DEW WEAPONS, Emerging Threats of Mini-Weapons of Mass Destruction and Disruption (WMDD), 2022) *Disruptive Technologies with Applications in Airline, Marine, and Defense Industries;* (Nichols & Sincavage, Disruptive Technologies with Applications in Airline, Marine, and Defense Industries, 2021)*; Unmanned Vehicle Systems & Operations on Air, Sea & Land;* (Nichols & Ryan, 2020) *Counter Unmanned Aircraft Systems Technologies & Operations* (Nichols & Mumm, 2020)*; Unmanned Aircraft Systems in the Cyber Domain, 2nd Edition* (Nichols & Mumm, Unmanned Aircraft Systems in the Cyber Domain, 2nd Edition., 2019)*; and Unmanned Aircraft Systems (UAS) in the Cyber Domain* (Nichols R. &., 2018).

Next comes our expanded Wildcat writing team: Dr. Suzanne E. 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 M. 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; Robert McCreight, a specialist in US Army Special Operations and National Security Expert in Defense programs associated with nuclear and biological defense matters; William Slofer, Dragon and SME in radar and Hypersonic technologies; Dr. Michael Pritchard, Dean and creator of the new Space Technologies Masters programs., Dr. Haley Larson, KSU expert in agriculture and cattle feeding, Dr. Siny Joseph KSU-AT Professor of economics and material science; and Dr. Michael Oetken our expert in virtual reality, extended reality, and robotics. We were fortunate to have Dr.

Sincavage and Professor Carter build our cover art. Many others have helped our team write this important book. We appreciate all of their contributions.

The Wildcat team especially thanks to Dr. Carolyn S. Jackson and Dr. Emily Finch, Scholarly Communication Librarians, for their expert guidance on the New Prairie Press and Pressbooks publishing journey.

We are Honored to have engaged LTC Jerry Drew, U.S. ARMY CGSC to write our Foreword. LTC Drew has the experience to understand our priorities and hope for the future. LTC Drew is an organizational planner for Space & Missile Defense Command, Space Command, and Space Force with eleven years as a space operations officer assigned in multiple mission areas

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 training resources to protect the United States from terrorism.

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

Professor of Practice

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, & Carter, H. J. (2022). *SPACE SYSTEMS: EMERGING TECHNOLOGIES AND OPERATIONS.* Manhattan, KS: New Prairie Press #TBA.

Nichols, R. &. (2018). *Unmanned Aircraft Systems (UAS) in the Cyber Domain.* Manhattan, KS: New Prairie Press #21.

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

Nichols, R. K., & Mumm, H. C. (2020). *Counter*

Unmanned Aircraft Systems Technologies & Operations. Manhattan, KS: www.newprairiepress.org/ebooks/31.

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

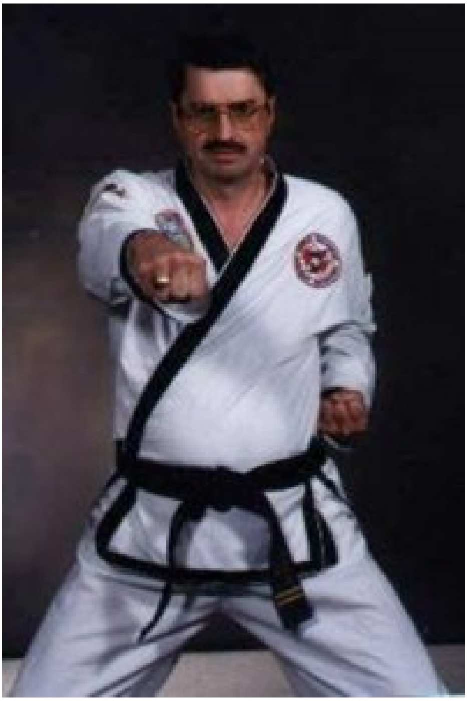
Nichols, R. K., & Sincavage, S. M. (2022). *DRONE DELIVERY OF CBNRECy – DEW WEAPONS, Emerging Threats of Mini-Weapons of Mass Destruction and Disruption (WMDD).* Manhattan, KS: New Prairie Press #46.

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

SERIES CONTRIBUTORS

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, GC Aerospace Cyber Operations program. Nichols is internationally respected, with 52 years of experience in leadership roles in cryptography, counterintelligence, counterterrorism, INFOSEC, UAS/ CUAS/UUV and sensitive computer applications. Throughout his career, Nichols has published *fourteen* 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 UAS/CUAS/UUVS Series:

Space Systems: Emerging Technologies and Operations. (SS:ET&O) (2022) Manhattan, KS: New Prairie Press #47. Available in October 2022 as a free book at: *http://newprairiepress.org/ebooks/47/* The Pressbooks edition is live and available at **https://kstatelibraries.pressbooks.pub/spacesystems/**

DRONE DELIVERY OF CBNRECy – DEW WEAPONS, Emerging Threats of Mini-Weapons of

Mass Destruction and Disruption (WMDD). **(2022)** Manhattan, KS: New Prairie Press #46. Available as a free eBook at: **https://newprairiepress.org/ebooks/46/**

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**

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
- CUAS – Designing advanced counter UAS systems with Stealth
- UUVs – Tracking Unmanned Underwater ISR Vehicles of hostile actors
- Designing Acoustic Countermeasures against hostile-actor UAS SWARMS & developing dual-purpose IFF sound libraries.

Contact Prof. Randall K Nichols at profrknichols@ksu.edu.

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

Dr. Hans C. Mumm (Co-Author)

Dr. Mumm has spent a combined twenty-eight years in government and contractor service building teams to address hard problems in the areas of national security, homeland security, and advanced technologies. He was the Division Chief for Cyber Security at the Office of The Director of National Intelligence (ODNI) programming and executing a budget of over $140M. Subsequently, he accepted a Branch Chief position with the CIA and built a unique set of continuous monitoring capabilities in support of the ICD503 Risk Management Framework. His achievements include establishing a rogue wireless framework, as well as the funding, technology, and teams to support the ICD 503 initiatives. His programmatic responsibilities included the auditable financial statements of assigned programs, the long-range planning for next-generation systems included tracking working capital funds through the CBJB and POM submissions.

He gained notoriety during Operation Iraqi Freedom as the officer in charge of the "Iraqi Regime Playing Cards; CENTCOM'S Top 55 Most Wanted List," which was touted by the Defense Intelligence Agency (DIA) as one the most successful Information Operations (IO) in the history of DIA. Due to combat injuries, he was medically retired through the Wounded Warrior Transition Program and was a direct hire to the ODNI. The successes of his teams live in history books, technology journals, and military museums.

Dr. Mumm is a proven leader in a diverse set of fields, including autonomous systems, AI/machine learning, energy research, advanced fuel systems, nuclear energy use and technologies, cognitive scientific research, and all aspects of the military intelligence communities. He is a published researcher in both the scientific and social science arenas and has won grants and contracts to further test and evaluate his original research. He has notable experience in research and systems engineering, which includes winning awards and contracts for UAV research and the creation of an advanced multiple fuel system (AI-based) where he operated the world's first and only helicopter that flies on five separate fuels without engine modifications. His research extends into emerging and disruptive technology for offensive and defensive missions supporting US and coalition operations. His UAV and robotics expertise has focused on determining the specific uses, exceptions, and allowances for robotics operations, including studying the unintended consequences, future use, and misuse of such technologies.

Dr. Mumm holds a Doctorate of Management with a concentration in Homeland Security from Colorado Technical University (CTU), an MS in Strategic Intelligence from American Military University (AMU), and a BS in Management from Chadwick University. His military education includes dozens of in-residence strategic and tactical courses, as well as specialized intelligence disciplines, leadership, and management courses.

Dr. Mumm was entered into US Congressional Record (E1201-E1202 Sept 5, 2018) for his decades of dedication and service to the United States of America. He has earned twenty-three personal military ribbons/medals, including six military unit medals/citations, and two Directors Awards, from the Defense Intelligence Agency. In 2016 he was awarded the People of Distinction Humanitarian Award as well as being granted a US Patent and Trademark for How to Harmonize the Speed of Innovation and Change with the Human Spirit's Need for Leadership. In 2005, Dr. Mumm was recognized as one of the "Ten Outstanding Young Americans," and in 2003, he was awarded the National Defense PAC "American Patriot Ingenuity Award" for his service during "Operation Iraqi Freedom."

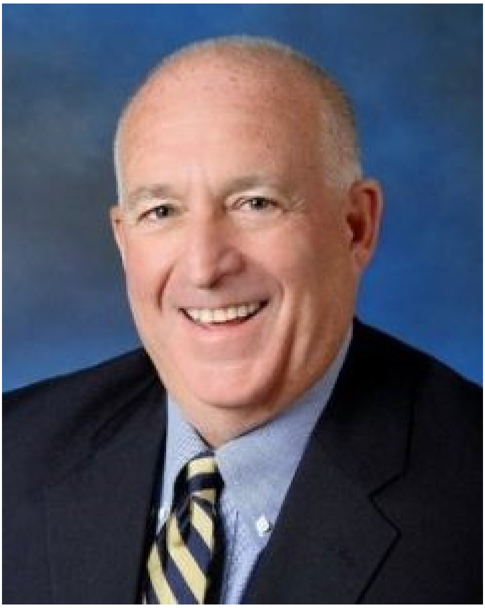
Dr. Mumm is an adjunct professor at the California

University of Pennsylvania (CALU), instructing Homeland Security courses in the Criminal Justice Department.

He recently co-authored "Drone Delivery of CBNRECy – DEW WEAPONS -Emerging Threats of Mini-Weapons of Mass Destruction and Disruption (WMDD) the sixth in a series of textbooks, which includes two editions titled "Unmanned Aircraft in the Cyber Domain; Protecting USA's Advanced Air Assets", "Unmanned Vehicle Systems & Operations on Air, Sea, Land," and an early 2020 book titled "Counter Unmanned Aircraft Systems Technologies and Operation." These textbooks are a follow-up to his international best-selling book in 2017 titled "Lightning Growth" and his best-selling book in 2015 titled "Applying Complexity Leadership Theory to Drone Airspace Integration."

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

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



Wayne Lonstein holds a Bachelor of Arts Degree in Political Science from Wilkes University, a Bachelor of Science Degree in Cyber Forensics, and Information Security from Syracuse University – Utica College, A Master of Science Degree in Homeland Security with a concentration in Information Security from The Pennsylvania State University and a Juris Doctor Degree from Pace University School of Law. Additionally, he holds a CISSP Certification from The Pennsylvania State University. He is a member of the state bars of New York, New Jersey, Massachusetts, 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)

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)

Prof. 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.

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 Aerospace and Technologies Campus; 2nd Ed. Foreword)

Dr. Starkey is a Professor and currently serves as the CEO and Dean of the Kansas State University Aerospace and

Technology 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 University Aerospace and Technology Campus 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 (FIIU), 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).

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.

Dr. Suzanne E. 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 intelligence 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, WMDD)

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.

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

Professor Michael L. Oetken (Co-author)

Michael L. Oetken is an Assistant Professor and Program Coordinator for Digital Media and Computer Systems Technology in the Department of Integrated Studies at Kansas State University Salina Aerospace and Technology Campus. Professor Oetken teaches courses in the areas of immersive media technology, user experience (UX) design, web development, web design, digital media design and graphic design. Professor Oetken's areas of expertise are augmented (AR), virtual (VR), and extended (XR) reality media technology, strategic media communications, web development, graphic design, motion graphics, 3D modeling, and video production. Professor Oetken holds a B.A. in Graphic Design from Fort Hays State University, an M.S. in Web Development from Fort Hays State University and is currently a Ph.D. candidate in the strategic media program at Liberty University. Oetken has over 20 years of industry experience in the areas of strategic communication, graphic design, marketing, and digital media technologies. Previous professional titles include graphic designer, webmaster, art director, assistant marketing director, and creative director. As senior creative director for Kansas State University, Oetken provided leadership, oversight, coordination, and creative direction for communications and marketing entities throughout the entire university system — including all major web, video, social media, and print projects. During Mr. Oetken's 20-plus years as an industry professional, he has been recognized for excellence in communication, marketing, and design with numerous Council for Advancement and Support of Education (CASE) and University & College Designers Association (UCDA) awards—including the 2013 and 2017 CASE International Circle of Excellence awards, which acknowledge superior accomplishments that have lasting impact, demonstrate the highest level of professionalism, and deliver exceptional results in regard to higher education communications and marketing.

Dr. Siny Joseph (Co-author)

Dr. Siny Joseph is a Professor of Economics and Graduate faculty member at Kansas State University's Aerospace and Technology Campus. She has an experience of 10 years of teaching graduate and introductory undergraduate economics courses at K-State. She has won awards for teaching excellence based on innovations in teaching pedagogy and developing open textbook materials. Dr. Joseph has a multidisciplinary background with a bachelor's degree in electrical engineering, a Master of Business Administration degree specializing in marketing and operations research, and a master's and PhD degree in resource economics from University of Massachusetts Amherst. Her research areas embody her multidisciplinary background with interests in the areas of agricultural trade, food policy, organic dairy and feed grain markets, mobile computing, accessible and assistive technologies, circular economy applications in space materials and integrated livestock-crop production. Dr. Joseph is active in securing grant funding both at the federal level and within K-State with proposals funded for a total of approximately $2 Million. She has been continually disseminating teaching scholarship, disciplinary and inter-disciplinary research findings through peer-reviewed academic journal articles, conference proceedings, and national/international conference presentations/posters. She plays an active role as a moderator/facilitator/panelist in academic conferences and workshops, reviewer for professional academic organizations, academic journals, and federal funding agencies such as NSF and USDA. Dr. Joseph serves as a consultant for various federal agencies funded projects. In addition, she has appeared in radio and television shows discussing various economics related topics.

Dr. Michael J. Pritchard (Co-author)

Dr. Michael J. Pritchard received a bachelor's degree in Anthropology from the University of Kansas, a Master of Science in Information Systems from Northwestern University, and a Doctor of Philosophy in Information Systems from Dakota State University in 2019. He is currently the Associate Dean for Research & Graduate Studies as well as the Assistant Professor for Machine Learning and Autonomous Systems at Kansas State University and a former graduate lecturer of Data Science at UC Berkeley. His research is published in Information Systems, IEEE Transactions on Professional Communication, International Journal of Transport and Vehicle Engineering, and Hawaii International Conference on System Sciences. His areas of research include integrated machine learning, autonomous systems, cybernetic systems, and information theory.

Dr. Haley Larson (Co-author)

Haley Larson, Ph.D., is a teaching assistant professor of animal health at Kansas State University's Olathe campus. Dr. Larson earned her B.S. in Animal Science and Ph.D. in ruminant nutrition from the University of Minnesota. Her graduate studies focused on understanding how manipulation of growth and fermentation patterns in feedlot cattle effects animal performance. While completing her degree, Larson began working as a senior scientist for Cargill Animal Nutrition and Health. In that role, she designed and developed the company's dual-flow continuous culture system – the first fully automated dual-flow system for cattle rumen simulation. This system, and the data she generated, is still being used for new product development and fermentation modeling within the company today. During her time with Cargill, Larson was also presented with many opportunities to develop and deploy on farm technologies for dairy, beef, swine, poultry, and aquaculture.

At Kansas State, Dr. Larson teaches several animal health graduate-level courses within the department of applied and interdisciplinary studies as well as the College of Veterinary Medicine's diagnostic medicine and pathobiology department. She leads regulatory affairs courses on preclinical and clinical research strategies, post-approval product stewardship, as well as EPA and FDA regulations for new animal health products. Her passion for educating the industry's next generation of agricultural professionals shines through in her courses, particularly those focused on the interconnections between the food and animal health industries.

In her role at K-State, Dr. Larson also designs academic courses and professional development programming tailored to Greater Kansas City's growing animal health industry. Most recently, she has been working to incorporate new opportunities for animal health students to understand the application of technology and data analytics to the industry.

Jerry V. Drew II, Space operations expert, author, and theorist. Foreword (SS:ET&O)

Jerry Drew is a space operations expert, author, and theorist. He holds a Bachelor of Science in art, philosophy, and literature from the U.S. Military Academy and a Master of Science in astronautical engineering from the Naval Postgraduate School where his work focused on applied robotic manipulation using small spacecraft. He is a 2017 Art of War Scholar and a 2018 graduate of the School of Advanced

Military Studies. Mr. Drew is currently enrolled as a PhD student in the Colorado School of Mines' Space Resource program.

Mr. Drew has served in numerous positions within the National Security Space community, including as a member of the planning teams that established U.S. Space Command and the U.S. Space Force. In addition to one science fiction novel and one poem, he has published a dozen articles and conference papers on tactics, military history, robotics, and operational art. His co-authored book, *The Battle Beyond: How to Fight and Win the Coming War in Space*, is due for publication later this year. He lives in Kansas with his wife and four children.

The Wildcat team is Honored to have Jerry Drew as our Foreword writer for *Space Systems: Emerging Technologies and Operations* **(SS:ET&O**).

ABBREVIATIONS AND ACRONYMS

ABBREVIATIONS, ACRONYMS AND DEFINITIONS [1] [2]

The following terms are common to the UAS / CUAS /UUV /SPACE industries, general literature, or conferences on UAS/UAV/Drone/UUV/ SPACE systems. A majority of the technical abbreviations come from DRONE DELIVERY OF CBNRECy – DEW WEAPONS Emerging Threats of Mini-Weapons of Mass Destruction and Disruption (WMDD); (Nichols & Sincavage, 2022) (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) (Adamy D. L., Space Electronic Warfare, 2021) (Nichols & Sincavage, 2022)

ABM Anti-ballistic missile

A/C Aircraft (Piloted or unmanned) also A/C

ACAS Airborne Collision Avoidance System

A/CFD Aircraft Flood Denial jamming

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

AMAZE EU’s Additive Manufacturing Aiming

Towards Zero Waste and Efficient Production of High-Tech Metal Products project

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
AOCS	Cooperative Attitude and Orbit Control System takeover
APC	Armored personnel carrier
APDS	Armor-piercing discarding sabot projectile
APFSDS	Armor-piercing fin-stabilized discarding sabot projectile
APHIS	Animal and Plant Health Inspection Service
AR	Augmented reality
ARW	Anti-radiation weapons
ASAT	Anti-satellite weapons / Anti-satellite missile system
ASREN	Association of Geospatial Industries, the Arab States Research and Education Network
ASW	Anti-Satellite Weapons
ATC	Air Traffic Control / Air traffic Control Signals
ATCC	Air Traffic Control Center
ATM	Air Traffic Management
ATS	Air Traffic Services

ATSAW Air Traffic Situational Awareness

AUV Autonomous underwater vehicle

Azimuth The angle between true North and the treat location, in a plane at the satellite perpendicular to the vector from the SVP [Sub-vehicle Point]

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.

B&B Branch & bound

B.C. Before Christ

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

BrO bromine oxide

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/No	Carrier to Noise ratio
c	Speed of light ~ (3 x 108 m/s) [186,000 miles per sec] in vacuum named after *Celeritas,* the Latin word for speed or velocity.
C	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 GPS Satellite Course Acquisition unique code

CAA Control Acquisition cyber attack

CAMS Copernicus Atmosphere Monitoring Service

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

CCC Circular Cross-Correlation in classical GPS receivers

CC&D Camouflage, Concealment, and Deception

CCTV Closed Circuit Television

CD Collective detection maximum likelihood localization approach (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019)

CD Charge diameters

Cd Drag coefficient

CDC	Center for Disease Control
CDMA	Code division multiple access protocol
CD	***Collective detection maximum likelihood localization approach*** (Eichelberger, 2019)
CE	Circular economy
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
CFSPH	Center for Food Security and Public Health (CFSPH)
CHAMP	Counter-Electronics High Power Microwave Advanced Missile Project
CHS	Cyber-Human Systems
CIA	Confidentiality, Integrity & Availability (standard INFOSEC paradigm)
CI / CyI	Critical Infrastructure / Cyber Infiltration
CIA	Confidentiality, Integrity, Availability / Central Intelligence Agency
CIRCIA	Cyber Incident Reporting for Critical Infrastructure Act
CIS	Critical Infrastructure Sector
CISA	Critical Infrastructure Security Agency
CJNG	Cártel de Jalisco Nueva Generación

CM / CyM	*Countermeasure* / 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
CO-ASAT	*Co-orbital (Co-ASAT)* missile system
COMINT	Communications intelligence
COMJAM	Communications Jamming
COMINT	Communications Intelligence
COMSEC	Communications Security
CONOP(S)	Concepts of Operations
CONUS	Continental United States
CONV	Convergent Technology Dynamics
CONV-CBRN	Convergent Technology Dynamics – Chemical, Biological, Radiation & Nuclear
COP	Common operating picture
COTS	Commercial off-the-shelf
CM	Apollo Command Modules
CNPC	Control and non-payload links
CPB	Charged particle beam
CPS	Cyber-physical systems
CR	Conflict Resolution / Close range / Cyber Raid (aka CyR)
CSI	Crime scene investigation

CSIS Center for strategic and International Studies

CT Counter-Terrorism / Counter-Terrorism Mission

CTN Course -Time Navigation , A-GPS technique which drops the requirement to decode the HOW timestamps from the GPS signals. CTN also refers to a snapshot receiver localization technique measuring sub-millisecond satellite ranges from correlation peaks, like classical GPS receivers.

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.

DA-ASAT *Direct Accent* or Hit-to-Kill (DA-ASAT) missile system

Danger Close

Definition www.benning.army.mil/infantry/magazine/issues/2013/May-June/Myer.html Nov 14, 2013 – 1) danger close is included in the "method-of-engagement" line of a call-for-fire request to indicate that friendly forces are close to the target. ... Danger close is a term that is exclusive from risk estimate distance (RED) although the RED for 0.1 percent PI is used to define danger close for aircraft delivery. Pi = Probability of incapacitation. 2) Definition of "danger close" (US DoD) In close air support, artillery, mortar, and naval gunfire support *fires*, it is the term included in the method of engagement segment of a call for *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) (Nichols & Sincavage, 2022)
DF	Direction-finding
DHS	Department of Homeland Security
DOF	Degrees of Freedom
DOS	Denial of Service attack
DPRK	Democratic People's Republic of Korea
DTRA	Defense Threat Reduction Agency
DUST	Dual-use Science & Technology threat
1090ES –	1090 Extended Squitter Data Link
EA	Electronic Attack
Earth Trace	The Earth Trace is the locus of latitude and longitude of the SVP as the satellite moves through its orbit
EARSC	European Association of Remote Sensing Companies
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)

ECCO	Estimating the Circulation and Climate of the Ocean
ECM	Electronic countermeasures
ECMWF	European Centre for Medium-Range Weather Forecasts
EHC	Extra high voltage
ELINT	Electronic Intelligence
ELSA-D	Twin small satellite launched in 2020 for End-of-Life-Servicing & Long-Term orbital sustainability
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
EOS	Earth Observation Satellites
ESA	European Space Agency
ESOC	European Space Operations Center located in Darmstadt, Germany
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 measures – (old ECCM) (Adamy D., EW 101 A First Course in Electronic Warfare, 2001) to guard friendly systems from hostile attacks.[2]

EW **Electronic Warfare (EW)** is the art and science of denying an enemy the benefits of the electromagnetic spectrum **(EMS)** while preserving them for friendly forces.

(Wolff, 2022)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)

EUMETSAT	European Organization for the Exploitation of Meteorological Satellites
ESA	European Space Energy
FAA	Federal Aviation Agency
FDM	Fused Deposition Modeling technique
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
FY-4	China (FY-4) Lightning Mapping Imager
GAO	Government Accountability Office
GCS	Ground control station
GEE	Google Earth Engine
GEO	Group on Earth Observations
GIS	Geographical information system
GLM	Geostationary Lightning Mappers
GNSS	Global Navigation Satellite System (GPS, GLONASS, Galileo, Beidou & other regional systems)
GNU	GNU / Linux Operating system

GOES R-series Geostationary Operational Environmental Satellites (GOES-16 and 17)

GPM Global precipitation measurement

GPS Global Positioning System (US) [3] (USGPO, 2021)

GPS Global Positioning System / Geo-Fencing

GPS/INS uses GPS satellite signals to correct or calibrate a solution from an inertial navigation system (INS). The method applies to any GNSS/INS system

GRU Russian military intelligence branch

GS Ground Station

gSSURGO Gridded Soil Survey Geographic Database

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)

HAPS UAVs UAVs dedicated to HAPS service (example to communicate via CNPC links)

HCM Hypersonic cruise missile

HGV Hypersonic glide vehicle

HEAT High-explosive anti-tank warhead

HEL High energy Laser

HPM High powered microwave

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
ICAO	International Civil Aviation Organization
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
INSA	Intelligence and National Security Alliance
INFOSEC	*Information Security*

IO /I.O.	Information Operations
IoT	Internet of things
IIoT	Industrial Internet of things
IP	Internet protocol
IR	Infrared
IS	Information security / Islamic State
ISO	International Organization Standardization
ISM	In-space manufacturing
ISS	International Space Station
ISIS	*Islamic State of Iraq and al-Sham (ISIS)*
ISR	Intelligence, Reconnaissance and Surveillance UAS Platform
ISTAR	Intelligence, surveillance, target acquisition, and reconnaissance
IT	Information Technology
IT/OT	Information Technology/ Operational Technology
ITE	Installation, Training, Expense
ITP	In trail procedure
IW	Information Warfare
JIM	Joint Investigative Mechanism
JPL	NASA Jet Propulsion Laboratory
JSR	Jamming-to-signal ratio
KE	Kinetic energy
KEW	Kinetic energy weapon
K'IHAP	Short Shout in Tae Kwon Do
KKW	Kinetic Kill Weapon/Warhead

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

LED- Light emitting diodes

LENS Laser-engineered net shaping

LDEF Long Duration Exposure Facility

LGF Low Gradient Furnace

LiDAR Light Detection and Ranging – a RS method using light in the form of a pulsed laser to measure ranges

LOS Line-of-sight / Loss of Signal / Loss of Separation

LLTR Low-level transit route

LM or L.M.	Loitering munitions
LMM	Lightweight Multi-role Missiles
LPI	Low Probability of Intercept
LRAD	Long Range Acoustic Device / Long-Range *Area* Denial [4]
LWSI	Livestock weather safety index
M&S	Modeling and simulation technologies
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
MMEVR	Multi-Mission Extra Vehicular Robot
MMOD	Micrometeoroids and orbital debris
MND	Ministry of National Defense
MOA	Minute of angle in degrees
MOPP	Mission Oriented Protective Posture (MOPP) Gear

MoU	Memorandum of Understanding
MRVs	Multiple Re-entry Vehicles
mTBI	mild Traumatic Brain Injury
MRG	Europe – Meteosat Third Generation Lightning Imager
MSFC	NASA Marshall Space Flight Center
MTI	Moving target indicator
MUM-T	Manned-unmanned teaming (MUM-T)
NAS	National Academy Of Sciences
NATO	North Atlantic Treaty Organization
NASA	National Aeronautical and Space Administration
NCSS	National Cooperative Soil Survey
NDM	Navigation data modification spoofing attack
NDVI	Normalized Difference Vegetation Index
NEB	New Economic Block soldier
NERC	North American Electric Reliability Corporation
NGB	National Guard Board
NGO	Nongovernmental organization
NHTSA	National Highway Traffic Safety Administration
NIEHS	National Institute of Environmental Health Sciences
NIR	Near Infrared
NKW	non-kinetic warfare
NMA	Navigation Message Authentication

NO2	Nitrogen dioxide
NOAA	National Oceanic & Atmospheric Agency
NV	Neurological vulnerability
OCONUS	Outside Continental United States
OLI	Operational Land Imager
OMAR	On-Orbit Manufacture, Assembly and Recycling
OMI	Ozone Monitoring Instrument
OODA	Observe, Orient, Decide, and Act decision loops
OPCW	Organization for the Prohibition of Chemical Weapons
OPSEC	Operational Security
OSINT	Open-source intelligence (also OSI)
OTH	Over-the-horizon
PFMI	Pore formation and mobility investigation furnace
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)
PMU	Phasor Measurement Unit
PNT	Positioning, navigation, and timing systems
POV	Point of view

PRAM	Photovoltaic Radio-frequency Antenna Module technology
PRN	Pseudo-Random Noise
PSA	Protective security advisors
PSR	Primary Surveillance Radar
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
RKA	Chinese Relativistic Klystron Amplifier
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
RPO	Rendezvous and proximity operations
RPV	Remotely piloted vehicle
RS	Remote sensing

RSS	Received signal strength / Remote Sensing & Surveillance
RTU	Remote terminal units
RV	Re-entry vehicle
SA	Situational Awareness
SAA	Sense and Avoid
SAM	Surface to Air missile
SAR	Synthetic aperture radar
SATINT	Satellite intelligence
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
SDA	Space Domain Awareness
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
SML	Space mobility and logistics area support
S/N	S / N = is one pulse received signal to noise ratio, dB: Signal to Noise ratio at HAPS receiver (also, SNR)

SO2 Sulfur dioxide

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]

SQF Solidification Quench Furnace

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) (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019) (Nichols & Sincavage, 2022)

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

SSN Space Surveillance Network

SSR Secondary Surveillance Radar

STEALTH to resist detection

STM Space traffic management

sUAS	Small Unmanned Aircraft System
SUBSA	Solidification using a Baffle in Sealed Ampoules
SVP	Sub-vehicle point – Point on earth's surface right below the Satellite
SWARM	High level, a dangerous collaboration of UAS, UUV, or unmanned boats
T2AR	T2 Augmented Reality project
Taiwan ROC	Taiwan is officially the Republic of China
TCAS	Traffic collision avoidance system
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.
TIROS	Television InfraRed Observational Satellite
TNT	Trinitrotoluene
TO	Theater of Operations
TOA	Time of arrival
ToF	Time of flight
TRANSEC	Transmission security
TTFF	Time to first fix (latency)
TTPs	Tactic, Technique, and Procedures
Tx	Transmit signal
UA	Unmanned Aircraft (non-cooperative and potential intruder)

UAM	Urban Air Mobile (vehicle)
UAS-p	UAS pilot
UAS	Unmanned aircraft system (popularly but incorrectly referred to as drones)
UAT	Universal access transceiver
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
UNOOSA	The United Nations Office for Outer Space Affairs
USDA	US Department of Agriculture
USV	Unmanned Surface Vessel
UUV	Unmanned underwater vehicle
UWB	Ultrawideband
VBN	Visual-based navigation
VBN LiDAR	Visual-based navigation: Light Detection and Ranging – a RS method using light in the form of a pulsed laser to measure ranges
VDL	VHF Data link

VI	Vegetation Indices
VIEW	Virtual Interface Environment Workstation
VIIRS	Visible Infrared Imaging Radiometer Suite
VIS	Visible
VPL	Visual Programming Languages
VR	Virtual reality
VRT	Variable rate technology
VLOS	visual line of sight
VTOL	Vertical take-off and landing
VX	Deadly nerve agent
WAM	Wide area multilateration
WFOV	Wide field of view
WFUL	Wake Forrest University Laboratory
WLAN	Wide Local area network
WMD	Weapons of Mass Destruction
WMDD	Mini-Weapons of Mass Destruction and Disruption
WMO	World Meteorological Organization
XR	Extended reality

Special Definitions (Nichols & Carter, 2022) (Nichols R. K., 2020)

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)

False Flag Operation – organized spreading of misinformation or disinformation.

Eichelberger Collective Detection (ECD) Definitions / Counter Spoofing Concepts

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:

N-1

Cxcorr (a, b , d) = Σ ai dot bI + d mod N Eq. 3-1

I=0

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 Ớ (N log N) time. [3](Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019)

Like classical GPS receivers, coarse-Time Navigation (CTN) is a snapshot receiver localization technique that measures sub-millisecond satellite ranges from correlation peaks. (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 combines all the available information and decides only at the end of the computation. 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.

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, ellipsoid, equator, meridian longitude, latitude, geodetic latitude, geocentric latitude, and geoid. [4]

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

Navigation Data is the data transmitted from satellites, which includes orbit parameters to determine the satellite locations, timestamps of signal transmission, atmospheric delay estimations, and status information of the satellites and GPS as a whole, such as the accuracy and validity of the data. (IS-GPS-200G, 2013) [5]

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)

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

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 (EOS) 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. LLO: low lunar orbit is approximately 100 km above the lunar surface. L1 and L2: "Lagrange points are caused by the balance between the gravitational fields of two large bodies; equilibria between two pulling forces.

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).

Agroterrorism / Bioterrorism Definitions

Agroterrorism is a subset of bioterrorism and is defined as the deliberate introduction of an animal or plant disease to generate fear, causing economic losses and/or undermining stability. (O.S. Cupp, 2004)

Bioterrorism is the threat or use of biological agents by individuals or groups motivated by political, religious, ecological, or other ideological objectives.

Earth Observation Epidemiology or **tele-epidemiology** is defined as 'using space technology with remote sensing in epidemiology. (Wiki, 2022)

MASINT – Measurement and signature intelligence (**MASINT**) is a technical branch of intelligence gathering that detect, track, identify or describe the distinctive characteristics (signatures) of fixed or dynamic target sources. This often includes radar, acoustic, nuclear, chemical, and biological intelligence. MASINT is scientific and technical intelligence derived from the analysis of data obtained from sensing instruments to identify any distinctive features associated with the source, emitter, or sender, to facilitate the latter's measurement and identification. (Wiki, 2022)

OSI, short for OPEN-SOURCE Intelligence (also known as OSINT), is defined as any intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience to address a specific intelligence requirement. (Bazzell, 2021)

Remote Sensing (RS) uses non-ground-based imaging systems to obtain information about processes and events on Earth. It is unique among the detection and diagnostic methods discussed herein in its ability to offer passive monitoring for the disease at scale rather than active sampling. (Silva & et.al, 2021)

References

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/: https://www.gps.gov/systems/gps/performance/accuracy/#problems

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

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

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

Adamy, D. L. (2004). *EW 102 ASecond Course in Electronic Warfare.* Norwood, MA: 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*.

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:

https://www.microsemi.com/document-portal/doc_download/133615-timing-sync-for-lte-tdd-lte-a-mobile-networks

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

Axelrod, P., & al, e. (2011). Collective Detection and Direct Positioning Using Multiple GNSS Satellites. *Navigation*, pp. 58(4): 305-321.

Bazzell, M. (2021). *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information, 8th edition.* Bazzell.

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). Pittsburg, PA: IPSN.

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

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 Detection. *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

FAA. (2018, April 27). *FAA Safety Management* . Retrieved from https://www.faa.gov/: https://www.faa.gov/regulations_policies/handbooks_manuals/aviation/risk_management/media/20180427_FAASRMGuidance5StepProcess_signed_508.pdf

FAA. (2019). *ATO-SMS-Manual.* Retrieved from https://www.faa.gov/: https://www.faa.gov/air_traffic/publications/media/ATO-SMS-Manual.pdf

FAA. (2021). *SRM Safety Management Quick Reference Guide.* Washington: FAA Manual Sections 3.5.4 & ff.

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 .

Fletcher, H. a. (1933). Loudness, its definition, measurement and calculation. *Journal of the Acoustical Society of America* , 5, 82-108 .

2628. Lopez-Risueno & Seco-Granados, G. (2005). Cn/sub 0/ estimation and near far mitigation for GNSS indoor receivers. *In 2005 IEEE 61st Vehiclar Technology Conf.*, V4: 2624-2628.

Global Security.Org. (2022, July 16). *Chapter 3 Intelligence, Surveillance, and Reconnaissance Planning.* Retrieved from https://www.globalsecurity.org/:

https://www.globalsecurity.org/military/library/policy/army/fm/3-21-31/c03.htm

Goward, D. (April 21, 2020). GPS circle spoofing discovered in Iran. *GPS World*.

GPSPATRON. (2022, July 9). *GNSS Interference in wildlife.* Retrieved from GPSPATRON.com: https://GPSPATRON.com/gnss-interference-from-wildlife/

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.

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

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

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/

ITU. (2019, July 19). *ARTICLE 2 – Nomenclature – Section I – Frequency and Wavelenght Bands.* Retrieved from ITU Radio Communication Edition 2008: https://web.archive.org/web/20111001005059/ http://life.itu.int/radioclub/rr/art02.htm

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.

Kahn, S. Z., & M. Mohsin, &. W. (2021, May 7). On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions. *Comp Sci*, p. 507 ff.

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

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.

MIT R&D. (2022, July 16). *ISR SYSTEMS AND TECHNOLOGY.* Retrieved from https://www.ll.mit.edu/r-d/isr-systems-and-technology: https://www.ll.mit.edu/r-d/isr-systems-and-technology

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

Nichols, & Carter, H. J. (2022). *Space Systems: Emerging Technologies and Operations.* Manhattan, KS: New Prairie Press.

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

Nichols, R. K., & Sincavage, S. M. (2022). *DRONE DELIVERY OF CBNRECy – DEW WEAPONS Emerging Threats of Mini-Weapons of Mass Destruction and Disruption (WMDD).* Manhattan, KS: New Prairie Press #46.

Nichols, R. K.-P. (2019). *Unmanned Aircraft Systems in the Cyber Domain, 2nd Edition.* Manhattan, KS : 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.

O.S. Cupp, D. W. (2004). Agroterrorism in the U.S.: key security challenge for the 21st century. *Biosecurity and Bioterrorism: Biodefense Strategy, Practice and Science 2, 97–105.*, pp. 2, 97–105. Retrieved from https://pubmed.ncbi.nlm.nih.gov/15225403/: https://pubmed.ncbi.nlm.nih.gov/15225403/

Ochin, E., & Lemieszewski, &. L. (2021). Chapter 3 Security of GNSS. In G. P. PETROPOULOS, & &. P. SRIVASTAVA, *GPS and GNSS Technology in the Geosciences* (pp. 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*, pp. 223-234.

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.

Ronfeldt, J. A. (1966). *The Advent of Netwar.* Santa Monica, CA: RAND.

Rosen, S. (2011). *Signals and Systems for Speech and Hearing (2nd ed.).* New York City: BRILL. p. 163.

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.

Silva, G., & et.al. (2021, May 20). Plant pest surveillance: from satellites to molecules. *Emerg Top Life Sci.*, pp. 5(2):275-287. doi:10.1042/ETLS20200300. PMID: 33720345; PMCID: PMC8166340.

Spilker, J. (1996). Fundamentals of Signal Tracking Theory. *Prog in Astronautics & Aeronautics*, 163:245-328.

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

Strohmeier, M. (2015). On the security of automatic dependent surveillance- broadcast protocol. *IEEE communications Surveys & Tutorials*, 17:1066-1087.

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.

Toomay, J. (1982). *RADAR for the Non – Specialist.*

London; Lifetime Learning Publications. London: Lifetime Learning Publications.

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

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/sysytems/gps

Warner, J. S., & Johnston, R. (2003). GPS Spoofing Countermeasures.*Journ of Security Administration*. Retrieved from https://www.semanticscholar.org/paper/GPS-Spoofing-Countermeasures-Warner-Johnston/36e17f723bff8d429aca4714abe54500a9edaa49

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

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

Wesson, K. (2014, May). Secure Navigation and Timing without Local Storage of Secret Keys. *PhD Thesis*.

Wiki. (2022). *Measurement_and_signature_intelligence (MASINT) definition.* Retrieved from https://en.wikipedia.org: https://en.wikipedia.org/wiki/Measurement_and_signature_intelligence

Wiki. (2022, Aug 26). *Tele-epidemiology.* Retrieved from https://en.wikipedia.org: https://en.wikipedia.org/wiki/Tele-epidemiology

Wikipedia. (2021, June 2). *Global Positioning System.* Retrieved from https://en.wikipedia.org/wiki/: https://en.wikipedia.org/wiki/Global_Positioning_System

Wolff, C. (2022). *Radar and Electronic Warfare Pocket Guide.* Munich, Germany: Rhode & Schwarz.

1026. Ng & Gao, G. (2016). Mitigating jamming & meaconing attacks using direct GPS positioning. *In Position, Location & Navigation Symposium (PLANS) IEEE/ ION*, 1021-1026.

Endnotes

[1] All Acronyms taken from (Nichols R. K., 2020) and (Nichols & Sincavage, 2022) unless otherwise noted.

[2] EM definitions from (Wolff, 2022)

[3] Ớ = Order of magnitude; dot = dot product for vectors

[4] All these systems are discussed in Chapter 2 of (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019)

[5] Each satellite has a unique 1023-bit PRN sequence, plus some current navigation data, D. Each bit is repeated 20 times for better robustness. Navigation data rate is limited to 50 bit / s. This also limits sending timestamps every 6 seconds, 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

TABLE OF CONTENTS -DETAILED

SECTION 1: C4ISR AND EMERGING SPACE TECHNOLOGIES

SECTION 2: SPACE CHALLENGES AND OPERATIONS

COPERNICUS

12. Humanitarian Use of Space Technologies to Improve Global Food Supply and Cattle Management (Larson)

TABLE OF FIGURES

TABLE OF FIGURES

SECTION 1: C4ISR AND EMERGING SPACE TECHNOLOGIES

1. Current State of Space Operations (Pritchard)

2. **Satellite Killers and Hypersonic Drones (Slofer)**

3. **Space Electronic Warfare, Jamming, Spoofing, and ECD (Nichols & Mai)**

4. **Manufacturing in Space (Jackson & Joseph)**

Materials science and manufacturing aboard the ISS

SECTION 2: SPACE CHALLENGES AND OPERATIONS

5. **Exploration of Key Infrastructure Vulnerabilities from Space-Based Platforms (McCreight)**

6. **Trash Collection and Tracking in Space (Hood & Lonstein)**

7. **Leveraging Space for Disaster Risk Reduction and Management (Carter)**

Damage Mapping After A Disaster

8. **Bio-Threats to Agriculture – Solutions from Space (Sincavage, Carter & Nichols)**

9. **Modeling, Simulations, and Extended Reality (Oetken)**

SECTION 3: HUMANITARIAN USE OF SPACE TECHNOLOGIES

10. Drones and Precision Agriculture Mapping (Mumm)

11. **Civilian use of Space for Environmental, Wildlife Tracking, and Fire Risk Zone Identification (Ryan)**

12. Humanitarian Use of Space Technologies to Improve Global Food Supply and Cattle Management (Larson)

TABLE OF TABLES

TABLE OF TABLES

SECTION 1: C4ISR AND EMERGING SPACE TECHNOLOGIES

SECTION 2: SPACE CHALLENGES AND OPERATIONS

SECTION 3: HUMANITARIAN USE OF SPACE TECHNOLOGIES

TABLE OF EQUATIONS

TABLE OF EQUATIONS

SECTION 1: C4ISR AND EMERGING SPACE TECHNOLOGIES

SECTION 2: SPACE CHALLENGES AND OPERATIONS

SECTION 3: HUMANITARIAN USE OF SPACE TECHNOLOGIES

PART I

SECTION 1: C4ISR AND EMERGING SPACE TECHNOLOGIES

1.

CURRENT STATE OF SPACE OPERATIONS (PRITCHARD)

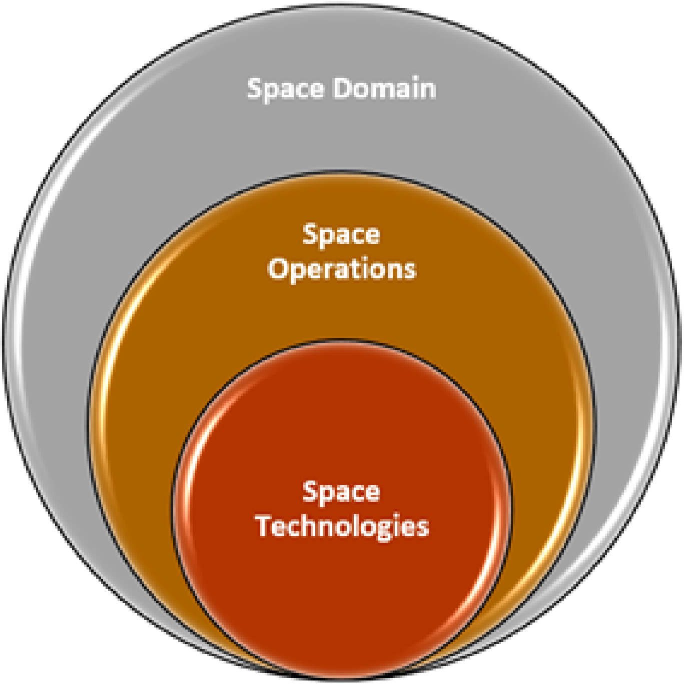
Student Objectives

- Introduce and integrate fundamental space operations terminology
- Identify the history and historical relationships of space operations
- Distinguish between space domain, space technologies, and space operations
- Understand technological development priorities

Introduction

To understand Space Operations, we first have to understand the broader concept of 'operations' as it relates to a domain and the technologies that operate within that domain. In other words, let us have a *non-space* conversation on just the following: domains, operations, and technologies. Generically speaking, what are these three concepts? And how are they interrelated? Foremost, *domains, operations*, and *technologies* are highly interconnected. Domains incorporate the objects, concepts, and rules that define a particular area of knowledge or activity. Operations are the basic actions that can be performed on those objects, concepts, and rules. Technologies are the means by which we perform those operations. (See Figure 1-1)

Figure 1-1 Domains, Operations, and Technologies



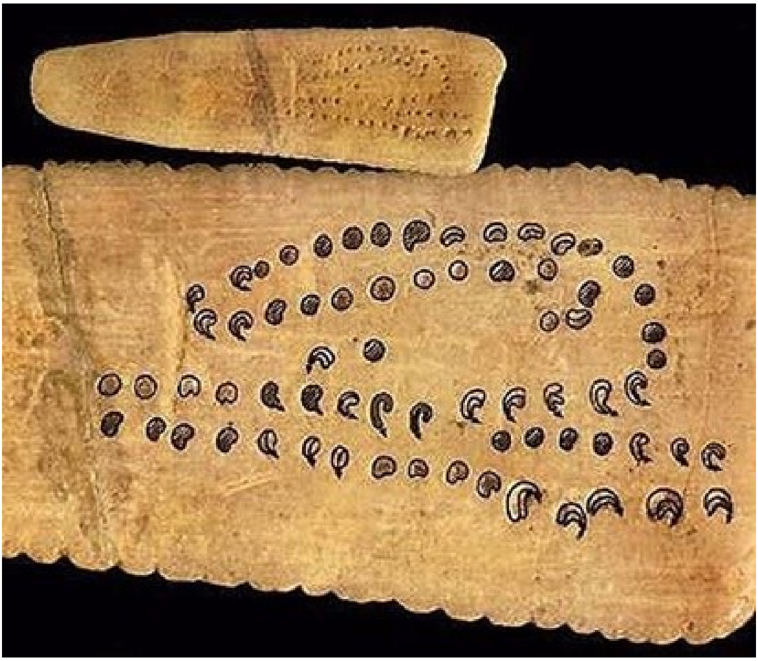
Source: (Pritchard M.) (Operations, 2022)

Now that we have our taxonomic relationships worked out, we can now overlay the concept of *Space* into this conversation. A space domain is an area of knowledge or activity that deals with objects, concepts, and space-related rules. A space operation is an action that can be performed on objects, concepts, and rules related to Space. Space technologies are the means by which we perform space operations. Okay, so maybe we need to add more definitions to this exercise. Space *technologies* allow humans to accomplish actions, which are *operations* within the environmental *domain* we call outer Space. These actions – these *space operations* – exemplify our ability to study celestial objects such as planets, pulsars, galaxies, and even black holes. They are further exemplified by our ability to traverse and explore our solar system. These specialized activities, which are classified as *space operations* within the harsh environmental *space domain*, are only possible through the design and employment of *space technologies*. So, to better understand Space Operations, let us take a historical journey through a) the Space Domain and b) Space Technologies. First up, is the Space Domain.

Space Domain

When did people first see Space as a working domain? Well, you would be surprised at how far back we can go. The evolvement of Space as a "working domain" can be categorized into a kind of product lifecycle: ideation, research, development, and operations. In total, these phases cover thousands of years. Humans have been fascinated by the waxing and waning of heavenly bodies for a long time. Many scholars believe that the development of the Aurignacian Lunar Calendar, nearly 32,000 years ago, is the earliest data point we have where there is demonstrable evidence of human celestial awareness (Peregrine, 2001) (Gheorghiu, 2013) (Soderman, 2021). Small and lightweight, these lunar calendars were simple to transport on long seasonal excursions and extended hunting expeditions (See Figure 1-2, Aurignacian Lunar Calendar). These calendars were often carved into animal bones (or stones). The largest creatures were difficult to hunt, and the codification of celestial phenomena into animal bones gave hunters the power of foresight. They used this antique space information system.[1] To predict the movement of Earth's Moon. At this point, a clearly documented *phase of ideation* occurs in human evolvement toward the space domain.

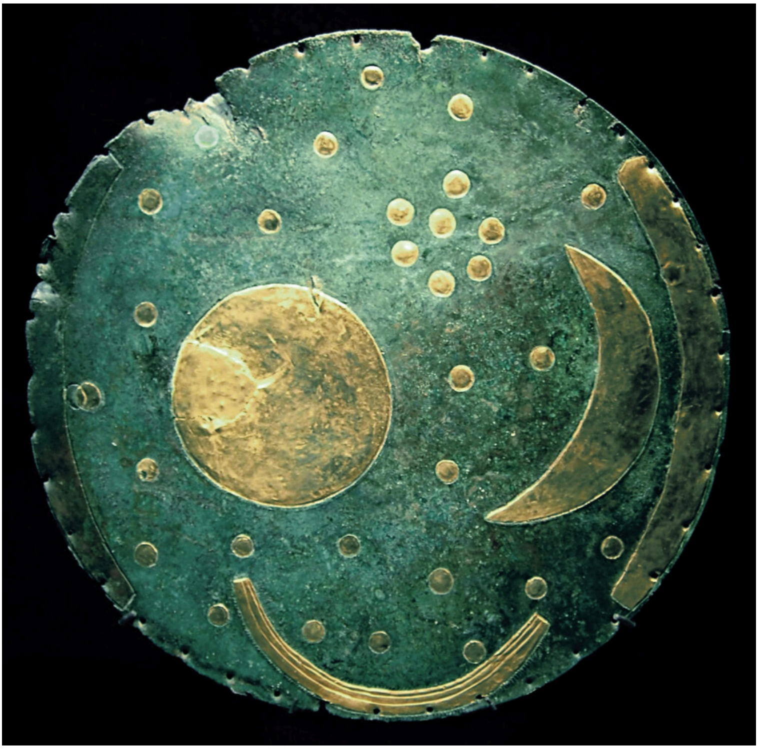
Figure 1-2 Aurignacian Lunar Calendar



Sources: (NASA, 2022) (Marchant, 2009)

These lunar calendars were not isolated to a few smart human hunters; their usage was found throughout Europe (Gaffney, 2013). Let us jump forward 30,000 years where we find the ideation phase of many cultures ends and the *research phase* begins. Roughly 3,600 years ago, humans began to develop better celestial tracking mechanisms. Humans started to create various sky mapping tools, such as the Nebra Sky Disc (See Figure 1-3, Nebra Sky Disc). This antique object, which measures around 30 centimeters, has been linked to the Unetice people who lived in a region of Europe. Reconstructed, the dots are believed to be stars, with the cluster standing in for the Pleiades. The huge circle and crescent represent the Sun and Moon.

Figure 1-3 Nebra Sky Disc



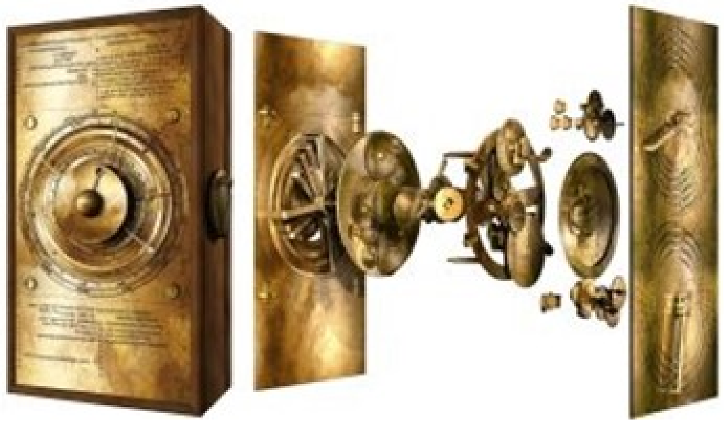
Source: (Google Images, 2018)

Figure 1-4 Recovered Antikythera Mechanism

Source: (Wikimedia, 2022)

The *research phase* of this story moves us forward a few hundred years to the creation of the Antikythera Mechanism (See Figure 1-4, Recovered Antikythera Mechanism). Created by Greek scientists roughly 2200 years ago, the device was used to forecast astronomical phenomena. It is described as the oldest example of an analog computer. A hypothetical schematic of the Antikythera Mechanism was proposed by Freeth and Jones in 2012. Using a stylized clockwork gearing structure, the mechanism showed in reverse engineering that it could forecast the elliptical trajectories of the planets and the retrograde movement of the Moon and Mars (Freeth & & Jones, 2012). The introduction of a pin-and-slot epicyclic mechanism, which is the circumference of a big circle with the Earth at its center, came more than a millennium before the first known clocks recorded in antiquity (Marchant, 2009)

Figure 1-5 Reconstructed Antikythera Mechanism



Source: (Freeth & & Jones, 2012)

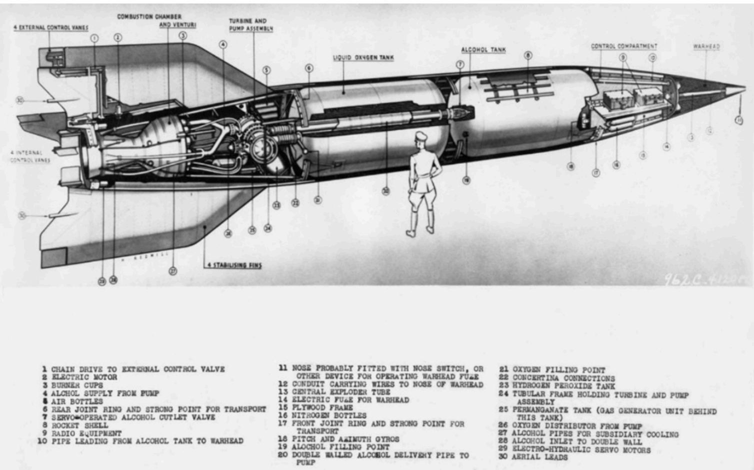
This phase of our story would last for nearly 2100 years. This time frame would include the likes of Abd al-Rahman al-Sufi (Azophi), who developed detailed star charts for each of the major constellations in the 10th Century. This would be followed by many great insights developed by Ibn ash-Shatir (planetary motions that were empirically testable, 14th

Century), Nicolaus Copernicus (Earth is not the center of the universe, 16th century), Sir Isaac Newton (Law of Universal Gravitation, 18th Century). The research phase largely ended at the beginning of the 20th Century (in 1905) when Special Relativity was first published by Albert Einstein (and General Relativity in 1915). It is during this time that the *development phase* of our story truly begins. In the early 20th Century, with scientific advances by Konstantin Tsiolkovsky, Robert H. Goddard, and Hermann Oberth (Neufeld, 2012). Initiated within Germany in the 1920s by Fritz von Opel and Max Valier, the first effective large-scale rocket experiments were ultimately performed by Werner von Braun. This is when *space technologies* finally begin to take shape.

Space Technologies

In October 1957, the Soviet Union sent the Sputnik 1 satellite into Space. This was the first time an artificial satellite was put into Earth's orbit. The satellite weighed 83 kg (183 lb) and orbited Earth at an altitude of 250 km (160 mi). Broadcasting for the world to hear, Sputnik produced a heartbeat signal at 20 megahertz. However, most people do not realize that Sputnik was, in fact, not the first time we put technology into Space. The first human-made object to ever reach outer Space was achieved by the Germans in 1944 via the *Aggregat 4****[2]*** (commonly known as the V-2) rocket development program (See Figure 1-6, V-2 Cutaway Diagram).

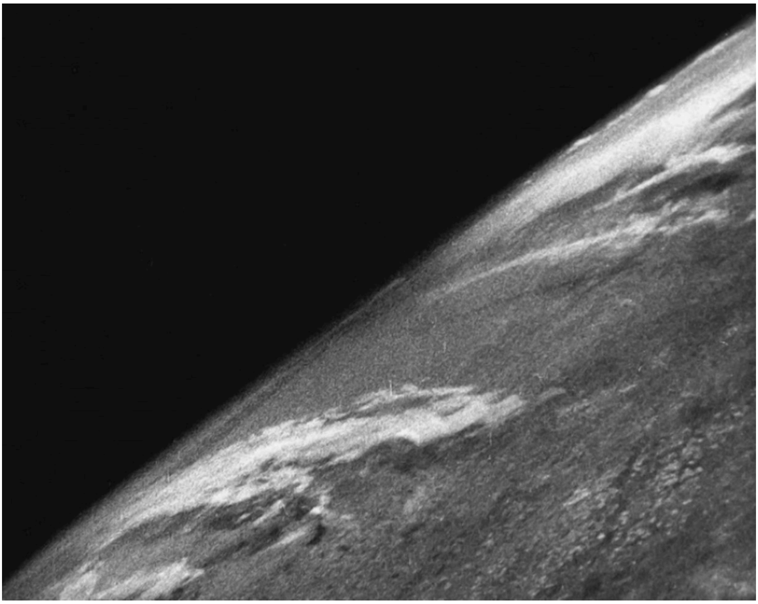
Figure 1-6 V-2 Cutaway Diagram


4 EXTERNAL CONTROL VANES
COMBUSTION CHAMBER AND VENTURI
TURBINE AND PUMP ASSEMBLY
LIQUID OXYGEN TANK
ALCOHOL TANK
CONTROL COMPARTMENT
WARHEAD
4 INTERNAL CONTROL VANES
4 STABILISING FINS
1 CHAIN DRIVE TO EXTERNAL CONTROL VALVE
2 ELECTRIC MOTOR
3 BURNER CUPS
4 ALCHOL SUPPLY FROM PUMP
5 AIR BOTTLES
6 REAR JOINT RING AND STRONG POINT FOR TRANSPORT
7 SERVO-OPERATED ALCOHOL CUTLET VALVE
8 ROCKET SHELL
9 RADIO EQUIPMENT
10 PIPE LEADING FROM ALCOHOL TANK TO WARHEAD
11 NOSE PROBABLY FITTED WITH NOSE SWITCH, OR OTHER DEVICE FOR OPERATING WARHEAD FUZE
12 CONDUIT CARRYING WIRES TO NOSE OF WARHEAD
13 CENTRAL EXPLODER TUBE
14 ELECTRIC FUZE FOR WARHEAD
15 PLYWOOD FRAME
16 NITROGEN BOTTLES
17 FRONT JOINT RING AND STRONG POINT FOR TRANSPORT
18 PITCH AND AZIMUTH GYROS
19 ALOCHOL FILLING POINT
20 DOUBLE WALLED ALCOHOL DELIVERY PIPE TO PUMP
21 OXYGEN FILLING POINT
22 CONCERTINA CONNECTIONS
23 HYDROGEN PEROXIDE TANK
24 TUBULAR FRAME HOLDING TURBINE AND PUMP ASSEMBLY
25 PERMANGANATE TANK (GAS GENERATOR UNIT BEHIND THIS TANK)
26 OXYGEN DISTRIBUTOR FROM PUMP
27 ALCOHOL PIPES FOR SUBSIDIARY COOLING
28 ALCOHOL INLET TO DOUBLE WALL
29 ELECTRO-HYDRAULIC SERVO MOTORS
30 AERIAL LEADS

Source: (forbes, 2019)

On June 20, 1944, the Germans performed a test launch with a rocket cryptically named MW 18014 (an A-4 rocket) at the Peenemünde Army Research Center. MW 18014 reached an apogee.[3] of 176 kilometers (109.3 miles…well above the Kármán line[4]). It was the first artificial object to enter Space and the first suborbital flight of a human-made object. While MW 18014 did enter orbit for a short period, it could not maintain orbital velocity and crashed back to Earth. During (and shortly after) the conclusion of World War II, Russia and the United States embarked on an intellectual property acquisition spree. The United States began acquiring a significant amount of science from Germany (nuclear physics and rockets) and Japan (biochemical weapons). After World War II, A-4 rocket hardware was quickly acquired by both Russia and the United States. Using a highly modified A-4 (V-2) rocket, the United States (US) captured the first-ever image of Earth from outer Space from the White Sands Missile Range in New Mexico (Vinogradov, 1968). In 1946, the footage was taken using a 35mm camera placed between the fuel tanks of the V-2 rocket (See Figure 1-7, First Photo of Earth). A single rocket launch from the New Mexican desert ignited the Space Race, the Cold War, and experimental space sciences all at once (Kelvey, 2021).

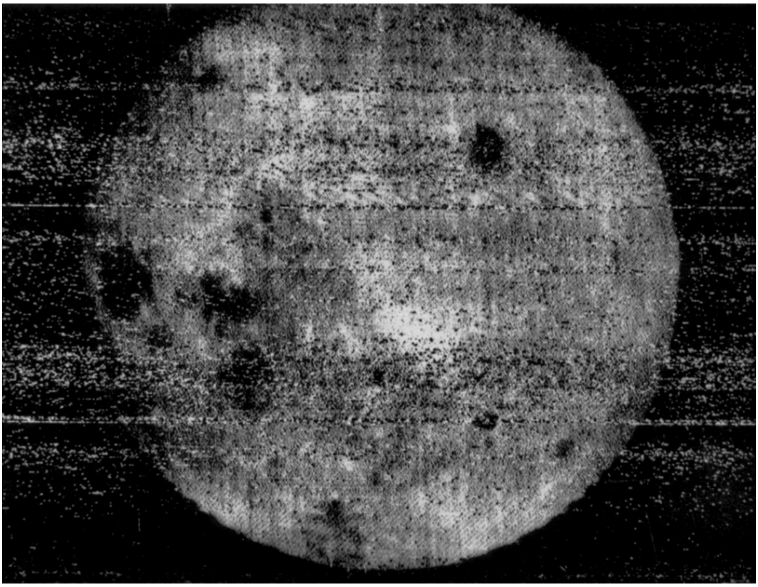
Figure 1-7 First Photo of Earth



Source: White Sands Missile Range / Applied Physics Laboratory (Pinterest, 1947)

Space technologies made rapid progress over the next two decades. The Soviet probe Luna 2, which made a hard landing on September 14, 1959, was the first spacecraft to make contact with the Moon's surface. On October 7, 1959, the Soviet (USSR) spacecraft Luna 3 took the first image of the Moon's far side (see Figure 1-8. Far Side of the Moon). The USSR successfully sent the first human into Space, Vostok 1, in April 1961. Automatic systems managed the whole mission. This was due to uncertainty on how a human may respond to weightlessness among medical personnel and spacecraft engineers. While the USSR was a dominant space engineering power throughout the 1950s and 1960s, the US made progress on human spaceflight via Project Mercury. Project Mercury was the first crewed US space program from 1958 to 1963. It had a round-trip objective; with a safe return, launch a man[5] into Earth orbit. The National Aeronautics and Space Administration (NASA) was formed and took over the program from the US Air Force. Six successful astronaut flights were performed.

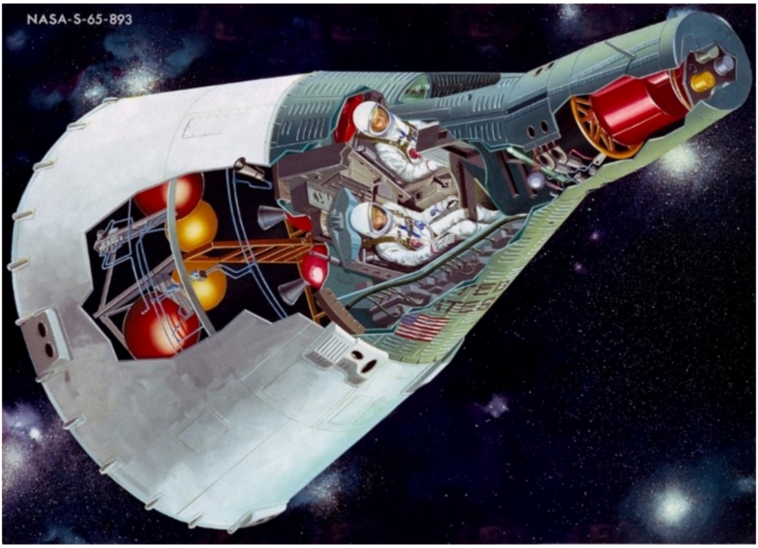
Figure 1-8 Far Side of the Moon



Source: Russian Space Agency (rankred, 2020)

NASA's second human spaceflight initiative was Project Gemini. Gemini, a project between Mercury and Apollo, began in 1961 and ended in 1966. Two astronauts were aboard the Gemini spacecraft (See Figure 1-9. Gemini Capsule Cutaway). In 1965 and 1966, 16 different astronauts and 10 Gemini teams completed low Earth orbit (LEO) flights. Gemini's goal was to create spaceflight technologies to help Apollo achieve its goal of putting humans on the Moon. Showing mission endurance up to slightly under 14 days, longer than the eight days needed for a round journey to the Moon, enabled the United States to catch up with human spaceflight capabilities that the Soviet Union had attained in the early years of the Space Race. In the race for Space, the US would eventually surpass the USSR. The Apollo 8 crew were the first humans to enter lunar orbit and actually sight the Moon's far side on December 24, 1968. On July 20, 1969, the US made the first human landing on the Moon. Commander of Apollo 11, Neil Armstrong, was the first person to set foot on the Moon.

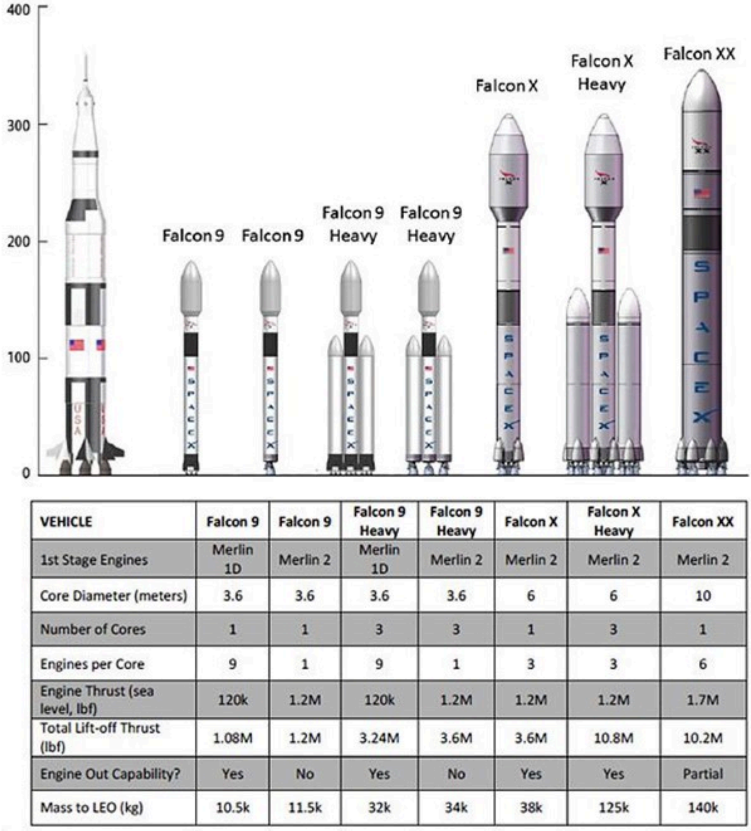
Figure 1-9 Gemini Capsule Cutaway



Source: (NASA, 2022)

Since then, space technology has advanced rapidly, enabling humans to land on the Moon and deploy extrasolar spacecraft.[6], explore other planets, and planetoids[7]. The *development phase* ended, and the *operational phase* began at 01:29 UTC on December 22, 2015. On flight 20, a Falcon 9 rocket launch became the first successful return (via vertical landing) of an orbital rocket's first-stage booster. After a five-year program to create a reusable launch system, the first stage made a successful landing. The success of flight 20 was a history-making moment for human spaceflight. It marked a significant milestone toward reusable and modular rocket systems that can significantly reduce the cost of launching payloads into orbit (Figure 1-10, SpaceX Falcon Rocket Program).

Figure 1-10 SpaceX Falcon Rocket Program



VEHICLE	Falcon 9	Falcon 9	Falcon 9 Heavy	Falcon 9 Heavy	Falcon X	Falcon X Heavy	Falcon XX
1st Stage Engines	Merlin 1D	Merlin 2	Merlin 1D	Merlin 2	Merlin 2	Merlin 2	Merlin 2
Core Diameter (meters)	3.6	3.6	3.6	3.6	6	6	10
Number of Cores	1	1	3	3	1	3	1
Engines per Core	9	1	9	1	3	3	6
Engine Thrust (sea level, lbf)	120k	1.2M	120k	1.2M	1.2M	1.2M	1.7M
Total Lift-off Thrust (lbf)	1.08M	1.2M	3.24M	3.6M	3.6M	10.8M	10.2M
Engine Out Capability?	Yes	No	Yes	No	Yes	Yes	Partial
Mass to LEO (kg)	10.5k	11.5k	32k	34k	38k	125k	140k

Source: SpaceX Corporation (SpaceX, 2022)

Space technologies span many categories: orbital launch systems, spacecraft, space stations, spaceflight, energy, communications, propulsion, navigation, security, and life-support. With increasing diversity, humans have been expanding their technological footprint; here is a summary snippet of our current technological capabilities:

- **Launching and moving space mobility and logistics** – Technologies in the space mobility and logistics (SML) area support the transportation of people and supplies into – and across – Space. This can include bringing astronauts to and from the International Space Station or transporting materials to be used in construction projects in Space. However, it also includes two important subcomponents: space accessibility and on-orbit sustainment. Space access includes the launch services to move a spacecraft from Earth to orbit (Operations, 2022). The durability of space operations is reinforced by using ridesharing and alternative launch services and sites. The lifespan of a spacecraft, including maintenance, reconstitution operations, operational deterioration or loss, and end-of-life actions, is included in on-orbit sustainment. These activities are supported by maneuvers referred to as rendezvous and proximity operations (RPO). The United States Government is no longer the dominant leader in this area. Advances in operational SML technologies are largely driven by private corporations (Orozco & & Simpson, 2020).

- **Exploring and mapping the solar system with**

robotic spacecraft – Robotic spacecraft are often used to explore and map the solar system. These missions are planned and executed by teams of scientists and engineers, who use the data gathered by the spacecraft to learn more about the planets and their moons. Robotic missions have also been used to study comets, asteroids, and other small bodies in the solar system. In 2020, 114 launches carried nearly 1,300 satellites into Space. The United Nations Office for Outer Space Affairs (UNOOSA) maintains an online index of objects launched into outer Space (United Nations Office for Outer Space Affairs, 2022). This list contains all objects ever launched into Space (i.e., including non-geocentric[8] Spacecraft). As of July 2022, there are 12,874 spacecraft located within the index. Four are classified as 'interstellar' (i.e., the Voyager and Pioneer programs).

- **Conducting research on the International Space Station** (as well as other governmental and soon-to-be commercial space stations) – The International Space Station (ISS) is a cooperative effort between multiple nations to conduct research in Space. Astronauts from various countries live and work on the station, conducting experiments in various fields. While it is starting to show its age, the space station has been used as a test bed for developing new technologies and has served as a platform for educational outreach programs. The International Space Station and Tiangong Space Station[9] They are the only operational space stations; however, there are plans to build commercially accessible space stations in the future. Private companies would own and operate these stations for research, manufacturing, and other commercial activities. It is difficult to say how soon commercial space stations would be up and running, as this depends on the development of the technology and the availability of funding. However, several companies are working on this technology, and it is possible that we could see commercial space stations in the next few years (Fiorentino, 2022).

- **Building and operating telescopes to study the universe** – Telescopes are often used to study the universe. They can be used to observe distant galaxies, stars, and other celestial bodies. Telescopes can also study the Sun, Earth's atmosphere, and other objects in our solar system. The most advanced telescopes in current operation are the Hubble Space Telescope and the James Webb Space Telescope. Launched in 1990, the Hubble

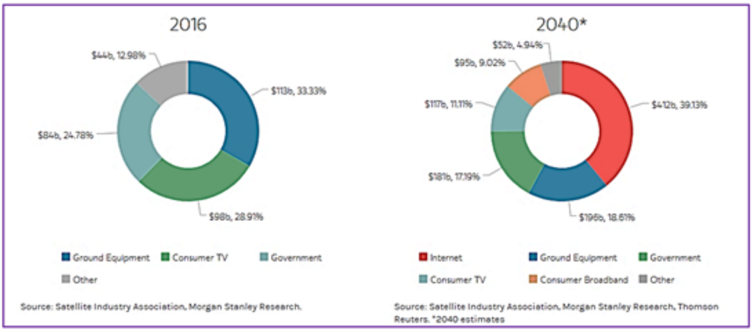
Space Telescope has provided some of the most detailed images of the cosmos up until very recently. The James Webb Space Telescope is a space-based telescope that began its first light operations in June 2022. Employing a liquid nitrogen-chilled beryllium mirror, it is currently the most powerful telescope ever built, with an ability to see back in time to the very early days of the universe.

- **Searching for space mining candidates** – While space mining is still ways away, searching for resources on other planets is currently occurring. If we can establish a permanent human presence on another planet, then we will need the ability to mine that planet for resources such as water, minerals, and energy. This would require developing new technologies to extract and process these materials. Humans have already discovered many ideal space mining candidates. For example, the large asteroid Ceres is a good space mining candidate; it is an asteroid that contains water and other minerals. It is also relatively close to Earth, which makes it easier to reach with current technologies (Ermakov, 2017). Other good candidates for space mining include the asteroids Vesta and Psyche, as well as the planet Mars (Thomas & Makowski, 2011). These bodies all contain water and other minerals that humans could use. Additionally, the

> complex moon systems on Jupiter and Saturn make excellent space mining candidates. For example, with an abundance of hydrocarbons, the Saturnian Moon Titan makes for a great forward operating fuel depot of the future.

Of course, there is a close relationship between space technologies and space operations. Space technologies enable space operations and space activities, while space operations use space technologies. According to the North Atlantic Treaty Organization (NATO), Space was declared an operational domain in November 2019 (Sultan, 2022). While this designation may have a militaristic focus, it extends well into the economic aspects of the domain as well. Morgan Stanley estimates that the global space industry may surge to over $1 trillion by 2040 (Stanley, 2022).

Figure 1-11 Future Growth of the Space Economy



Source: Satellite Industry Association, Morgan Stanley Research.

Source: Satellite Industry Association, Morgan Stanley Research, Thomson Reuters. *2040 estimates

Source: Morgan Stanley (Stanley, 2022)

Figure 1-12 Space, From Ideation to Operation

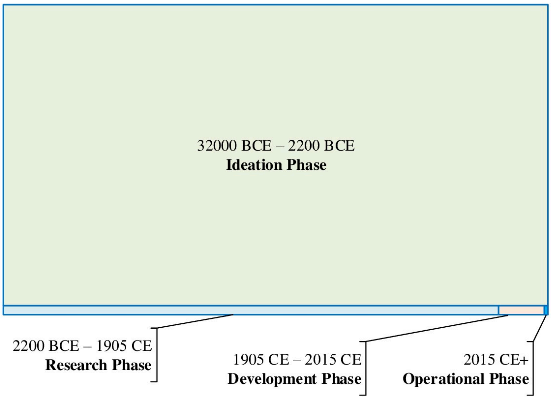


Figure 1-12 Space, From Ideation to Operation

Source: (Pritchard M.)

Source: (Pritchard M.)

So, there you have it, from our early ideation roots 34,000 years ago to the present day, we have come a long way (See Figure 1-12, Space: From Ideation to Operation). We have only just begun the operational phase of our journey. The pace of technological development in this domain is running at an exponential rate, and the rate of progress is increasing

(Berman, 2016). From here, what are the top technological priorities?

Enhancing Space Operations: Top Technological Priorities

Space Domain Awareness

Formerly known as space situational awareness (Erwin, Air Force: SSA is No More; It's Space Domain Awareness, 2019), Space Domain Awareness (SDA) is focused on tracking objects in Space, identifying them, determining their orbits, comprehending the environment they are working in, and projecting their future positions and any hazards to their operations. Data is used to forecast conjunctions between objects and warn space operators of potentially hazardous close approaches to enable collision avoidance operations. On occasion, it would be necessary to anticipate and respond to meteor storm debris, fragmentation event debris, or other natural events that could impact operations. All space safety and space traffic management operations are predicated on SDA. Space traffic management (STM) is defined as using SDA to accomplish a real-time goal.

It is crucial to thoroughly understand all the satellites' orbits as space activity rises. Integrating data from more sensors, even those belonging to our allies, is one method to increase tracking capabilities. There are a variety of difficulties involved with incorporating external data, and there is no assurance that having more data would lead to better tracking. Aerospace has assisted government investigations in exploring the implications and advantages of adding satellite tracking information from foreign sensors into US space object catalog upkeep.

Among many other things, SDA accomplishes the following:

- Ability to perform orbital tracking, determination, and flight predictions at scale
- Creating an ongoing orbital space inventory of items manufactured by humans
- Provide multi-modal data for the development of new offensive and defensive capabilities

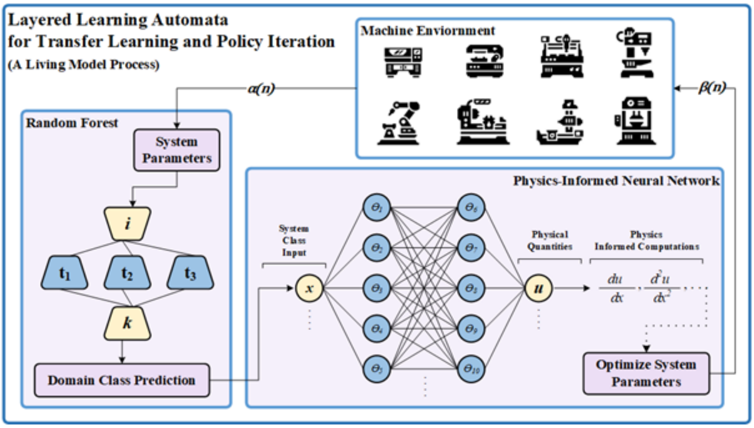
A complex and crowded space environment results from the ongoing development of new space technologies and spacefaring entities, as well as the existence of dangerous debris. For instance, in 2021, there were approximately 3,372 active satellites in the Earth's orbit, more than twice the number of satellites in orbit five years ago. The increase in the number of satellites in orbit is due to the expanding importance that space systems play in terrestrial applications, including GPS, meteorology, and telecommunications. Additionally, the number of satellites is growing due to the continual growth in the number of spacefaring nations and the expansion of space commerce. The commander of US Space Command, Gen. James Dickinson, recently called space domain awareness the command's "No. 1 need." (Erwin, Space Domain Awareness: A Secret Weapon Against Shadowy Threats in Orbit., 2022).

The development of SDA requires transdisciplinary development programs. For example, mechanical engineering, electrical engineering, or computer science alone cannot achieve SDA. It requires a wide range of applied transdisciplinary program expertise in Machine Learning, Autonomous Systems, Modeling & Simulation, Cyber Human Systems, Cyber-Physical Systems, and Remote Sensing. Each of the areas mentioned earlier leverages a *Systems Engineering* approach (Aniculaesei, 2018) (Roscoe, 2019); (Tadjdeh, 2018); (Mittal, 2008); (Akkaya, 2016). While the traditional verticals of engineering education (i.e., mechanical, electrical, computer, chemical, industrial, etc.....) are still very important for building specialized vertical expertise within their respective domains, space systems require transdisciplinary systems engineering program skills to be successful (Watson, 2020).

Machine Learning & Autonomous Systems

Autonomous and automated systems incorporate machine learning into the intelligent management and control of complex systems (Nilsson, 1982). Although they may include crew members as part of the operation, autonomous systems are run independently of other management and control systems. Crewed ships, planes, and spacecraft are instances of autonomous systems. Despite having centralized or decentralized management and control, automated systems are not dependent on human operators. The incorporation of system physics highlights an emergent area for autonomous systems research and operations. For example, Physics-Informed Neural Networks (PINN) can dramatically reduce the amount of onboard training data required to perform autonomous shipboard tasks. A physics-informed autonomous systems integration gives an AI a better ability to manage and predict system dynamics ((Mao, 2020); (Raissi, 2019). PINN seeks to integrate physics-based knowledge in mathematical equations and data-driven AI/ML for complex scientific and engineering problems (See Figure 1-13, Layered Learning Automata).

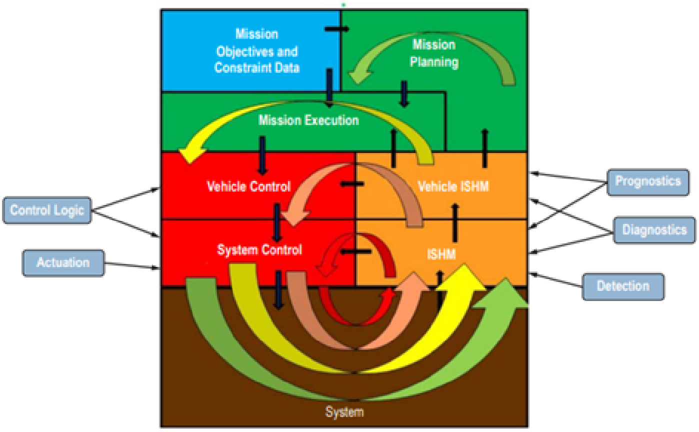
Figure 1-13 Layered Learning Automata



Source: (Pritchard M.)

For AI judgments to be useful concerning system operations, each system function, subsystem, and environment must be as efficient as possible. New AI models that can leverage less training data – while still maintaining precision, recall, and accuracy – will be better positioned to propagate beneficial second-order effects throughout the system (e.g., fewer computational operations per second, increased system responsiveness, less system power required, etc.....).

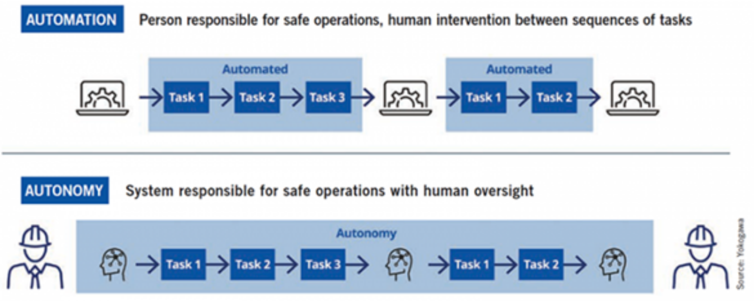
Figure 1-14 Autonomous System Stack



Source: (Watson, 2020)

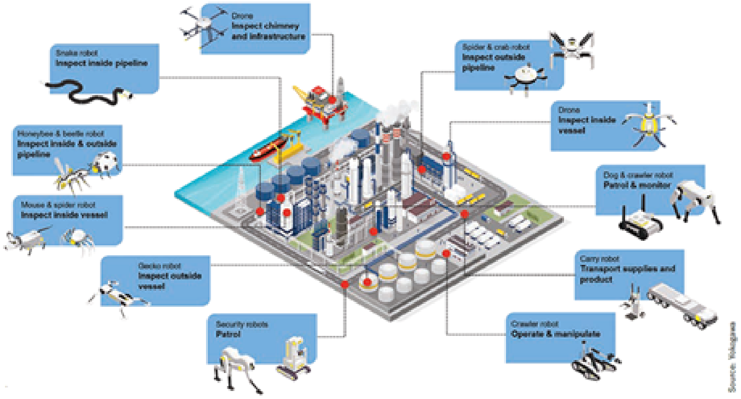
The difference between automation and autonomy must be understood. Automation is the substitution of mechanical action for human action. This automation may be integrated into the system or used independently in a control center. The relative physical and/or functional separation of decision-making and action or response capacities is referred to as autonomy (e.g., independence of action from a control location). Simply stated, the term automation describes a system process carried out deterministically without human involvement. An automation system cannot extend beyond what it was procedurally developed to do. An autonomous system is an intelligent system that illustrates autonomy when its system process can logically coordinate deterministic, non-deterministic, and stochastic learning functions.

Figure 1-15 Automation versus Autonomy


AUTOMATION
Person responsible for safe operations, human intervention between sequences of tasks
Automated
Task 1
Task 2
Task 3
Automated
Task 1
Task 2
AUTONOMY
System responsible for safe operations with human oversight
Autonomy
Task 1
Task 2
Task 3
Task 1
Task 2
Source: Yokogawa

Source: (Fiske, 2021)

Figure 1-16 Automation versus Autonomy



Source: (Fiske, 2021)

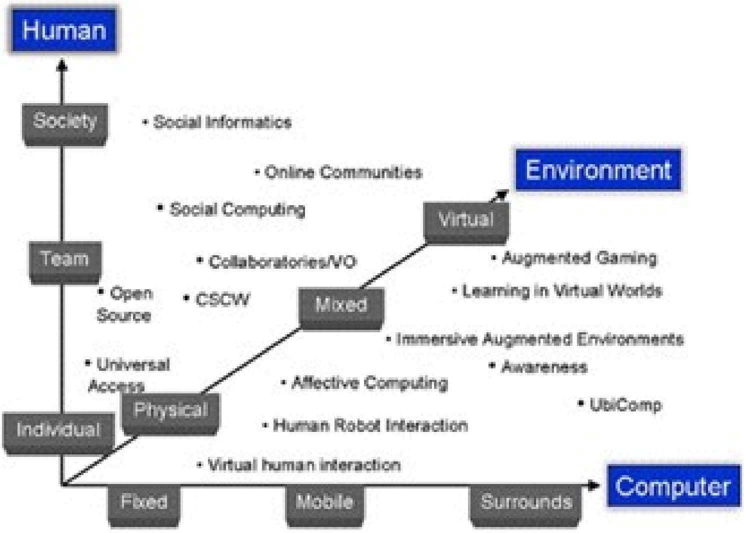
According to a joint study conducted by TEConomy Partners LLC, the global market for terrestrial autonomous mobile systems alone is predicted to increase to an estimated

$802 billion by 2025–2026. That figure can potentially exceed $1 trillion when Defense, airborne, and autonomous marine systems are included to represent the larger autonomous mobile systems market sector (Tripp, 2021). And just a small portion of that market value will be made up by self-driving automobiles. The scope of autonomous technology, including robotics, artificial intelligence, autonomous cars, and other related sectors, is far greater and broader than that (i.e., space systems operations and exploration).

Cyber-Human Systems

Cyber-Human Systems is a developing transdisciplinary field. Robots, wearable technology, personally integrated sensors & computers, and virtual & augmented reality, are examples of Cyber-Human Systems (Eskins, 2011); (Krugh, 2018). The NSF classifies trends within Cyber-Human Systems (CHS) as taking place across three dimensions: people, computers, and the environment (Foundation, 2022). The human dimension encompasses everything from individuals to society. An important fundamental aspect of CHS is Cybernetics. Cybernetics offers a solution for how a system that controls another system might make up for greater control process mistakes by having a wider range of operational possibilities (Chacón, 2020). The human will take on the function of a higher-level control instance since they are the most adaptable entity in the cyber-physical framework (Barbosa, 2018).

Figure 1-17 Cyber Human Systems



Source: (Foundation, 2022)

The computer dimension includes anything from stationary computing equipment, where a person must be close by, to portable devices (which follow a person wherever they go) to embedded computational systems comprising sensors and visual/auditory devices. Extended reality systems[10] fall in the center of the environmental dimension, which includes discrete physical computational devices and lifelike virtual worlds. Cyber-human systems are a key national security component for the United States; it is part of their "third offset strategy" (Tadjdeh, 2018) (Freedberg Jr, 2014).

Modeling & Simulation

Modeling and simulation (M&S) technologies are used to generate advanced models. Models can be physical, mathematical, or logical representations of systems, entities, phenomena, or processes. In the computer application of modeling and simulation, a mathematical model that comprises important physical model parameters is built on a computer. The mathematical model simulates the physical model and applies the necessary circumstances to set up the desired experiment. A simulation often refers to a computerized version of the model performed over time to analyze the effects of the stated interactions. In general, simulations are developed iteratively. When a sufficient degree of knowledge is achieved, one constructs a model, simulates it, learns from the simulation, revises the model, and repeats the process.

- System:
    - A system exists and operates within four dimensions (*x, y, z, & t*)[11].
- Model:
    - A model is a system representation within these

four dimensions.

- Simulation:
  - A simulation enables human perception, interaction, and analysis of system dimensionality within a complex domain.

The major benefit of high-fidelity modeling and simulation (M&S), supported by high-performance computing, advanced information processing, and artificial intelligence, is the empowerment of a virtual solution space that allows for lower-cost validation of new design concepts. This can provide valuable insights into the relationships between the simulated environment and associated system responses. M&S frameworks also allow for large-scale data analysis and integrated system testing, increasing our ability to find new scientific discoveries. This creates an ability for near real-time numerical experimentation to explore mission trade spaces and evaluate complex systems throughout their lifecycle. Additional M&S opportunities include:

- Reducing program acquisition and systems integration costs through rapid modeling and prototyping of systems
- Immersive visualization systems: 3D immersive, augmented, virtual, and mixed reality technologies for visualization and training

- Predictive threat modeling, agent-based simulations, wargaming & simulation technologies, and multi-domain risk modeling
- Support research, development, and acquisition programs by leveraging advanced simulation technologies to reduce technical risks
- Provide specialized industry training capabilities via advanced simulators and highly immersive scenarios
- Support training and decision-support systems that increase performance and safety while decreasing cost by using modeling and simulation directly in mission systems.
- Increasing mission readiness and outcomes through advanced threat modeling
- Process Modeling and Gaming: Predictive models using machine learning algorithms
- Fosters collaboration among federal agencies, industries, and academia

While Modeling & Simulation activities are traditionally focused on artificially representing the dimensionality of physical systems, new research areas are exploring Real-time Model Projections & Simulation Effects. For example, if you are in a pilot simulation flying across the United States, actual weather patterns would be modeled in real-time within the simulation. In the reverse, simulated models (and digital twins) can be projected over real-world objects to enhance and highlight important physical object features (both externally and internally).

Cyberspace within Space

Cyberspace and extraterrestrial security challenges are merging. Space-based communication and information services are becoming more and more important to the internet. Similar to cars and medical equipment, satellites and other space assets are considered devices on the internet of things since they operate on internet-based networks. Space-related activities are growing and changing due to new government actors, businesses, ambitions, and technologies. However, neither cybersecurity nor space policy is equipped for the difficulties brought about by blending cyber and physical Space, which could raise national security vulnerabilities.

Since the 1950s, spacefaring nations have prioritized the security of outer Space. Governments launched space projects for intelligence, military, political, and scientific reasons. They also created defenses against rivals' space-based threats, such as anti-satellite weapons. By outlawing the deployment of nuclear and other high-tech weapons in Space and collaborating on peaceful uses of the planet, nations regulated security competition. The commercial sector's use of dual-use technologies to offer satellite communication services was sparked by government projects. In contrast to a decade ago, the pace of technological advancement is now enabling nations, international groups, enterprises, and people to utilize space capabilities. In other words, the game has changed as more nations advance their capabilities to reach Space.

Understanding the specific cyber vulnerabilities that develop in distinct space operations is necessary for protecting space activities. For instance, ground stations, communications to and from Earth, and satellites themselves are all included in satellite cybersecurity. The American military and intelligence systems are susceptible to physical and digital attacks, given the absence of cybersecurity in their design, the usage of commercially available components, and the vulnerabilities that could be produced by connecting satellites to operate as intricate, circling networks, civilian smallsat.[12] Systems may likewise prove to be vulnerable. Considering what we've previously seen with regulatory oversight of key infrastructures that are already in place, regulatory action will similarly proceed slowly to allow for efficient responses to cyber threats from Space. To effectively counter threats, we must look beyond conventional deterrence tactics. As new technologies come online, new standards must be created.

Space Manufacturing & Mining

Mostly still in the research phase, the developing sector of space mining is filled with both potential and difficulties (Sivolella, 2019). For instance, Ceres has an escape velocity of 0.51 km/s and surface gravity of 0.029 g. By comparison, Earth has an escape velocity of 11.186 km/s and surface gravity of 1.00 g. While you could stand up and maintain your balance without floating off the dwarf planet, a game of basketball on Ceres would be radically different. It would take around 10 seconds for an object to fall over. Anything kicked up during mining activities (e.g., debris, dust, etc.....) would stay in the air for considerably longer. Due to the significantly reduced friction, your earth-based skid steer would have difficulty scooping up loose materials (e.g., space dirt would quickly turn into a cloud of dirt around the operator). Additionally, mining machines would require new tethering technologies to maintain proper planetary surface tension. A small drilling rig would easily tip over if it tried to drill into the surface of a dwarf planet without being first anchored to the surface.

Figure 1-18 Ceres, Dwarf Planet in the Asteroid Belt

Source: (NASA, 2022)

The question for space mining is one of timing. Technological developments in the space sector continue to accelerate. Launch and operations costs are falling as reusable rocket components become more common and off-the-shelf parts are used more frequently. Private companies are now emerging as leaders in developing emergent space activities (e.g., orbital manufacturing, smallsat services, and orbital tourism). While previously limited to government entities, these activities have become commercially accessible. As we have said before, the current market value of the space industry sits at roughly $400 billion; the space industry might reach $1 trillion by 2040 as private investment surges.

The concept is transitioning from the domain of science fiction into the world of scientific fact as several firms are already forming with the specific goal of asteroid prospecting, exploration, and mining. Space mining opportunities can be made by making orbital refueling cheaper, lowering overall mission costs, enhancing space manufacturing activities, and, more broadly, developing a better understanding of operating in space environments. Although there are still many unknowns, space mining eventually promises to speed up space exploration and strengthen terrestrial economies significantly. While the Industry in Space's interests may sometimes conflict with those of science, the infrastructure built during these early stages will shorten the space mining timeline.

Remote Sensing & Surveillance

Commercial Space remote sensing's revolution can change how national security experts see indicators and warnings of hostile operations. Commercial sensing gives orders of magnitude higher coverage and visitation rates that can supplement and enhance the sensing capabilities supplied by more exquisite government-owned and government-operated systems rather than relying solely on high-demand, low-density government-owned national assets. With the help of artificial intelligence, human analysts will no longer have to laboriously count bombers and tanks in pictures, and robots will be able to look at enemy movements collectively across enormous territories at a scale and pace that is not humanly conceivable. Machines can simultaneously collect data from all domains, operational locations, and intelligence sources to inform their algorithms, unlike humans, who must develop expertise in knowing how enemies typically operate in a small number of important areas.

Machines can detect subtle changes in large data sets that human analysts might miss in the data noise and combine them with other open-source data to produce useful insights. These automated insights, which are communicated to people via alerts, put analysts in the best position to make recommendations and conclusions based on the totality of the circumstances. To support a US deterrence action, machine learning systems can process the raw data to generate products that improve early warning awareness and empower people to take more educated judgments. Early warning systems that focus on people frequently cause late awareness and reactive actions. Reactive state entities will struggle to attain dominance in an environment where larger government actors are engineering evermore advanced decision support systems to simulate and forecast advanced operational movements within a given domain. A nation can actively dissuade and respond to threats only if it has the technological skills, workforce, and capabilities to remotely understand enemy actions more quickly.

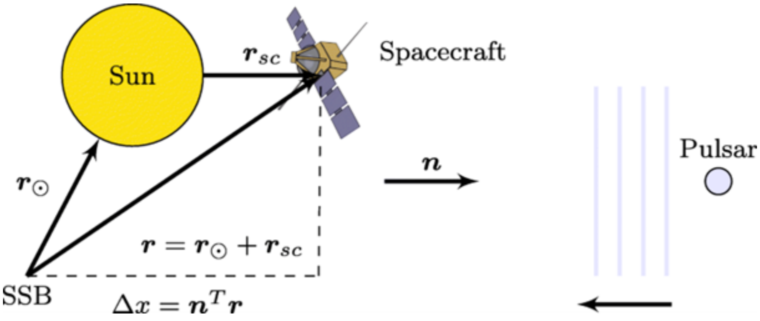
For more than 60 years, remote sensing technologies have been crucial to intelligence-gathering efforts. This capability is directly correlated to an ability to project power within a given domain. Although the remote sensing paradigms that were initially established (government-developed satellites, manual processing, and siloed data) were beneficial to the United States during the Cold War, developments in commercial frameworks have the potential to change these paradigms in ways that offer new benefits. The commercial remote sensing sector is advancing quickly. Remote sensing technologies rely heavily on integrating Machine Learning Systems to swiftly transform unprocessed sensory data into knowledge that human analysts can use.

Celestial Positioning Systems

To expand spacecraft capabilities, future deep space missions will need accurate positioning, navigation, and timing (PNT) systems. This technology must withstand radiation exposure and wide temperature swings in deep space conditions. The design of spaceborne instruments and components must now meet new requirements due to these operational needs. Spacecraft must regularly contact Earth to verify their position without pulsar navigation. However, such communication is time-consuming, expensive, and gets harder the further a probe is from Earth. Systems like NASA's Deep Space Network, a collection of enormous satellite dishes, are used for this purpose.

Pulsars are incredibly precise clocks, especially millisecond ones. These pulses, best seen in X-rays, can be used akin to GPS satellites. Naturally, GPS signals have a timestamp that enables a receiver to estimate the satellite's distance and measure the delay with which they come. Although pulsars are very distant, they allow us to measure the period precisely between pulses. Due to the Doppler shift, there will be a temporal discrepancy between them. They are then very simply translated into speed. However, calculating a position requires more mathematical skills.

Figure 1-19 Pulsar-based Navigation



Source: (Chen, 2020)

Until recently, we had to compare the pulsar signal with a relayed signal from a known location in the solar system to extract these measurements. However, more recent research has developed the mathematical framework necessary to enable a spaceship to plot its position in Space fully (and independently). Practically, an initial position can be established with a minimum of four pulsars. A spacecraft might determine its location in Space to within three miles by integrating information from a pulsar's pulses with a reference point. Pulsar navigation systems have more signals available to them versus traditional satnav.[13] Systems have more resistance to jamming and spoofing due to the wide range of frequencies accessible and the security of signal sources against possible anti-satellite operations (Adamson, 2022).

Conclusions

We started 34,000 years ago and brought you to the present. We covered the operational and technological highlights of each time period. This chapter – and each of the chapters within this book – could be their book. In other words, this is by no means an exhaustive view of the Industry; however, it is a nice view of where the space industry is today and where it is heading. As you navigate the remaining chapters, you will find additional details, concepts, technologies, and use cases.

The top technological priorities illustrated in this chapter will be exhibited in varying detail as you progress through each of the readings. Each will provide emergent ideas and innovative perspectives on space systems. Ideas are like spacecraft; they are meant to be launched, get out there and make things happen.

References

Adamson, J. (2022). Use of pulsars for ship navigation: an alternative to the sextant. *The Journal of Navigation*, pp. 1-20.

Akkaya, I. D. (2016). Systems engineering for industrial cyber–physical systems using aspects. *Proceedings of the IEEE*, pp. 104(5), 997-1012.

Aniculaesei, A. G. (2018). Toward a holistic software systems engineering approach for dependable autonomous systems. *In 2018 IEEE/ACM 1st International Workshop on Software Engineering for AI in AuEngineering for AI in Autonomous Systems (SEFAIAS) IEEE*, pp. pp. 23-30.

Barbosa, M. W. (2018). Managing supply chain resources with Big Data Analytics: a systematic review. *International Journal of Logistics Research and Applications*, pp. 21(3) 177-200.

Berman, A. a. (2016). *Technology Feels Like It's Accelerating – Because It Actually Is.* SingularityHub.

Biocca, F. (1992). Virtual reality technology: A tutorial. *Journal of communication*, pp. 42(4), 23-72.

Chacón, A. A. (2020). Developing cognitive advisor agents for operators in industry 4.0. . *New Trends in the Use of Artificial Intelligence for the Industry*, pp. 4, 127.

Chen, P. T. (2020). Aspects of pulsar navigation for deep space mission applications. *The Journal of the Astronautical Sciences*, pp. 67(2), 704-739.

Ermakov, A. I.-R. (2017). Constraints on Ceres' internal structure and evolution from its shape and gravity measured by the Dawn spacecraft. *Journal of Geophysical Research: Planets*, pp. 122(11), 2267-2293.

Erwin, S. (2019). *Air Force: SSA is No More; It's Space Domain Awareness.* Retrieved from https://spacenews.com/: https://spacenews.com/air-force-ssa-is-no-more-its-space-domain-awareness

Erwin, S. (2022). *Space Domain Awareness: A Secret Weapon Against Shadowy Threats in Orbit.* Retrieved from https://spacenews.com/: https://spacenews.com/air-force-ssa-is-no-more-its-space-domain-awareness

Eskins, D. &. (2011). The multiple-asymmetric-utility system model: A framework for modeling cyber-human systems. *In 2011 Eighth International Conference on Quantitative Evaluation of SysTems*, pp. pp. 233-242 IEEE.

Fiorentino, A. (2022). *The First Space Hotel Could Open as Soon as 2025. AFAR: The Future of Travel.* Retrieved from https://www.afar.com: https://www.afar.com/magazine/space-hotel-pioneer-station-to-open-in-2025

Fiske, T. a. (2021). *Industrial autonomy: How machines will perform their own maintenance. Plant Service.* Retrieved from https://www.plantservices.com/: https://www.plantservices.com/articles/2021/automation-zone-industrial-autonomy/

forbes. (2019, June). *v2-army-cutaway-1200×741.jpg.* Retrieved from https://blogs-images.forbes.com/brucedorminey/files: https://blogs-images.forbes.com/brucedorminey/files/2019/06/v2-army-cutaway-1200×741.jpg

Foundation, N. (2022). *Cyber-Human Systems. Computer and Information Science and Engineering (CISE).* Retrieved from National Science Foundation: https://www.nsf.gov/cise/iis/chs_pgm13.jsp

Freedberg Jr, S. J. (2014). Hagel Lists Key Technologies for US Military; Launches 'Offset Strategy. *Breaking Defense*, p. 16.

Freeth, T., & & Jones, A. (2012). The cosmos in the Antikythera mechanism. *Institute for the Study of the Ancient World (ISAW).*

Gaffney, V. (2013). Mesolithic timelords: a monumental hunter-gatherer" calendar" at Warren Field, Scotland. *Current archaeology*, pp. (283), 12-19.

Gheorghiu, D. &. (2013). *Place as Material Culture: Objects, Geographies and the Construction of Time.* Cambridge: Cambridge Scholars Publishing.

Google Images. (2018, June). *Nebra_Scheibe-1024×1007.jpg.* Retrieved from https://www.ancient-code.com/: https://www.ancient-code.com/wp-content/uploads/2018/06/Nebra_Scheibe-1024×1007.jpg

Kelvey, J. (2021). *75 Years Ago, A Nazi Rocket Took the First Photo of Earth from Space.* Inverse.

Krugh, M. &. (2018). A complementary cyber-human systems framework for industry 4.0 cyber-physical systems. *Manufacturing letters*, pp. 15, 89-92.

Mao, Z. J. (2020). Physics-informed neural networks for high-speed flows. *Computer Methods in Applied Mechanics and Engineering*, pp. 360, 112789.

Marchant, J. (2009). *Decoding the Heavens: A 2,000-Year-Old Computer–and the Century-Long Search to Discover Its Secrets.* NYC: Da Capo Press.

Mittal, S. Z. (2008). *Modeling and simulation for systems of systems engineering. Systems of Systems–Innovations for the 21st Century* . Wiley.

NASA. (2022). *Aurignacian Lunar Calendar.* Retrieved from https://i.pinimg.com/: https://i.pinimg.com/originals/c8/40/10/c84010201d8fd16ab2b768383e0af23a.jpg

NASA. (2022). *Gemini Capsule Cutaway.* Retrieved from https://i.pinimg.com/: https://i.pinimg.com/originals/74/d2/a5/74d2a5a9fe00775c751ac03f105e6aff.jpg

NASA; & Marshack . (2022, Aug 28). *oldest lunar calendars.* Retrieved from https://sservi.nasa.gov: https://sservi.nasa.gov/articles/oldest-lunar-calendars/

Neufeld, M. J. (2012). The Three Heroes of Spaceflight: The Rise of the Tsiolkovsky-Goddard-Oberth Interpretation and Its Current Validity. *Quest: The History of Spaceflight Quarterly*.

Nilsson, N. J. (1982). *Principles of artificial intelligence.* Springer Science & Business Media.

Operations, S. (2022). *Space Doctrine Note (SDN) Operations: Doctrine for Space Forces.* United States Space Force, Headquarters.

Orozco, J. A., & & Simpson, C. R. (2020). Commercial Crew successes lead the way in a pivotal year. *Aerospace America*, pp. 58(11), 69-69.

Peregrine, P. N. (2001). *Aurignacian. In Encyclopedia of Prehistory.* Boston, MA.: Springer.

Pinterest. (1947, Oct 24). *First Photo of Earth.* Retrieved from https://i.pinimg.com/: https://i.pinimg.com/originals/27/b8/74/27b874a0e9093ef8f2d236e5c4221c4b.jpg

Pritchard, M. (n.d.). Domains, Operations, Technologies. *Space Systems: Emerging Technologies and Operations 2022.* KSU, Manahattan, KS.

Pritchard, M. (n.d.). Space, From Ideation to Operation. *Space Systems: Emerging Technologies & Operations.* KSU, Manhattan, KS.

Raissi, M. P. (2019). Physics-informed neural networks: A deep learning framework for solving forward and inverse problems involving nonlinear partial differential equations. *Journal of Computational physics*, pp. 378, 686-70.

rankred. (2020, July). *Far-Side-of-the-Moon-by-Luna-3.* Retrieved from https://i1.wp.com/www.rankred.com/:

https://i1.wp.com/www.rankred.com/wp-content/uploads/2020/07/Far-Side-of-the-Moon-by-Luna-3.jpg?fit=779%2C600&ssl=1

Roscoe, R. D. (2019). *Advancing diversity, inclusion, and social justice through human systems engineering.* CRC Press.

Sivolella, D. (2019). *Space mining and manufacturing: Off-world resources and revolutionary engineering techniques.* Springer Nature.

Soderman, T. (2021). *SERVI, The Oldest Lunar Calendars. National Aeronautics and Space Administration.* Retrieved from https://sservi.nasa.gov/: https://sservi.nasa.gov/articles/oldest-lunar-calendars/

SpaceX. (2022). *SpaceX Falcon Rocket Program.* Retrieved from https://i.pinimg.com: https://i.pinimg.com/originals/f2/1a/47/f21a47342bb3ef674720f0bfc722f3df.jpg

Stanley, M. (2022). *A New Space Economy on the Edge of Liftoff.* Retrieved from https://www.morganstanley.com/: https://www.morganstanley.com/Themes/global-space-economy

Sultan, B. &. (2022). BRICS space diplomacy and response of non-Western countries: the inscription of Neo-Functionalism. *Journal of Humanities, Social and Management Sciences (JHSMS)*, pp. 3(1), 351-365.

Tadjdeh, Y. (2018). Defense Applications Envisioned For Cyber-Human Systems. Robotics and Autonomous Systems. *Robotics and Autonomous Systems, National Defense*, pp. 102(774), 40-45.

Thomas, V. C., & Makowski, J. M. (2011). *The dawn spacecraft. In The Dawn Mission to Minor Planets 4 Vesta and 1 Ceres.* NYC: Springer.

Tripp, S. (2021). Self-driving cars only a fraction of projected $1-trillion global autonomous technology market. *Boston Business Journal.*

United Nations Office for Outer Space Affairs. (2022). *Online Index of Objects Launched into Outer Space. United Nations Office for Outer Space Affairs.* NYC: United Nations.

Vinogradov, B. V. (1968). *Space Photography for the Geographic Study of the Earth (No. NASA-CR-93287).* Houston: NASA-CR-93287.

Watson, M. M. (2020). *Engineering Elegant Systems: Theory of Systems Engineering. National Aeronautics and Space Administration.* Marshall Space Flight Center.

Wikimedia. (2022). *440px-NAMA_Machine_d%27Anticyth%C3%A8re_1.jpg.* Retrieved from https://upload.wikimedia.org/: https://upload.wikimedia.org/wikipedia/commons/thumb/6/66/NAMA_Machine_d%27Anticyth%C3%A8re_1.jpg/440px-NAMA_Machine_d%27Anticyth%C3%A8re_1.jpg

Endnotes

[1] An information system need not be a computationally derived device; it can be a book, a carving, or hieroglyphs; any mechanism that allows for information storage is considered an information system.

[2] More commonly known as the V-2 rocket program, it was technically known as Aggregat 4 (A4) program. It was the world's first guided ballistic missile. It was fueled by a liquid propellent mixture of liquid oxygen and alcohol.

[3] Perigee is the location where an object comes closest to Earth. Apogee is the location where an object is furthest away from Earth. For orbital determinations around generic celestial bodies, we would use pericenter (periapsis, closest) and apocenter (apoapsis, furthest).

[4] The Fédération Aéronautique Internationale (FAI) uses the term Kármán line to define the boundary between aeronautics and astronautics. Aeronautics is aerial activities, including all air sports, within 100 km of Earth's surface. Astronautics are activities more than 100 km above Earth's surface. (100 kilometers equals 62.14 miles).

[5] The Mercury 13 were thirteen American women who completed the same physiological screening tests as the astronauts chosen by NASA on April 9, 1959. It was a privately funded initiative loosely affiliated with the Mercury program. Female astronaut candidates were not selected for spaceflight until Astronaut Group 8, for the Space Shuttle program, in 1978

[6] An extrasolar spacecraft is designed to travel beyond our solar system. These spacecraft are typically equipped with advanced power systems and innovative propulsion systems. Voyager 1 and Voyager 2 have left our Solar System. While not originally designed to be extrasolar spacecraft, both have reached interstellar Space.

[7] A minor planet is an astronomical object in direct orbit around the Sun that is exclusively classified as neither a planet nor a comet.

[8] Geocentric refers to spacecraft in Earth's orbit. Non-Geocentric would refer to all manner of spacecraft in other orbital patterns (e.g., heliocentric (Sun), selenocentric (Moon), areocentric (Mars), etc…).

[9] The Tiangong Space Station (TSS) core module was launched into low earth orbit (LEO) on April 29, 2021.

[10] Extended reality systems (XR) encompass Augmented

Reality (AR), Mixed Reality (MR), and Virtual Reality (VR). (Biocca, 1992)

[11] Three dimensions of Space (*x,y,z*) and one dimension for time (*t*)

[12] While there are no official standards when it comes to SmallSats (Small Satellites), it is a term used that includes the following: nanosatellites (1-10 kilograms), microsatellites (10 to 100 kilograms), and minisatellites (100 to 500 kilograms). The term also includes CubeSats, the only class of smallsats that are more clearly defined.

[13] A satellite navigation system (satnav) employs satellites to provide geospatial location. Satellite navigation equipment may pinpoint their location (longitude, latitude, and altitude/elevation) with great precision (within a few centimeters to meters).

2.

SATELLITE KILLERS AND HYPERSONIC DRONES (SLOFER)

Student Objectives

- Understand the concept and importance of satellite technology
- Various orbits and significance
- Threat deterrence and first strike capabilities in warfare
- Satellite countermeasures
- Satellite platforms for deployment of hypersonic weapons

This chapter will set a foundation for instruments to kill satellites. Some methods exploit existing hazards, and others have been intentionally devised for that purpose. However, each is discussion worthy when planning the destruction or protection of satellite assets. This chapter will cover physical considerations surrounding the deployment of Anti-Satellite

Weapons (AWS). For example, the layers of the atmosphere are important because air density will result in frictional drag; it will also affect Direct Energy Weapons (DEW) because atmospheric density and ionization must be part of the calculus. (Nichols, et al., 2022) Orbits and their various altitudes are also discussed, along with their influence on delivery system selection based on the target's distance and orbital velocity. We will also cover the existence of space debris. This is a critical point because millions of pieces of space junk are traveling at thousands of miles per hour, and any collision, intentional or not, could destroy a multimillion-dollar asset. Post-review of satellite attrition methods; we will discuss hypersonic drones and how an orbital platform can be utilized as a launch point for Hypersonic Glide Vehicles (HGV), which could have devastating results due to the impact velocity that would be similar to a small meteorite, striking an object at 17-20,000 mph, resulting in the high-velocity impact that will pulverize its target. The chapter's goal is not to engage in the details surrounding the science of orbital velocity and the associated physics but on the importance, as they pertain to a military perspective on offensive and countermeasure considerations.

Overview of Satellite Technology

To take a quote from NASA, "A satellite is a moon, planet or machine that orbits a planet or star. " (NASA, 2015).

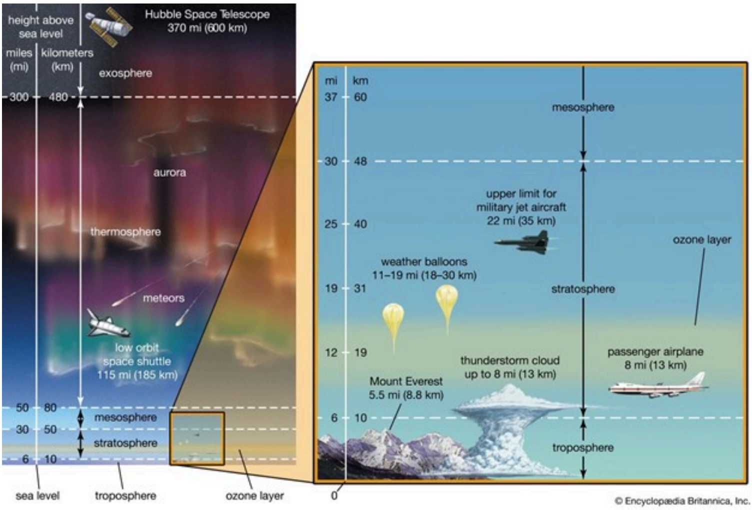
Because of their attitude, satellites are uniquely positioned to provide a beyond-the-horizon communications platform and a Birdseye view of a vast surface area of the earth. These capabilities offer a tactical advantage to anyone with access to such technology. With this understanding, the then Union of Soviet Socialist Republic (USSR), now Russia, developed and launched the first artificial earth-orbiting satellite, Sputnik 1 (PS-1), in 1957. The US followed with secret satellite projects like CORONA, in which the NSA, CIA, and other intelligence agencies would use satellite technology to obtain intelligence on Soviet missile locations (Dickson, 2001).

From 1957 to now, the heavens have gone from 1 artificial satellite to approximately 4,852 as of 12/31/21, according to information collected from the UCSUSA satellite database (USCUSA, 2021). To obtain an appreciation for the material to follow, it is vital to understand the various layers of the atmosphere, types of orbits, and satellite tracks within those orbits. This will lay the foundation for presenting the effectiveness of multiple methods for satellite positioning and assaults.

Atmospheric layers

At first glance, one may be tempted to discount any practical impacts the layers may have on satellite offenses and defenses. Each layer will have impacting characteristics, for example. The troposphere and stratosphere are denser than the higher levels of the atmosphere. They will produce more drag and friction, producing surface heating of any fast-moving ground deployed defenses against a satellite or platform. A typical missile used in ICBM interception is the Raytheon RIM-161 SM-3, which travels at approximately 3 km/second or about 6,700 mph (Mostly Missile Defense, 2012). The X-15 only traveled at 4,520 mph and encountered an aerodynamic heating temperature of 1200 degrees Fahrenheit (Dryden Flight Research Center, n.d.). It should be noted that such temperatures will melt aluminum, magnesium, zinc, and lead. At higher layers, reduced atmospheric pressure will determine the propulsion system and the need to account for the increased solar and cosmic radio interference. The increased distance of various orbits increases projectile travel time and targeting complexities. For example, many satellites are between 100 and 22,000 miles from the earth's surface. Additional travel time will allow the target satellite's nation(s) extra time to execute their OODA (Observe, Orient, Decide, Act) loop to engage countermeasures.

Figure 2-1 Common layers of the Earth's atmosphere


height above sea level
miles (mi)
kilometers (km)
Hubble Space Telescope 370 mi (600 km)
exosphere
300
480
aurora
thermosphere
meteors
low orbit space shuttle 115 mi (185 km)
50
80
mesosphere
30
50
stratosphere
6
10
sea level
troposphere
ozone layer
mi
km
37
60
mesosphere
30
48
upper limit for military jet aircraft 22 mi (35 km)
25
40
ozone layer
weather balloons 11–19 mi (18–30 km)
19
31
stratosphere
12
19
thunderstorm cloud up to 8 mi (13 km)
passenger airplane 8 mi (13 km)
Mount Everest 5.5 mi (8.8 km)
6
10
troposphere
0
© Encyclopædia Britannica, Inc.

Note: Relative activities occur at various atmospheric layers (Britannica, n.d.)

Source: *https://cdn.britannica.com/42/90442-050-6CB42E65/layers-atmosphere-Earth-phenomena-heights.jpg*

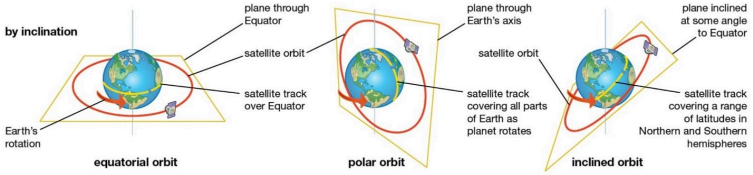
Types and Shapes of Orbits

As with the previous topic on atmospheric layers, the type of orbit a satellite is in will significantly contribute to the countermeasures or counter-countermeasures employed. The following are critical concepts that will be understood and considered.

As previously stated, this part of the chapter does not perform a deep dive into the mathematics of orbital velocities or the other aspects of orbital mechanics. This will be further discussed in the following chapter(s). However, it is essential to understand that each orbit can have a specific shape and distance. The one selected will vary based on its intended operation/mission and acceptance of that selection's associated benefits and risks.

Inclination: Orbital inclination is identified as the amount of angle or tilt. In the case of a satellite orbiting the earth, that angle is referenced as the angle between the satellite's orbit and the planet's equator. Generally, such orbits are referenced as near equatorial, polar, or inclined.

Figure 2-2 Orbital Inclination

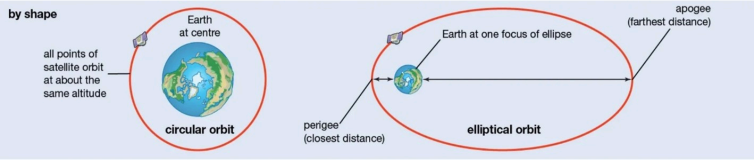

by inclination
plane through Equator
satellite orbit
satellite track over Equator
Earth's rotation
equatorial orbit
plane through Earth's axis
satellite orbit
satellite track covering all parts of Earth as planet rotates
polar orbit
plane inclined at some angle to Equator
satellite track covering a range of latitudes in Northern and Southern hemispheres
inclined orbit

Note: The same concept applies to retro rotation, which is the satellite rotating in the reverse direction of the planet.

Source: https://www.britannica.com/science/spaceflight

Shape: There are two general orbital shapes, circular and elliptical. Circular orbits are a fixed distance from the earth and are designated as LEO, MEO, and HEO, which are described in detail in the next section. This orbit is usually performed for geosynchronous orbits in which the satellite maintains a fixed earth position. The other orbital shape is elliptical and is defined by two different points regarding the planet being orbited. The closest point is the perigee, and the furthest is the apogee, which will play a role in any attack or asset protection determinations.

Figure 2-3 Orbital Shape


by shape
Earth at centre
all points of satellite orbit at about the same altitude
circular orbit
Earth at one focus of ellipse
apogee (farthest distance)
perigee (closest distance)
elliptical orbit

Source: https://www.britannica.com/science/spaceflight

Orbits by Attitude

Talk about the types of orbits and the significance of each. Also, how this aligns with the orbital inclination and shapes:

LEO or Low-Earth Orbit satellites can employ an elliptical or circular orbital shape, as illustrated in Figure 2-3. LEO orbits are mainly in the altitude range of 155 to 1243 miles (250–2000 km). Satellites in this orbit class complete an earth orbit in approximately 84-127 minutes, depending on the altitude. This low altitude requires a faster orbital speed to maintain the balance between centrifugal force and gravity, which is approximately 17,500 mph or 7.8 km/s. At this speed, the International Space Station (ISS) will circle the earth

16 times daily at 90 minutes intervals (European Space Agency, n.d.). Examples of satellites in this orbit would be Remote Sensing Satellites such as weather, terrestrial surface mapping, climate change, oceanographic observation/ monitoring, spy/surveillance, and Hubble and the International Space Station.

Table 2-1 A*dvantages and disadvantages for satellites in GEO orbit*

The following table list some advantages and disadvantages for satellites in GEO orbit:

Advantages:

1. Small, less expensive launch vehicles can push the satellite into an LEO orbit.

2. The quicker orbit speed makes for a faster moving target in the event Anti-Satellite Weapons (ASW) were deployed against it. For perspective, a typical 55 grain NATO 5.56x45mm bullet, used in AR15 assault rifles, travels at approximately 3,250 ft/s (991 m/s) (Wikipedia, 2001) or a little over 3,500 mph compared to a satellite traveling at about 17,500 mph.
3. The lower orbit allows for better clarity for imaging and surveillance
4. Lower proximity to the surface reduces communications latency between the satellite and ground station, which will be in the low range of 5 to 10 msec.
5. Low-earth orbits (LEOs) can also be effectively used for satellite communications. LEO orbits range from 250 to 1000 miles, and signal time delays are only 5 to 10 msec. This advantage also includes reduced power consumption for the communication links, with an average power usage of .5W (Perez, 1988).

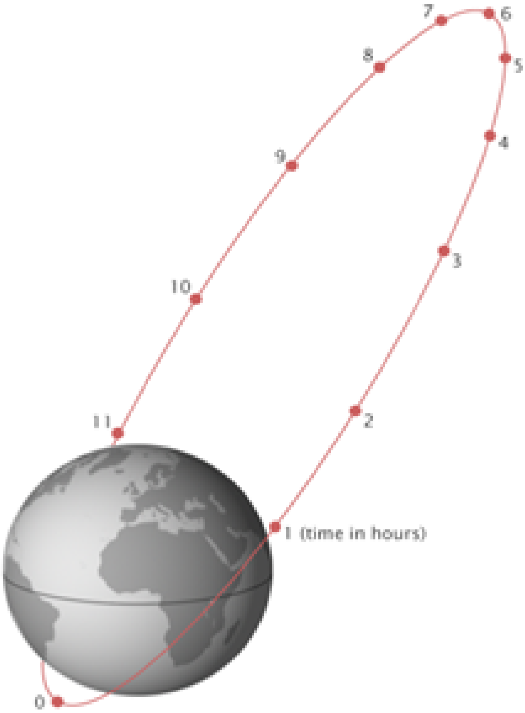
Disadvantages:

1. The low but fast orbit limits the satellite to a small field of view compared to other orbits. It has a short duration over any given geographical location of about 5-20 minutes per orbit. Requires a network or constellation of satellites working together to provide adequate coverage. Also, the ground station and satellite must use highly directional antennas to conserve power consumption.

2. The LEO orbit has become congested with space debris from other satellites and rocket boosters from previous launches, which can result in high-velocity impacts.
3. The low orbit would make an ASW assault more feasible and allow multiple attack attempts since it will be more difficult for the protection agency to re-task the satellite to a safe position due to orbital congestion.
4. Due to orbital decay resulting from atmospheric drag, the satellites typically have a 7–10-year lifespan, although some were extended due to the refueling/repair work from various Space Suttle missions.

MEO or Medium Earth Orbit satellites operate in the boundary between 1,243 – 22,235 miles (2,000-35,768 km). Their orbital time can be between 2 hours at the lower altitudes and just under 24 hours at the higher altitudes, but in either case, the satellite will cross two points on the equator at the same time interval per orbit. Generally, t, the satellites employ a near-circular, semi-synchronous, low eccentricity orbit or use an elliptical pattern. A standard elliptical orbit is the Molniya orbit, a combination of a high inclination and high eccentricity. The Russians invented this orbit, which provides a wider viewing area and a more extended viewing period when approaching and leaving the apogee and moves quickly when approaching the perigee. These orbits usually contain satellites for GPS, navigation, communication (Sirius and XM radio), cellular, internet, and surveillance.

Figure 2-4 ***Molniya orbit***



Note: The Molniya orbit is a preferred method when observing areas of high latitudes and will spend approximately 2/3rd of its orbit over one hemisphere (NASA, 2009). There is *also a Tundra orbit which is well suited for communications satellites.*

Source: https://earthobservatory.nasa.gov/features/OrbitsCatalog

Table 2-2 *Advantages and disadvantages for satellites in LEO orbit*

The following table list some advantages and disadvantages for satellites in LEO orbit:

Advantages:	
	1. Launched into higher altitudes than LEO satellites and are subject to less orbit decay. This typically increases their expected lifespan to approximately 10 – 15 years. 2. Have an improved communication time delay compared to higher orbit satellites (40 ms vs. 120 ms for GEO orbits) 3. Slower rotation and more time over viewing area and requiring fewer satellites in a constellation/network for global coverage.
Disadvantages:	
	1. Requires a more powerful launch vehicle to obtain higher orbit 2. Slower speed can make it a more assessable target for Anti-Satellite Weapons (ASW) systems. 3. Require a more robust power system for transmission.

Source: Information sourced from (RF Wireless World, n.d.)

GEO or Geosynchronous/Geostationary Earth Orbit is generally accepted to range from 22,236 – 26,199 miles (22,236 – 42,164 km). Their primary feature is their ability to remain over a geographic area due to their 24-hour orbital rotating of 23 hours, 56 minutes, and 4.1 seconds matching the earth's rotation. Maintaining the orbital speed and distance requires some station-keeping and, when retired, are placed in a higher orbit. Satellites generally found in this orbit are communications, meteorology, and navigation. Because of their extreme distance, it is possible to provide global coverage with as few as three satellites (Wikipedia, 2001). This is coveted international real estate since only a limited number of satellites can exist here due to spacing and RF interference requirements.

Table 2-3 A*dvantages and disadvantages for satellites in GEO orbit*

The following table list some advantages and disadvantages for satellites in GEO orbit:

Advantages:

1. They are less affected by atmospheric drag that results in orbit decay, extending their life expectancy by 15 years.

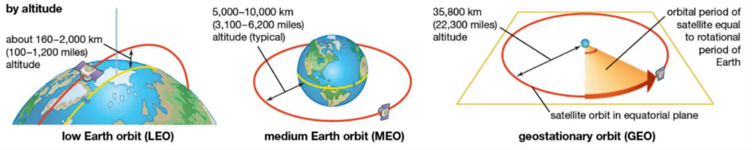
2. Excellent for TV and radio broadcasts and weather forecasting.
3. Ground stations do not need to hand off communications to other stations because they remain within line of sight; footprints can cover approximately 1/3 of the earth's surface.
4. High altitude has less debris and will take ASWs longer to get to.

Disadvantages:

1. Solar and lunar forces will cause satellite deviation from the planned orbit requiring the use of thrusters for adjustments.

2. Communication delays make real-time or interactive impractical.
3. Slower moving and stationary orbit make for a more vulnerable ASW target.
4. Expensive to maintain due to increased weight, need for more powerful transmitters, and fuel to maintain orbit.

Figure 2-5 Orbital Altitude

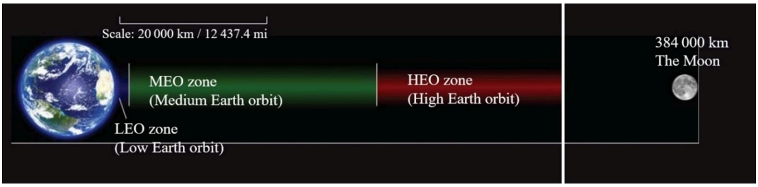


Note: The same concept applies to retro rotation, which is the satellite rotating in the reverse direction of the planet.

Source: *https://www.britannica.com/science/spaceflight*

HEO or High Earth Orbit and High Elliptical Orbit are essentially any orbits above 22,235 miles (35,768 km). Satellites in this zone will have orbital periods greater than 24 hours and appear to move backward or retrograde, although they are moving forward. Satellites in this orbit require huge boosters and usually require a transition orbit to obtain such altitudes. These devices are typically large and require significant power demands for signal transmission. Satellites in this orbit have been related to the military, deep space astronomy, nuclear monitoring/compliance, and deep space research.

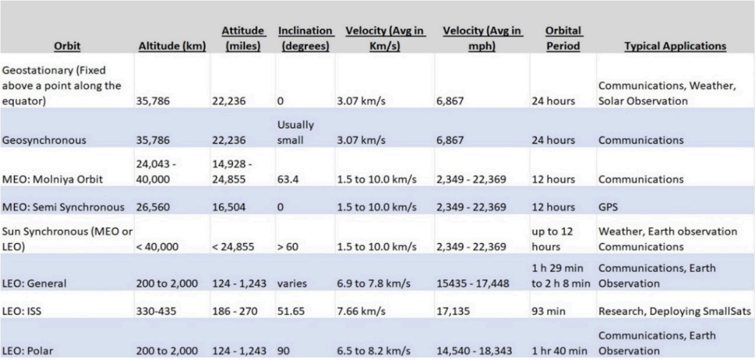
Figure 2-6 High Altitude Orbits



Note: The image is not to scale with HEO tapering off into space approximately halfway to the moon and is a modification of work from Mark Mercer.

Sourced: https://upload.wikimedia.org/wikipedia/commons/b/b8/Orbitalaltitudes.svgt

Table 2-4 Additional Orbital Information



Orbit	Altitude (km)	Attitude (miles)	Inclination (degrees)	Velocity (Avg in Km/s)	Velocity (Avg in mph)	Orbital Period	Typical Applications
Geostationary (Fixed above a point along the equator)	35,786	22,236	0	3.07 km/s	6,867	24 hours	Communications, Weather, Solar Observation
Geosynchronous	35,786	22,236	Usually small	3.07 km/s	6,867	24 hours	Communications
MEO: Molniya Orbit	24,043 - 40,000	14,928 - 24,855	63.4	1.5 to 10.0 km/s	2,349 - 22,369	12 hours	Communications
MEO: Semi Synchronous	26,560	16,504	0	1.5 to 10.0 km/s	2,349 - 22,369	12 hours	GPS
Sun Synchronous (MEO or LEO)	< 40,000	< 24,855	> 60	1.5 to 10.0 km/s	2,349 - 22,369	up to 12 hours	Weather, Earth observation Communications
LEO: General	200 to 2,000	124 - 1,243	varies	6.9 to 7.8 km/s	15435 - 17,448	1 h 29 min to 2 h 8 min	Communications, Earth Observation
LEO: ISS	330-435	186 - 270	51.65	7.66 km/s	17,135	93 min	Research, Deploying SmallSats
LEO: Polar	200 to 2,000	124 - 1,243	90	6.5 to 8.2 km/s	14,540 - 18,343	1 hr 40 min	Communications, Earth Observation

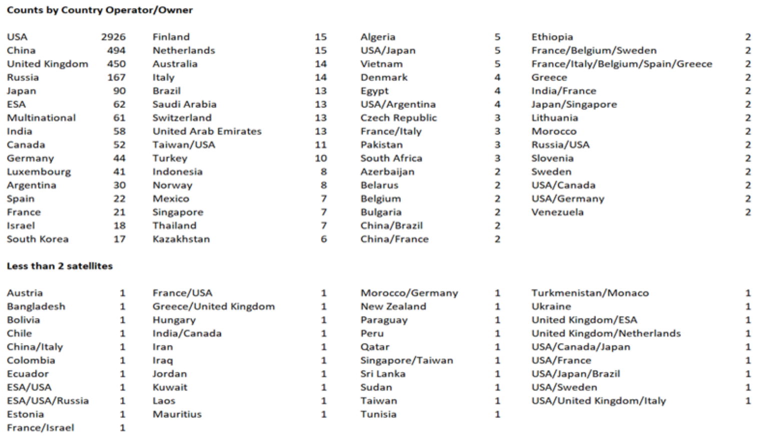
The table provides additional summary information on the previously described orbits.

Adapted from: https://newspaceglobal.com/operational-orbits-advantages-and-disadvantages

Orbital Congestion and Debris

Before discussing actual Anti-Satellite Weapons (AWS) and their systems, a final and critical topic is the vast number of objects that encircle the earth and who owns them. As stated at the beginning of the chapter, from 1957 to now, the heavens have gone from 1 artificial satellite to approximately 4,852 as of 12/31/21. This distribution of this number is illustrated in the following table.

Table 2-5 4,852 as of 12/31/21



Counts by Country Operator/Owner

USA	2926	Finland	15	Algeria	5	Ethiopia	2
China	494	Netherlands	15	USA/Japan	5	France/Belgium/Sweden	2
United Kingdom	450	Australia	14	Vietnam	5	France/Italy/Belgium/Spain/Greece	2
Russia	167	Italy	14	Denmark	4	Greece	2
Japan	90	Brazil	13	Egypt	4	India/France	2
ESA	62	Saudi Arabia	13	USA/Argentina	4	Japan/Singapore	2
Multinational	61	Switzerland	13	Czech Republic	3	Lithuania	2
India	58	United Arab Emirates	13	France/Italy	3	Morocco	2
Canada	52	Taiwan/USA	11	Pakistan	3	Russia/USA	2
Germany	44	Turkey	10	South Africa	3	Slovenia	2
Luxembourg	41	Indonesia	8	Azerbaijan	2	Sweden	2
Argentina	30	Norway	8	Belarus	2	USA/Canada	2
Spain	22	Mexico	7	Belgium	2	USA/Germany	2
France	21	Singapore	7	Bulgaria	2	Venezuela	2
Israel	18	Thailand	7	China/Brazil	2		
South Korea	17	Kazakhstan	6	China/France	2		

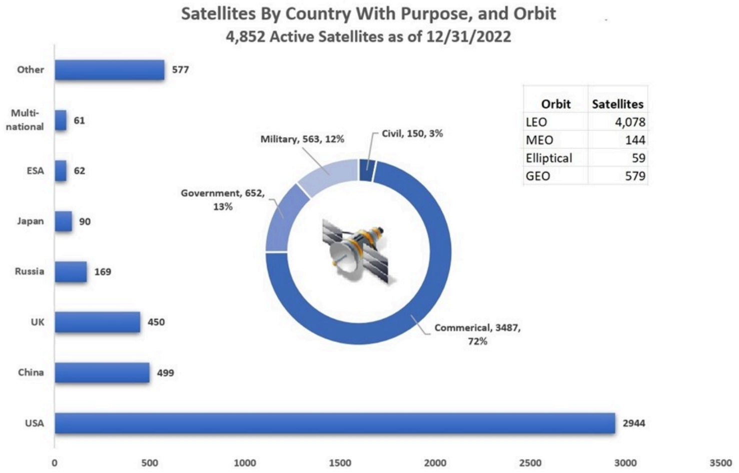
Less than 2 satellites

Austria	1	France/USA	1	Morocco/Germany	1	Turkmenistan/Monaco	1
Bangladesh	1	Greece/United Kingdom	1	New Zealand	1	Ukraine	1
Bolivia	1	Hungary	1	Paraguay	1	United Kingdom/ESA	1
Chile	1	India/Canada	1	Peru	1	United Kingdom/Netherlands	1
China/Italy	1	Iran	1	Qatar	1	USA/Canada/Japan	1
Colombia	1	Iraq	1	Singapore/Taiwan	1	USA/France	1
Ecuador	1	Jordan	1	Sri Lanka	1	USA/Japan/Brazil	1
ESA/USA	1	Kuwait	1	Sudan	1	USA/Sweden	1
ESA/USA/Russia	1	Laos	1	Taiwan	1	USA/United Kingdom/Italy	1
Estonia	1	Mauritius	1	Tunisia	1		
France/Israel	1						

Sourced from: https://www.ucsusa.org/media/11491

The location, identification/owner, and tracking of satellites and debris are essential to ensure the safe placement or movement of new or existing satellites and protect the space assets of allies. The below displays the number of satellites in space as of 12/31/22-That count has grown during this writing.

Figure 2-7 Satellite By Country with Purpose & Orbit



Orbit	Satellites
LEO	4,078
MEO	144
Elliptical	59
GEO	579

Note: This contains only known active satellites and does not account for any that may have been retired or space debris.

Adapted from: https://www.ucsusa.org/media/11491

Satellite image from: https://findicons.com/icon/28535/satellite#

The number of active satellites dwarfs the number of actual decommissioned satellites and other space debris currently in orbit. It is essential to determine whose and what objects are encircling the earth when discussing Anti-Satellite Weapons (AWS) systems and understand that space debris has accumulated over sixty decades of defuncted satellites, experiments, and components from launch vehicles. This issue is of such concern that the DoD and NASA work jointly using the Space Surveillance Network (SSN), optical telescopes, DebriSat, Haystack X-Band Radar, and Long

Duration Exposure Facility (LDEF) to track debris in the known orbital planes (NASA Orbital Debris Program Office, n.d.). Similarly, the European Space Agency, whose Space Debris Office in the European Space Operations Center (ESOC)is located in Darmstadt, Germany, also tracks an orbital collision risk assessment team. (European Space Agency, n.d.) It is important to note that contrary to popular belief, not all space debris is cataloged and tracked; statistical analysis and modeling are used for objects smaller than 10 centimeters or 4 inches (NASA, 2021). According to measurements from the ESA, as of July 11, 2022, the below satellite and space debris data has been observed:

Table 2-6 Space Satellite & Space Debris Data

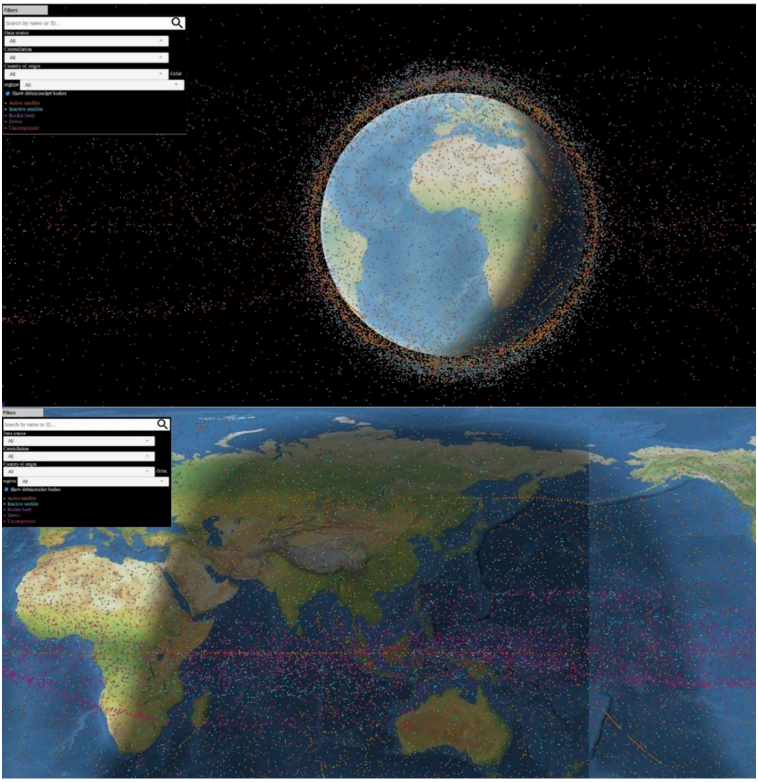
Activity/Event	Count
Satellite Data	
· Satellites placed in orbit via rocket launches	13,320
· Satellites in orbit	8,580
· Functioning satellites in orbit (maybe the end of life, out of fuel, or placed in graveyard orbit but electronics still working)	6,100
· Debris is regularly tracked and cataloged by SSN.	31,740
· Estimated events (explosions, collisions, etc.) resulting in fragmentation.	630
General Debris Data	
· Debris greater than 10cm (4 inches)	36,500
· Debris > 1cm (approx. size of #2 pencil) but less than 10 cm	1,000,000
· Debris > 1 mm but less than 1 cm	130,000,000

Sourced from: (European Space Agency, 2022)

As previously noted in the LEO, orbital speeds are very fast, and as an example, a NATO 5.56mm bullet travels at approximately 3,260 f/s or about one km/s. Debris from a satellite, including paint chips, can travel between 4-8 km/s or roughly 13,123-26,246 f/s. These velocities translate to small objects containing high amounts of kinetic energy, sufficient to destroy a functioning satellite on impact.

Figure 2-8 Partial view of satellites and space debris

in orbit from a global and continental view perspective



Filters

Search by name or ID...

Data source: All

Constellation: All

Country of origin: All

Orbit regime: All

☑ Show debris/rocket bodies

- Active satellite
- Inactive satellite
- Rocket body
- Debris
- Uncategorized

Filters

Search by name or ID...

Data source: All

Constellation: All

Country of origin: All

Orbit regime: All

☑ Show debris/rocket bodies

- Active satellite
- Inactive satellite
- Rocket body
- Debris
- Uncategorized

Note: Due to cropping, images do not capture full orbital tracks for outer orbits.

Source: Realtime satellite and debris tracking (AstriaGraph, 2022). https://astria.tacc.utexas.edu/AstriaGraph/

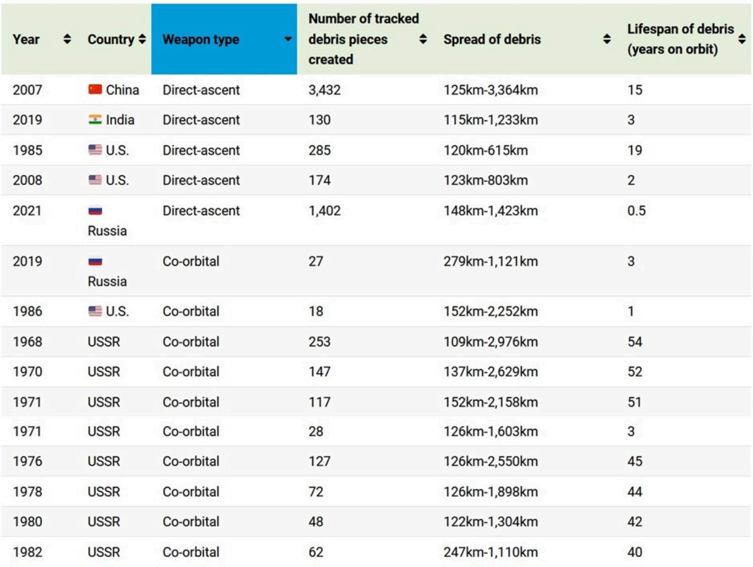
The weaponization of Space and Methods of Satellite Attrition

Due to the vastness of the topic and out of respect for chapter length, an in-depth review of ground-based Direct Energy Weapons (DEW) will not be explored at this time. However, it is one of the multiple methods of satellite eradication.

Of the many methods of obtaining kill proximity to a satellite, there are only a few principles, *Direct Accent* or Hit-to-Kill (DA-ASAT) and *Co-orbital (Co-ASAT)*. These two principles allow for deploying such methods as Direct Energy Weapons, Anti-satellite missiles, killer satellites, and the use of natural and artificial debris. The following will provide examples of direct and indirect attacks that could be employed to destroy a satellite or constellation of satellites. It is also critical to understand the existence of space debris caused by numerous ASAT tests executed since the 1960s and the role it can play in the intentional destruction of satellite assets.

Initially, weapons testing in space was conducted by the United States and Russia. This has since expanded to include China and India.

Table 2-7 Space Debris because of ASAT Tests

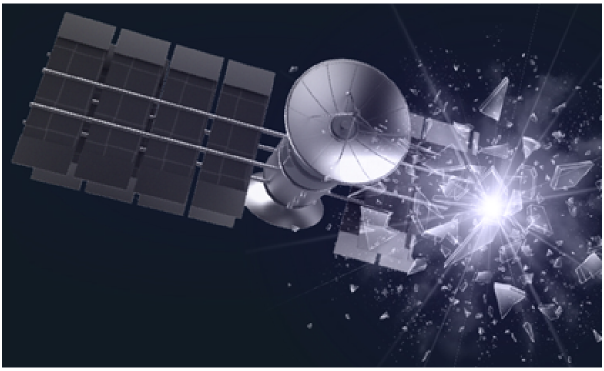


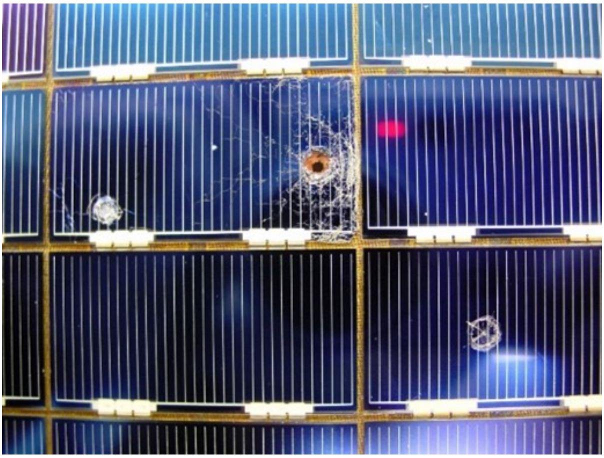
Year	Country	Weapon type	Number of tracked debris pieces created	Spread of debris	Lifespan of debris (years on orbit)
2007	China	Direct-ascent	3,432	125km-3,364km	15
2019	India	Direct-ascent	130	115km-1,233km	3
1985	U.S.	Direct-ascent	285	120km-615km	19
2008	U.S.	Direct-ascent	174	123km-803km	2
2021	Russia	Direct-ascent	1,402	148km-1,423km	0.5
2019	Russia	Co-orbital	27	279km-1,121km	3
1986	U.S.	Co-orbital	18	152km-2,252km	1
1968	USSR	Co-orbital	253	109km-2,976km	54
1970	USSR	Co-orbital	147	137km-2,629km	52
1971	USSR	Co-orbital	117	152km-2,158km	51
1971	USSR	Co-orbital	28	126km-1,603km	3
1976	USSR	Co-orbital	127	126km-2,550km	45
1978	USSR	Co-orbital	72	126km-1,898km	44
1980	USSR	Co-orbital	48	122km-1,304km	42
1982	USSR	Co-orbital	62	247km-1,110km	40

Sourced from: https://www.visualcapitalist.com/sp/anti-satellite-weapons/ (Bhutada & Smith, 2022)

Debris field disruption: Each orbital level has various amounts of debris. LEO is not only very saturated but also has the fastest traveling objects. A collision of any type will cause a cascade of collisions, also known as the Kessler Syndrome. In short, the concept is based on the collision of two or more objects. Although the physic associated with the laws of collisions and motion is outside the study of this text, it is essential to understand that objects traveling at such high velocities, even objects of negligible mass, will have high-energy impact collisions that will result in the creation of smaller objects moving in opposite directions with equal force. These smaller objects will collide with other debris, and the crashes will continue resulting in a debris storm. As previously discussed, the LEO orbit has numerous entities, including functional satellites and the ISS (International Space Station). There have been noted satellite collisions, with the first known collision occurring in 1991 when Russia's Cosmos 1934 was struck by a piece of Cosmos 926. Then, in 1996, France's Cerise satellite was hit by an Ariane 4 rocket fragment. In 2005 a US upper stage was hit by a piece of a Chinese rocket's third stage. In 2009 an Iridium satellite collided with Russia's Cosmos-2251", with devastating results (European Space Agency, n.d.).

Left Figure 2-9 / Hits on Satellites / Right Figure 2-10



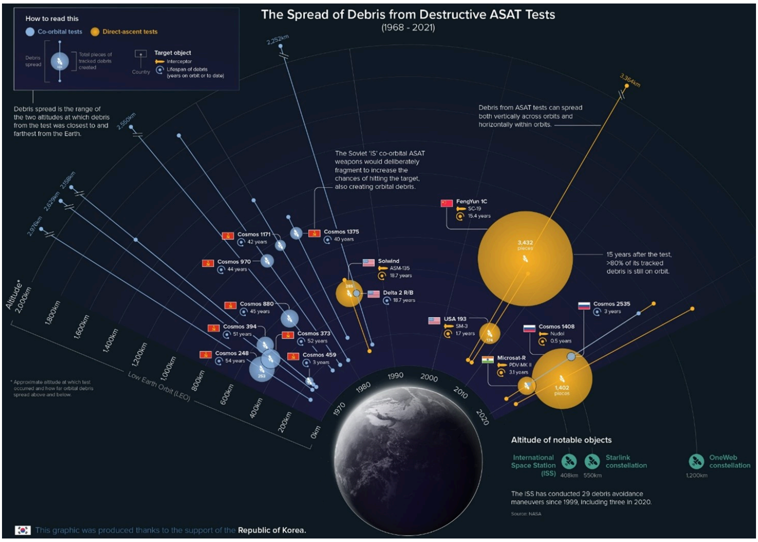


Right Source: Source: https://space-env.esa.int/madweb/

Left, altered from: https://www.visualcapitalist.com/sp/anti-satellite-weapons/ (Bhutada & Smith, 2022)

Debris weaponization needs to be a concern of any nation owning or operating a satellite. The importance of satellites and their ability to provide Realtime intelligence to military troops is well known. Some countries may not have the technical capabilities of their adversaries but wish to disrupt the ability to collect SATINT or disrupt their communications, command, and control capabilities to ground, naval, and aviation forces to level the playing field. Such a country may be short on resources to perform satellite management or even the technology to track and target an object in orbit. However, they may be able to use the debris field to destroy their opponent's space assets and cause the desired disruption. For example, North Korea has developed and test-launched the Hwasong-12 ballistic missile. This rocket is reported to have reached an altitude of 2,111 km or 1,311 miles. As previously studied, the LEO orbit is generally below 2,000 km. (Center for Strategic and International Studies, 2022). This attitude provides the capability to deliver a payload anywhere within the LEO and lower portions of the MEO orbit. As discussed, tracking, and striking a fast-moving object is a complex operation. However, delivery of a high explosive detonation does not contain near the level of sophistication but will render similar results. Such a scenario would begin a chain of reactions in which space debris would become an ever-growing cloud of shrapnel that would increase with the destruction of other objects in the ongoing collisions. This could eliminate observation, monitoring, and communications satellites for virtually every country. The increasing proliferation of surplus missile boosters makes such scenarios a viable threat vector.

Figure 2-11 Various ASTAT Tests and debris creation



The Spread of Debris from Destructive ASAT Tests
(1968 - 2021)

Debris spread is the range of the two altitudes at which debris from the test was closest to and farthest from the Earth.

The Soviet 'IS' co-orbital ASAT weapons would deliberately fragment to increase the chances of hitting the target, also creating orbital debris.

Debris from ASAT tests can spread both vertically across orbits and horizontally within orbits.

15 years after the test, >80% of its tracked debris is still on orbit.

* Approximate altitude at which test occurred and how far orbital debris spread above and below.

The ISS has conducted 29 debris avoidance maneuvers since 1999, including three in 2020.

Source: NASA

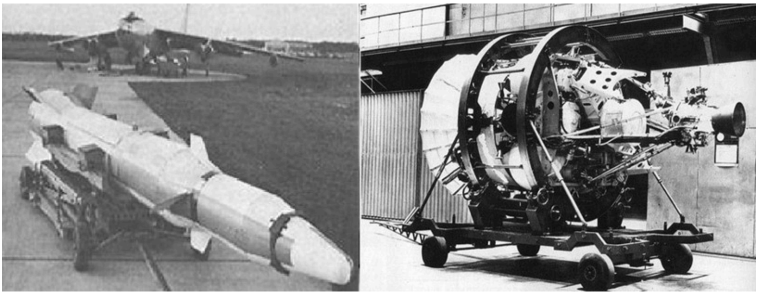
This graphic was produced thanks to the support of the Republic of Korea.

Altered from: https://www.visualcapitalist.com/sp/anti-satellite-weapons/ (Bhutada & Smith, 2022).

Surface/Air to Space missiles (DA-ASAT, non-DEW): After the successful launch of Sputnik, The US quickly became aware that Russia had established space superiorly and could spy on US installations. In addition, it was conceived that the Russians would begin to deploy nuclear projects into orbit, providing a first-strike capability. The initial US response in 1958 was developing and testing the ASAT weapon Bold Orion or (WS-199B), an air-launched missile. Testing and development continued until a successful near interception test was performed in LEO, where the missile came within 4 miles (6.4 km) of the Explorer 6 satellite in October of 1959 (Pike, 2016). This was countered by the

Russians in 1960 with a Co-Orbital device, “Dubbed Istrebitel Sputnikov (for the Satellite Destroyer) ...” (Zak, 2013).

Figure 2-12 First, ASAT weapons used by US and Russia



Right is the Bold Orion (WS-199B) 1959. Source: https://www.globalsecurity.org/space/systems/bold-orion.htm

left is the Istrebitel Sputnikov. 1960. Source: https: //www.jejaktapak.com/2015/09/06/istrebitel-sputnikov-pemburu-dan-pembunuh-satelit/

From the 1950s to the early 1970, the tactical approach of choice was the use of nuclear warheads and high-explosive warheads for the attrition of enemy satellite assets. In 1963, the US, Soviet Union, and Great Britain signed the Limited Nuclear Test Ban Treaty, understanding that any such explosion could cause collateral damage to both sides and allies. It should be noted that this treaty did not cover the use of other kinetic-type weapons. By the 1970s, tactics changed, and research began using Kinetic Kill weapons which would strike a target with extreme force. However, the force is such that targets are reduced to thousands of smaller pieces of debris. This was proven out in a few relatively recent events:

2007 China destroyed its old weather satellite (Keck, 2019).

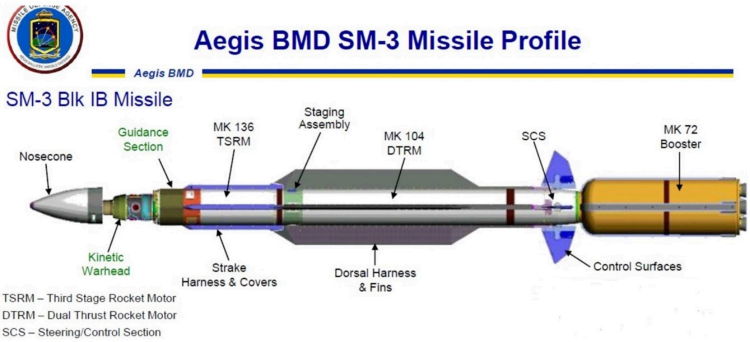
2008 US shoots down its spy satellite in low orbit (Oberg, 2021).

In 2021 Russia shot down its satellite (Litovkin, 2021).

Each of these satellites created large volumes of debris, with the 2021 event causing personnel on the ISS to shelter in place (Mogg, 2021) for multiple orbits until the debris field was no longer considered a danger. However, the debris will remain in orbit for decades, as outlined in table 2-7.

An overview of the Kinetic Kill Weapon/Warhead (KKW) can be illustrated by the SM-3 missile, which is a DA-ASAT hit-to-kill system that releases an independent 21-inch (530mm), Lightweight Exo-Atmospheric interceptor kill vehicle that will close on the target at approximately 10km/s (22,000 mph) (GAO, 2011).

Figure 2-13 AEGIS BMD SM-3 Missile Profile



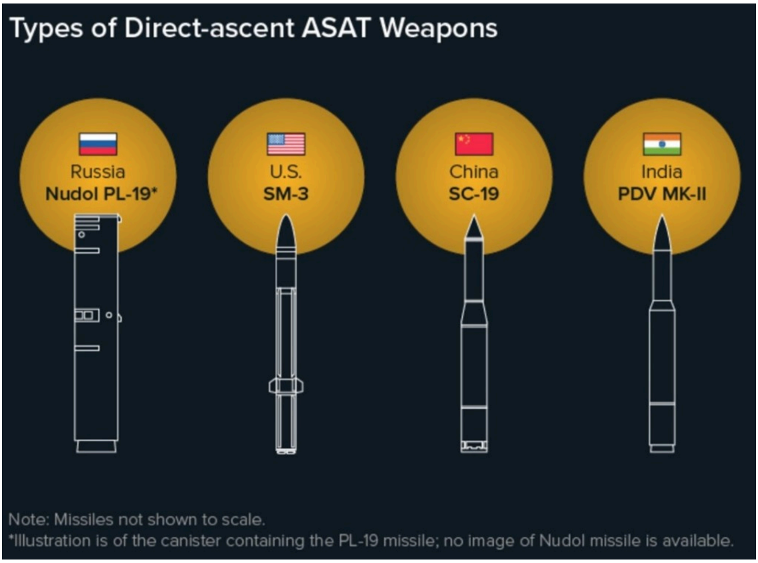
Adapted from: https://missiledefenseadvocacy.org/defense-systems/standard-missile-3-sm-3/

At this velocity, the impact would be equivalent to "…130 megajoules of kinetic energy, or the equivalent of a 10-ton truck traveling at 600 miles per hour." (Raytheon, 2007). For perspective, that would be roughly equivalent to a standard school bus traveling near the top speed of a 747 commercial jet crashing into an object. The result will be the pulverization of the target and the creation of additional high-velocity space debris.

DA-ASAT challenges include previously identified obstacles associated with LEO. First and foremost, the DA-ASAT will require a propulsion system with sufficient force to obtain attitude. Although some missiles can reach low to middle LEO, fewer can reach higher regions. If the attitude barrier is overcome, objects in this orbit travel at high velocities, making it very difficult to perform target identification, tracking, and acquisition. This will leave little time for developing a firing solution before the target passes from range. Although there are numerous claims of success, failed attempts are seldom discussed for obvious reasons. A consideration continuously mentioned is the ever-increasing space debris. Any DA-ASAT must navigate past debris traveling at velocities in the "high" hypersonic speed spectrum and have superior target identification facilities as part of its instrumentation.

It is important to note that the missile system illustrated is only one of many designs in which each company, country, and their associated engineers, will have varying methods. Still, the general concepts and principles will be virtually identical regardless of design differences.

Figure 2-14 Other types of ASATs and their countries

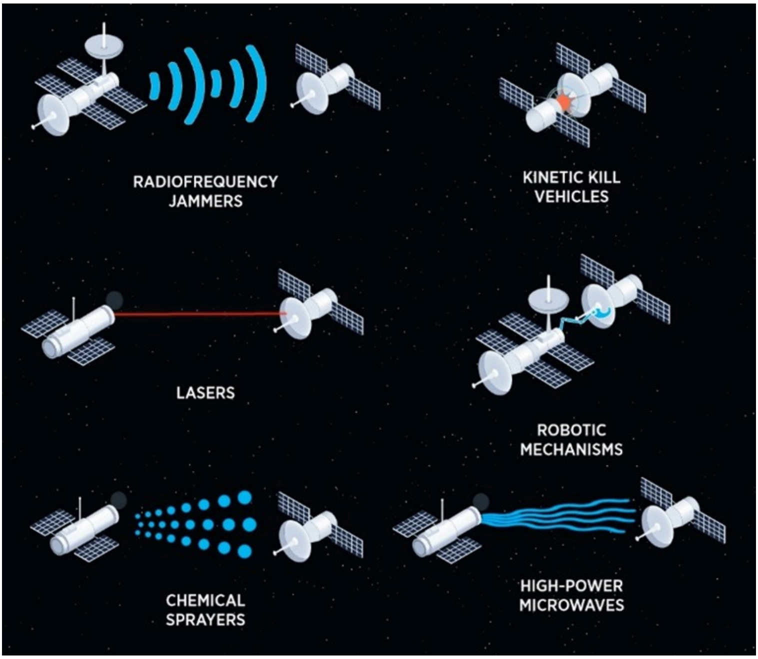

Types of Direct-ascent ASAT Weapons
Russia
Nudol PL-19*
U.S.
SM-3
China
SC-19
India
PDV MK-II
Note: Missiles not shown to scale.
*Illustration is of the canister containing the PL-19 missile; no image of Nudol missile is available.

Source: https://www.visualcapitalist.com/sp/anti-satellite-weapons/ (Bhutada & Smith, 2022)

Co-Orbital (CO-ASAT): These are weapon systems that are placed in orbit with the intent of maneuvering close to a target satellite from its orbital parking plane and can maneuver to the higher or lower plane of the target satellite and destroy it via various means. Such ASAT devices can have a dual objective. Being disguised as weather, communications, or having other non-imposing intentions, may allow them to remain in orbit without attracting attention to their disguised mission until called to action. This ASAT class could also chase down another orbital body over multiple orbits until it is close enough to perform its kill protocol. Such maneuvering has been observed by activities from Kosmos-2543 to match the orbit of Kosmos-2535 for a rendezvous and was able to change fore and aft orbital positions (Chabot, 2019). As referenced in table 2-7, Russia/USSR has performed nine co-orbital tests since 1982 and the US 1. Before 1982 there were 17 documented Russia/USSR co-orbital-related tests confirmed from 1963-1981 (The Space Review, n.d.). Due to state secrets, it is difficult to know how many co-orbital satellite activities related to eliminating adversary assets have occurred.

The following are examples of co-orbital actions that can occur; some have been demonstrated.

Figure 2-15 Co-orbital-based weapon types



Source: https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Challenges_Security_Space_2022-pdf

Direct collision or Kinetic Kill Vehicles are based on techniques discussed in our exploration of DA-ASAT and how high-velocity impacts can cause extensive damage to a targeted satellite. The concept is the same, except the kill vehicle is an orbital device that can transition orbital planes in pursuit of a target.

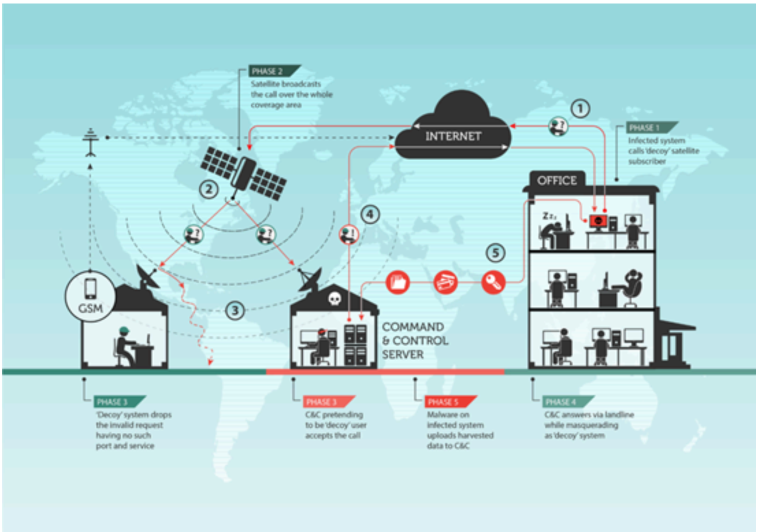
Radiofrequency Jammers would permit an attacking satellite to maneuver near another satellite and jam its sending and receiving singles. An attacking satellite could align its orbit close enough to the target satellite to perform cognitive jamming via spectrum sensing. This technology will allow the attacker to sense the transmit-receive frequencies used by the target and use a "detect and jam" strategy. Even as the target satellite attempts to perform anti-jamming mitigation, the attacking satellite could continue its spectrum analysis via techniques such as detection sliding energy window analysis. (Tianq, Pham, & Blasch, 2012) Jamming may only need to exist for a short period to cause a disruption, especially if the target is in LEO.

Microwave bombardment has become a feasible attack method for satellite-to-satellite conflicts, as proven with high-power microwave (HPM) experiments on electronic circuits using narrow-band and ultra-wide-band (UWB) pulsed radiation to damage the electronic circuitry of the target (SAE Media Group, 2008). A microwave-capable ASAT maneuvering near a target could emit microwaves creating an energy transference that would build up additional voltage within the target satellite. This would generate thousands of volts, causing the target's electronics conductors to build up voltage and heat, which would semiconductors, processors, and even melt critical components. Space research has proven this using Photovoltaic Radio-frequency Antenna Module (PRAM) technology. "PRAM converts sunlight for microwave power transmission." (Trevithick, 2020) to provide power.

Cyber-attacks are not limited to terrestrial devices.

(Nichols, et al., 2022) Satellites will have similar vulnerabilities. Satellites receive communication from earth stations and, in many cases, multiple earth stations, all of which will require authentication. This implies the need for a communication and security protocol to serve the receival of the request, acknowledgment, and handshaking necessary for passing credentials. This can be subject to a DoS (Denial of Service) attack where the satellite could become overwhelmed attempting to service the request and unable to authenticate with the legitimate source, affecting its ability to receive instructions from its base. Depending on the orbit and satellite's velocity, it may pass its communication window with a particular ground station and must proceed to the next. As discussed in orbit advantages and disadvantages, LEO orbits require less power to communicate with the ground and usually have smaller antennas and less powerful transmitters. Another satellite or constellation of satellites in orbit could potentially provide more focused signaling and begin an attack before the target satellite enters its communication window with the ground and cause disruption. This is one of the numerous possible cyber-attacks that could be performed. A similar cyber situation occurred where hackers acquired control of a decommissioned satellite and broadcasted their conference via the Anik F1R satellite (Paganini, 2022).

Figure 2-16 Illustration of a practical satellite hack scenario


PHASE 2
Satellite broadcasts the call over the whole coverage area
INTERNET
1
PHASE 1
Infected system calls 'decoy' satellite subscriber
OFFICE
2
4
5
GSM
3
COMMAND & CONTROL SERVER
PHASE 3
'Decoy' system drops the invalid request having no such port and service
PHASE 3
C&C pretending to be 'decoy' user accepts the call
PHASE 5
Malware on infected system uploads harvested data to C&C
PHASE 4
C&C answers via landline while masquerading as 'decoy' system

Source: Arstechnica.com via https://universemagazine.com/en/how-to-destroy-a-satellite-without-firing-a-single-shot/

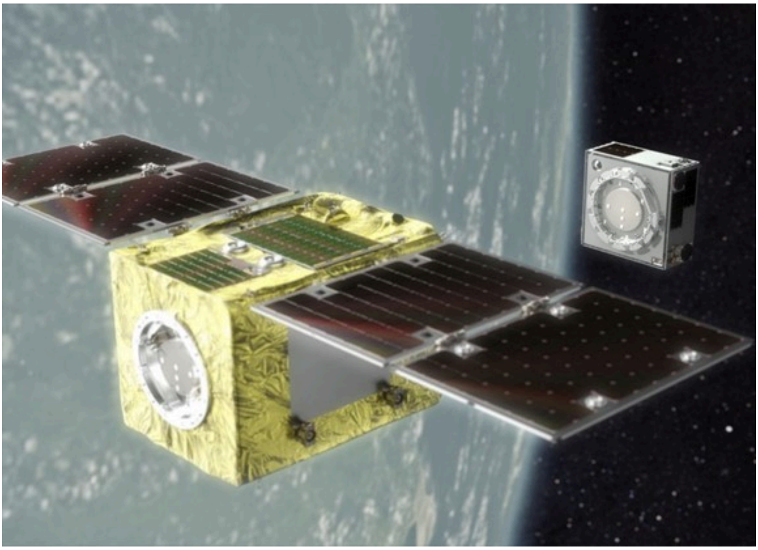
Laser weaponry for the use of co-orbiting attack satellites, lasers may not be a practical solution at this point due to the amount of power necessary to burn through the materials of a target satellite effectively. However, much work is underway to create more powerful lasers that require less power consumption. It should also be noted that additional energy would not be lost due to distance spreading, atmospheric ionization, atmospheric dispersion, and refraction as a ground-to-space attack. However, the technology does exist to use laser light to blind a target. This could be useful in anti-surveillance and detection, especially in the detection of hypersonic missile launches, which have a less pronounced launch signature than the standard ICBM.

Chemical sprayers would be a more insidious method of attack where the target would be sprayed with a chemical agent that would cause corrosion of the satellite surface and eventually compromise the system, which is already under stress due to thermal changes and forces associated with high-velocity travel. "Thermal stresses occur in the LEO orbit on the outer surface of satellites due to periodic in and out of the sunshade during orbiting. At LEO, this happens every 90 minutes and is roughly +100°C to -100°C. This temperature change causes thermal stresses in materials, and the difference in CTE will cause spalling of the oxide layer present on metal surfaces and results in constantly exposing fresh material to the atomic oxygen environment." (European Space Agency, n.d.). Such a dispersal of corrosive materials could reduce the efficiency of solar panels and their components and eventually comprise the structural integrity of the satellite.

Satellite robotic mechanisms have advanced exponentially over the past decade with the advancement of cube satellites, cheaper transport, improved robotic arm, camera systems, faster computing power, advanced software for accurate target identification and acquisition, and improved autonomous response. These improvements are now enabling devices to intercept and capture fast-moving objects. Recently, the US, England, and China have embarked on several experiments testing this technology under the guise of space debris removal to clean up the lower orbits. These countries have performed technological demonstrations giving each other weighty reasons for concern because the same technology used for debris removal can do the same to opposition assets. The following are known efforts that reflect the technology being tested.

1. In March 2021, a Japanese firm Astroscale Holdings Inc. launched a test mission with two satellites, "…a servicer designed to safely remove debris from orbit and a client satellite that serves as a piece of replica debris… this pioneering mission to demonstrate the technologies and capabilities necessary for debris capture and removal. The servicer satellite will release and dock magnetically with the client satellite in the first three complex demonstrations. Following this demonstration of non-tumbling capture, ELSA-d will perform two additional demonstrations: one to capture the client while it is tumbling, and one to lose deliberately, re-locate, approach, and re-capture the client from far-range." (Howlett, 2021), intending to pull it to a lower altitude where it will burn up in the atmosphere.

Figure 2-17 ***Image of Astroscale's ELSA-d with the "chaser" and "target" vehicle***



Source: https://astroscale.com/astroscale-statement-on-our-elsa-d-demonstration/

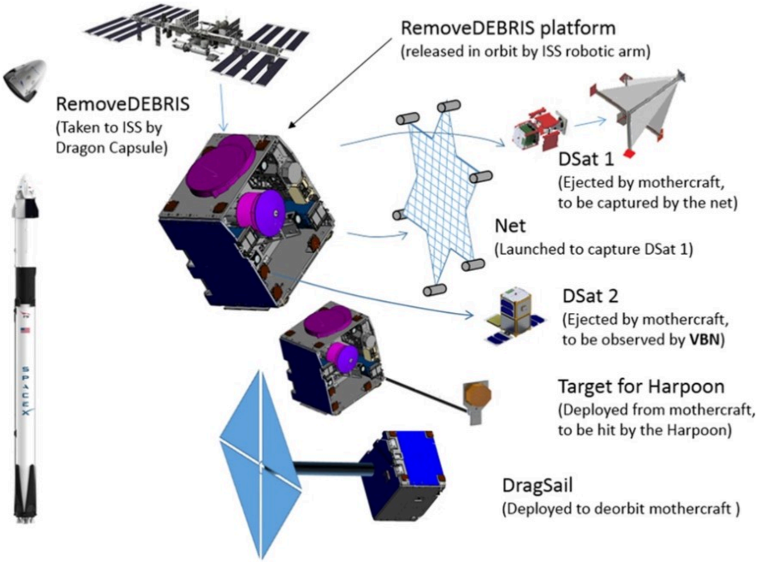
1. On January 2022, China's Shijian-21 (SJ-21) satellite was observed leaving its orbit and approaching the DeiDou-2 G2- It was later observed attaching to the G2 and throwing it into what is known as a "graveyard" orbit, where dysfunctional satellites are typically relocated, except under their power, to be retired. After performing this act, the SJ-21 returned to its regular GEO orbit. There are concerns that this was not only a test to remove debris but also to demonstrate the ability to push a satellite into an unwanted atmospheric re-entry (Hitchens, 2022).
2. "RemoveDebris" is a European consortium satellite

operated by Surrey Satellite Technology Ltd. Launched in April 2018, its mission was to:

- Flight a capturable object.
- Track and capture with net technology.
- Test a VBN LiDAR camera system for ranging.
- Perform accuracy tests for harpoon capture.
- Drag sail deployment for expedited orbit decay.

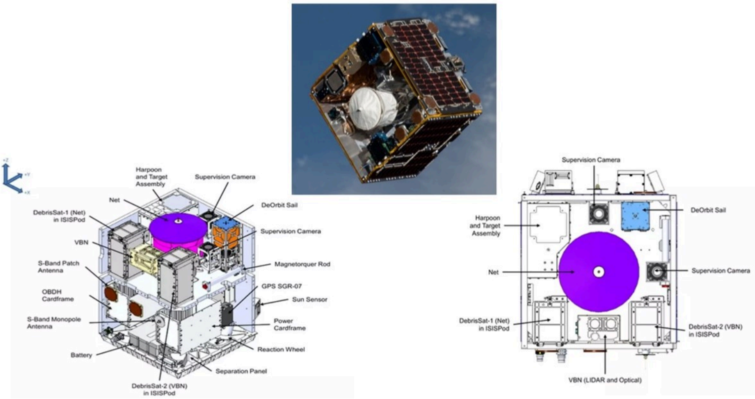
The mission accomplished its stated objectives (Aglietti, et al., 2019).

Figure 2-18 Visual of the mission profile for the RemoveDebris mission



Source: https://www.cambridge.org/core/journals/aeronautical-journal/article/removedebris-an-inorbit-demonstration-of-technologies-for-the-removal-of-space-debris/88B966915E7A3BD6F0B047A38FF713D2

Figure 2-19 Photo and cutaway views of the RemoveDebris cube satellite



Top image source: https://www.nasa.gov/mission_pages/station/research/experiments/explorer/Investigation.html#id=7350

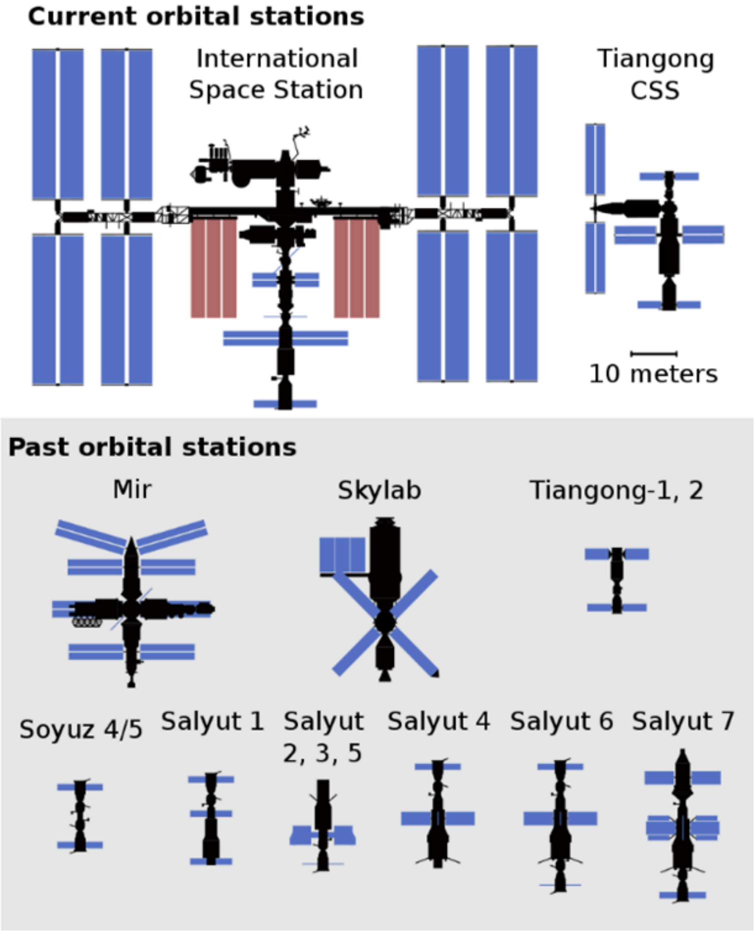
Bottom images source: https://www.surrey.ac.uk/surrey-space-centre/missions/removedebris

Of the many ASAT technologies being explored, there seems to be a trend towards solutions that would minimize collateral damage. Other than Kinetic Kill Weapons, the other co-orbital methods target a specific asset and do not disturb the orbiting debris field, which could also impose uncontrolled collateral damage on the attacking nations' assets.

Orbiting Hypersonic Missile Platforms

In addition to weather, communication, and spy satellites, there are orbiting platforms. The diagram below identifies 15 different platforms across 11 different types.

Figure 2-20 Sample of current and past orbital platforms



Source: https://upload.wikimedia.org/wikipedia/commons/thumb/7/77/Space_station_size_comparison.svg/836px-Space_station_size_comparison.svg.png

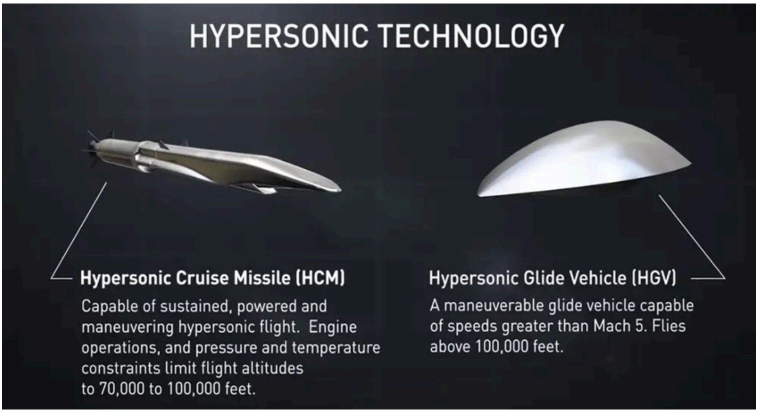
In 1963, 112 countries signed the Outer Space Treaty, which essentially bands the use of nuclear weapons in space. "Key provisions of the Outer Space Treaty include prohibiting nuclear weapons in space; limiting the use of the Moon and all other celestial bodies to peaceful purposes; establishing that space shall be freely explored and used by all nations; and precluding any country from claiming sovereignty over outer space or any celestial body. Although it forbids establishing military bases, testing weapons, and conducting military maneuvers on celestial bodies, the treaty does not expressly ban all military activities in space, nor the establishment of military space forces or the placement of conventional weapons in space." (Wikipedia, 2003). The specific declaration against nuclear weapons has left the door open for other possible systems, such as the launching of Kinetic Energy systems that do not need a nuclear warhead since their hypersonic velocities will produce devastating results by releasing the equivalent of kilotons of TNT (depending on weight, density, and final impact speed).

A known weapons platform that has been part of the escalating arms race has been the development of hypersonic weapons. A quick recap from book 6, these are vehicles traveling at speeds greater than Mach 5 (>3,806 mph) and attitudes below 90K (295,276 ft). Most objects in LEO orbit travel at velocities of 17,500 mph, and these speeds are known as high-hypersonic, ranging from Mach 10-25. Some Apollo Command Modules (CM) were recorded traveling at reentry velocities at Mach 36 (Smithsonian National Air and Space Museum, n.d.).

In general, there are two types or classes of Hypersonic

Missiles. The first being of the Cruise Missile type also referred to as Hypersonic Cruise Missile (HCM), which maintains speed via a SCRAM propulsion system, and the Hypersonic Glide Vehicle (HGV), which uses the forces of gravity and aerial dynamics to obtain its speed and stability.

Figure 2-21 Categories of Hypersonic missiles

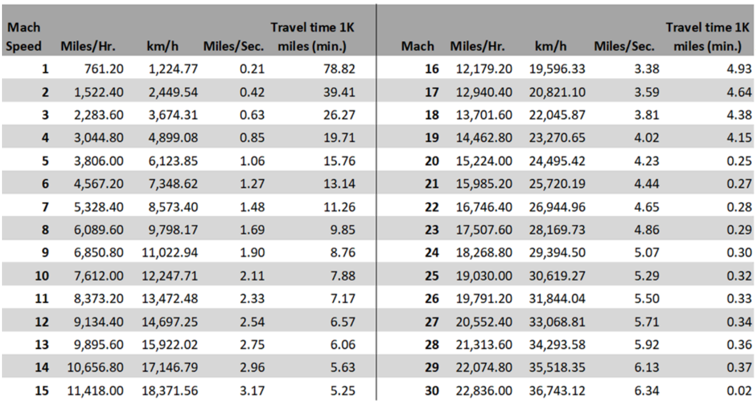

HYPERSONIC TECHNOLOGY
Hypersonic Cruise Missile (HCM)
Capable of sustained, powered and maneuvering hypersonic flight. Engine operations, and pressure and temperature constraints limit flight altitudes to 70,000 to 100,000 feet.
Hypersonic Glide Vehicle (HGV)
A maneuverable glide vehicle capable of speeds greater than Mach 5. Flies above 100,000 feet.

Source: The RAND Corporation (Speier, Nacouzi, Lee, & Moore, 2017)

The focus of this topic will be on the HGV and how it would be applied as a space-based attack vector.

Currently, there are limited ways to detect the launch or deployment of hypersonic missiles. The standard defense strategy, since the cold war era, has focused on detecting ICBM launches and interception. Hypersonic technology has become a game changer in the OODA-loop decision strategy process of Observe, Orient, Decide and Act (Devost & Courley, 2022). The process is impacted because the observation cycle is delayed, which is the start of the process. It should be noted that most early warning technology is optimized to the infrared signature of an ICBM surface or naval launch. This reduction in identification then compresses the time available for the other processes, including the ability to orient. The decrease further shortens the time the under-siege entity needs to act because the devices are so fast. For example, if we were to use the below table, extracted from Chapter 12 of Book 6 on Hypersonic weapons,

Table 2-8 Speed, time, and distance comparisons at various Mach speeds from 1-30 and times to cover 1000 miles



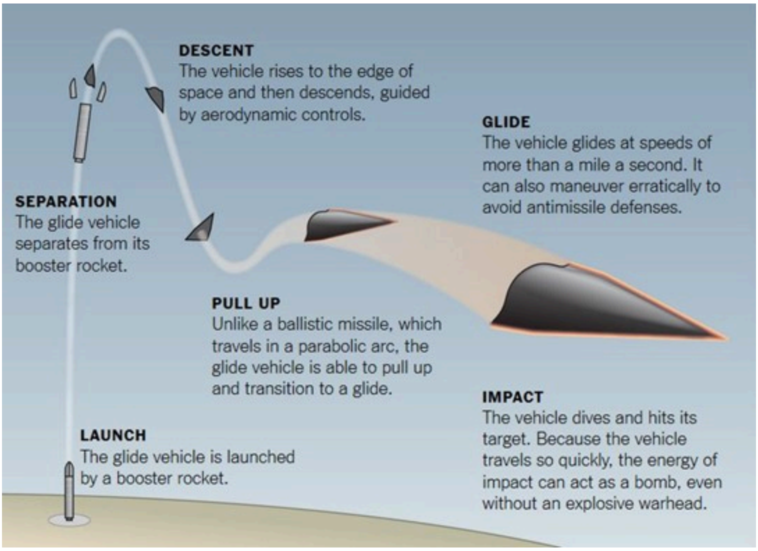
Mach				Travel time 1K					Travel time 1K
Speed	Miles/Hr.	km/h	Miles/Sec.	miles (min.)	Mach	Miles/Hr.	km/h	Miles/Sec.	miles (min.)
1	761.20	1,224.77	0.21	78.82	16	12,179.20	19,596.33	3.38	4.93
2	1,522.40	2,449.54	0.42	39.41	17	12,940.40	20,821.10	3.59	4.64
3	2,283.60	3,674.31	0.63	26.27	18	13,701.60	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	0.25
6	4,567.20	7,348.62	1.27	13.14	21	15,985.20	25,720.19	4.44	0.27
7	5,328.40	8,573.40	1.48	11.26	22	16,746.40	26,944.96	4.65	0.28
8	6,089.60	9,798.17	1.69	9.85	23	17,507.60	28,169.73	4.86	0.29
9	6,850.80	11,022.94	1.90	8.76	24	18,268.80	29,394.50	5.07	0.30
10	7,612.00	12,247.71	2.11	7.88	25	19,030.00	30,619.27	5.29	0.32
11	8,373.20	13,472.48	2.33	7.17	26	19,791.20	31,844.04	5.50	0.33
12	9,134.40	14,697.25	2.54	6.57	27	20,552.40	33,068.81	5.71	0.34
13	9,895.60	15,922.02	2.75	6.06	28	21,313.60	34,293.58	5.92	0.36
14	10,656.80	17,146.79	2.96	5.63	29	22,074.80	35,518.35	6.13	0.37
15	11,418.00	18,371.56	3.17	5.25	30	22,836.00	36,743.12	6.34	0.02

Source: (Nichols, et al., 2022)

It indicates how fast such weapons can move. It is not impractical for an HGV to move around the upper atmosphere over Mach 23 and about the lower altitudes at Mach 10, which can cover 1000 miles in under eight minutes.

The trajectory of HGV may resemble the diagram in a typical launch-to-guide scenario.

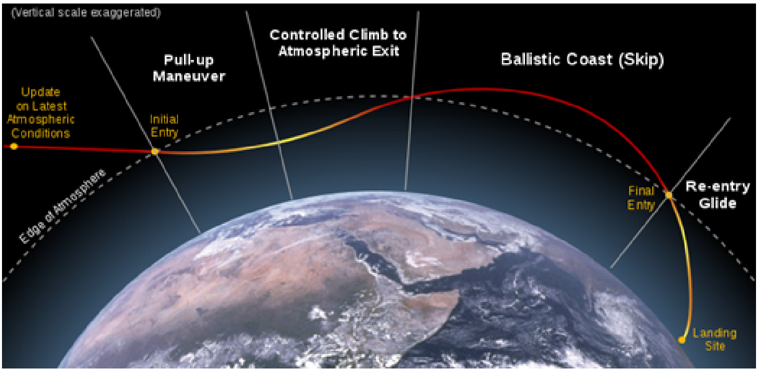
Figure 2-22 Launch – to – Glide Scenario


DESCENT
The vehicle rises to the edge of space and then descends, guided by aerodynamic controls.
GLIDE
The vehicle glides at speeds of more than a mile a second. It can also maneuver erratically to avoid antimissile defenses.
SEPARATION
The glide vehicle separates from its booster rocket.
PULL UP
Unlike a ballistic missile, which travels in a parabolic arc, the glide vehicle is able to pull up and transition to a glide.
IMPACT
The vehicle dives and hits its target. Because the vehicle travels so quickly, the energy of impact can act as a bomb, even without an explosive warhead.
LAUNCH
The glide vehicle is launched by a booster rocket.

Source: http://www.space4peace.org/articles/race_for_new_nukes.htm

In such a scenario, there is the ability to observe the infrared signature of the missile booster. In addition, the targets of the HGV will be less due to the height constraint of the booster. In a space-drop deployment scenario, the height restriction will be removed. Also, there will not be an infrared heat signature from the ground for observation satellites to detect and report and depending on the time of day; it may be challenging to obtain early confirmation that an HGV has been launched and started its re-entry trajectory, which may resemble an atmospheric skip as displayed in the below diagram.

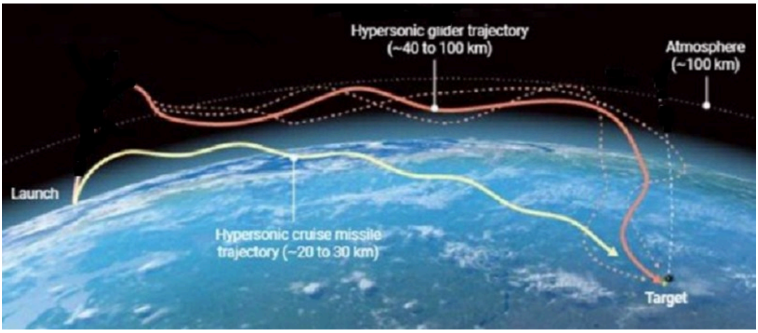
Figure 2-23 HGV is capable of skipping across the atmosphere to engage any target on the globe



Source: https://alphadefense.in/hypersonic-technology-and-its-future/

This will provide the HGV stealth because it can be dropped from a different global location and begin its targeting activities. Once entering the atmosphere, it will have the ability to maneuver, and because of its high altitude, it can confuse enemy tracking as to the actual target. Also, if the primary target is no longer available, multiple alternates can be selected. It should be noted that the options are fewer as the HGV gets lower. At a designated point, the HGV will drop on its target with maximum velocity to unleash as much kinetic energy and destruction as possible.

Figure 2-24 HGV will have more targeting options available


Hypersonic glider trajectory
(~40 to 100 km)
Atmosphere
(~100 km)
Launch
Hypersonic cruise missile
trajectory (~20 to 30 km)
Target

Source: Modified from https://alphadefense.in/hypersonic-technology-and-its-future/

Despite treaties and national agreements, the use of hypersonic weapons being launched from space is a consideration that must be pondered. The ability to have a first strike capability is too much of an enticement for nations that have demonstrated a tradition of breaking treaties or violating established norms and rules of engagement. Any country that would ignore such may do so at its demise.

Summary

In this chapter, we have studied atmospheric and orbital impacts associated with the advantages and disadvantages of orbiting or attacking a satellite. We have also briefly explored the history and evolution of Anti-Satellite (ASAT) technology and the earth-covering debris it has created. This reading has also covered various methods to kill satellites through intentional and unintentional means and the ongoing efforts of some countries to obtain and maintain space superiority. This chapter's concepts and principles should provide a foundation for the upcoming reading.

References

European Space Agency. (n.d.). *Low earth orbit*. Retrieved from ESA.int: https://www.esa.int/ESA_Multimedia/Images/2020/03/Low_Earth_orbit

Aglietti, S., Taylor, B., Fellowes, S., Ainley, S., Tye, D., Cox, C., & Steyn, W. H. (2019, November 26). *RemoveDEBRIS: An in-orbit demonstration of technologies for the removal of space debris*. Retrieved from cambridge.org: https://www.cambridge.org/core/journals/aeronautical-journal/article/removedebris-an-inorbit-demonstration-of-technologies-for-the-removal-of-space-debris/88B966915E7A3BD6F0B047A38FF713D2

AstriaGraph. (2022, August 14). *Realtime Satellite and Debris Map*. Retrieved August 14, 2022, from astria.tacc.utexas.edu: https://astria.tacc.utexas.edu/AstriaGraph/

Bhutada, G., & Smith, M. (2022, June 14). *Anti-Satellite Weapons: Threatening the Future of Space Activities*. Retrieved from visualcapitalist.com: https://www.visualcapitalist.com/sp/anti-satellite-weapons/

Britannica. (n.d.). *Atmosphere Vertical Structure.* Encyclopedia Britannica, Inc.

Center for Strategic and International Studies. (2022, May 20). *Hwasong-12 (KN-17).* Retrieved from missilethreat.csis.org: https://missilethreat.csis.org/missile/hwasong-12/

Chabot, A. (2019, November). *Soyuz-2-1v launches a possible military inspector satellite*. Retrieved from russianspacewab.com: http://www.russianspaceweb.com/cosmos-2542.html

Devost, M., & Courley, B. (2022, August 23). *The OODA loop explained: The real story about the ultimate model for decision-making in competitive environments*. Retrieved from oodaloop.com: https://www.oodaloop.com/the-ooda-loop-explained-the-real-story-about-the-ultimate-model-for-decision-making-in-competitive-environments/

Dickson, P. (2001). *Sputnik the shock of the century.* New York: Walker Publishing Company, Inc.

Dryden Flight Research Center. (n.d.). x-15 fact sheet. *Dryden Flight Research Center*.

European Space Agency. (2022, July 11). *Space debris by the numbers*. Retrieved July 14, 2022, from esa.int: https://www.esa.int/Space_Safety/Space_Debris/Space_debris_by_the_numbers

European Space Agency. (n.d.). *About the space debris office*.

Retrieved from esa.gov: https://www.esa.int/Space_Safety/Space_Debris/About_the_Space_Debris_Office

European Space Agency. (n.d.). *Corrosion in space*. Retrieved from esmat.esa.int: http://esmat.esa.int/Publications/Published_papers/Corrosion_in_Space

European Space Agency. (n.d.). *Space smash: Simulating when satellites collide*. Retrieved from esa.int: https://www.esa.int/Enabling_Support/Preparing_for_the_Future/Discovery_and_Preparation/Space_smash_simulating_when_satellites_collide

GAO. (2011, March). *Missile Defense: Actions Needed to Improve Transparency and Accountability*. Retrieved from goa.gov: https://www.gao.gov/assets/gao-11-372.pdf

Hitchens, T. (2022, January 27). *China's SJ-21 'tugs' dead satellite out of GEO belt: Trackers*. Retrieved from breakingdefense.com: https://breakingdefense.com/2022/01/chinas-sj-21-tugs-dead-satellite-out-of-geo-belt-trackers/

Howlett, A. (2021, June 2). *Astroscale celebrates successful launch of ELSA-D*. Retrieved from astroscale.com: https://astroscale.com/astroscale-celebrates-successful-launch-of-elsa-d/

Keck, Z. (2019, October 3). *How China could win a war against America: Kill the satellites*. Retrieved from nationalinterest.org: https://nationalinterest.org/blog/buzz/how-china-could-win-war-against-america-kill-satellites-85176#:~:text=China%20also%20used%20the%20S

C-19%20missile%20to%20destroy,tests%2C%20including%20ones%20in%202010%20and%20January%202013

Litovkin, N. (2021, November 16). *Why Russia shot down its old satellite and what weapon was used*. Retrieved from rbth.com: https://www.rbth.com/science-and-tech/334418-why-russia-shot-down-satellite

Mogg, T. (2021, November 16). *Space station emergency caused by cloud of satellite debris*. Retrieved from digitaltrends.com: https://www.digitaltrends.com/space/space-station-emergency-caused-by-cloud-of-satellite-debris/

Mostly Missile Defense. (2012). Aegis ballistic missile defense interceptors (SM-3, SM-2 block IV, and SM-6) (May 2, 2012). *Mostly Missile Defense*.

NASA. (2009, September 4). *Catalog of earth satellite orbits*. Retrieved from earthobservatory.nasa.gov: https://earthobservatory.nasa.gov/features/OrbitsCatalog

NASA. (2015). *What is a satellite?* NASA.

NASA. (2021, May 26). *Space Debris and Human Spacecraft*. Retrieved from nasa.gov: https://orbitaldebris.jsc.nasa.gov/measurements/

NASA Orbital Debris Program Office. (n.d.). *Debris Measurements*. Retrieved from orbitaldebris.jsc.nasa.gov: https://orbitaldebris.jsc.nasa.gov/measurements/

Nichols, R. K., Sincavage, S., Mumm, H. C., Lonstein, W., Carter, C., Hood, j. p., . . . Slofer, W. (2022, June). *DRONE DELIVERY OF CBNRECy – DEW WEAPONS Emerging Threats of Mini-Weapons of Mass Destruction and Disruption*

(WMDD). Retrieved from kstatelibraries.pressbooks.pu: https://kstatelibraries.pressbooks.pub/drone-delivery/

Oberg, J. (2021, July 27). *U.S. satellite Shootdown: The inside story*. Retrieved from sprectrum.ieee.org: https://spectrum.ieee.org/us-satellite-shootdown-the-inside-story

Paganini, P. (2022, August 21). *White hat hackers broadcasted talks and hacker movies through a decommissioned satellite*. Retrieved from securityaffairs.co: https://securityaffairs.co/wordpress/134637/hacking/hackers-take-control-decommissioned-satellite.html

Perez, R. (1988). *Wireless communications design handbook: Terrestrial and mobile interference: Aspects of noise, interference, and environmental concerns.* Cambridge: Elsevier.

Pike, J. (2016). *Bold Orion weapons system 199 (WS-199B)*. Retrieved from globalsecurity.org: https://www.globalsecurity.org/space/systems/bold-orion.htm

Raytheon. (2007). *Standard Missile-3*. Retrieved from raytheon.com: http://www.raytheon.com/products/stellent/groups/public/documents/content/cms01_055769.pdf

RF Wireless World. (n.d.). *Advantages of MEO orbit | disadvantages of MEO orbit*. Retrieved from rfwireless-world.com: https://www.rfwireless-world.com/Terminology/Advantages-and-Disadvantages-of-MEO-orbit.html

SAE Media Group. (2008, August 1). *Effects of high-power microwave pulses on electronic systems*. Retrieved from aerodefensetech.com: https://www.aerodefensetech.com/component/content/article/adt/tech-briefs/electronics-and-computers/4871

Smithsonian National Air and Space Museum. (n.d.). *Hypersonic flight*. Retrieved Aug 26, 2022, from https://airandspace.si.edu/stories/editorial/hypersonic-flight

Speier, R. H., Nacouzi, G., Lee, C., & Moore, R. M. (2017). *Hypersonic Missile Nonproliferation Hindering the Spread of a New Class of Weapons*. Retrieved August 28, 3019, from rand.org: https://www.rand.org/pubs/research_reports/RR2137.html

The Space Review. (n.d.). *Through a glass, darkly: Chinese, American, and Russian anti-satellite testing in space*. Retrieved from thespacereview.com: https://www.thespacereview.com/article/2473/2

Tianq, X., Pham, K. D., & Blasch, E. (2012, May). *Jamming/Anti-jamming Game with a Cognitive Jammer in Space Communication*. Retrieved from researchgate.net: https://www.researchgate.net/publication/258716106_JammingAnti-jamming_Game_with_a_Cognitive_Jammer_in_Space_Communication#:~:text=The%20cognitive%20jammer%20is%20assumed%20to%20have%20powerful,transmitter%20to%20the%20receiver%20over%20the%20communicatio

Trevithick, J. (2020, May 19). *X-37B's power beaming Payload a reminder of potential orbital microwave anti-satellite weapons*. Retrieved from thedrive.com:

https://www.thedrive.com/the-war-zone/33531/x-37bs-power-beaming-payload-a-reminder-of-potential-orbital-microwave-anti-satellite-weapons

USCUSA. (2021). *UCS satellite database.* Union of Concerned Scientists.

Wikipedia. (2001, October 1). *5.56×45mm NATO*. Retrieved from wikipedia.org: https://en.wikipedia.org/wiki/5.56%C3%9745mm_NATO#:~:text=In%20September%201963%2C%20the.223%20Remington%20cartridge%20was%20officially,and%20a%20chamber%20pressure%20of%2052%2C000%20psi.%20

Wikipedia. (2001, October 1). *Geosynchronous satellite*. Retrieved from wikipedia.org: https://en.wikipedia.org/wiki/Geosynchronous_satellite

Wikipedia. (2003, May 22). *Outer space treaty*. Retrieved August 28, 2022, from en.wikipedia.org: https://en.wikipedia.org/wiki/Outer_Space_Treaty

Zak, A. (2013, November 1). *The hidden history of the Soviet satellite-killer*. Retrieved from popularmechanics: https://www.popularmechanics.com/space/satellites/a9620/the-hidden-history-of-the-soviet-satellite-killer-16108970/

3.

SPACE ELECTRONIC WARFARE, SIGNAL INTERCEPTION, ISR, JAMMING, SPOOFING, & ECD (NICHOLS & MAI)

Student Objectives

Space is the new frontier of electronic warfare (EW), intelligence, and reconnaissance. Space is also the place to view the earth in large "earth traces." These views can help military and agricultural planners make better decisions on protecting the United States and managing (increase) global food supply, land usage, irrigation, and health. The same information for diametrically different uses. This chapter is concerned with the former. We peruse:

- Key definitions in EW, satellite systems, and ECD countermeasures
- A look at space calculations and satellite threats using

plane and spherical trigonometry to explain orbital mechanics

- A brief review of EMS, signals, RADAR, Acoustic, and UAS Stealth principles,
- Signals to/from satellites and their vulnerabilities to Interception, Jamming, and Spoofing,
- Signals to/from satellites and their vulnerabilities to Interception, Jamming, and Spoofing
- The promising ECD technology countermeasure to spoofing can detect, mitigate, and recover fake and genuine signals.

EW Definitions [1]

Electronic Warfare (EW) is the art and science of denying an enemy the benefits of the electromagnetic spectrum **(EMS)** while preserving them for friendly forces. (Wolff, 2022)

Signals Intelligence (SIGINT) is the analysis and identifying intercepted transmissions, including frequency, bandwidth, modulation (“waveform”), and polarization. Four categories of SIGINT are: (Wolff, 2022)

- Electronic Intelligence **(ELINT)**
- Communications Intelligence **(COMINT)**
- Foreign instrument SIGINT **(FISINT)**

- Measurement intelligence **(MASINT)** Covered in Chapter 10 of *DRONE DELIVERY OF CBNRECy – DEW WEAPONS Emerging Threats of Mini-Weapons of Mass Destruction and Disruption (WMDD)* (Nichols & Sincavage, 2022)

EW Sub-Areas

Electronic Warfare Support (EWS/ES) measures detection, intercept, identification, location, and localizes sources of intended and unintended radiated electromagnetic **(EM)** energy. **(Wolff, 2022)**

Activities related to **ES** include:

- *Electronic Reconnaissance*: location, identification, and evaluation of foreign electromagnetic radiation
- *Electronic intelligence*: Technical and geolocation intelligence derived from foreign non-communications electromagnetic radiation emanating from sources other than nuclear detonations or radioactive sources
- *Electronics security*: protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the interception and study of non-communications electromagnetic radiation, e.g., radar. (Wolff, 2022)[2]

Electronic Attack (EA) activities – may be either offensive or defensive and include: (Wolff, 2022)

- *Countermeasures:* employment of devices and/or techniques that has as their objective the impairment of the operational effectiveness of enemy activity
- *Electromagnetic deception*: Covered in Chapter 7 of *DRONE DELIVERY OF CBNRECy – DEW WEAPONS*
- *Emerging Threats of Mini-Weapons of Mass Destruction and Disruption (WMDD)* (Nichols & Sincavage, 2022) Various **EM** deception techniques, such as a false target or duplicate target generation, confuse the enemy intelligence, surveillance, and reconnaissance systems **(ISR). (Wolff, 2022)**
- *Electromagnetic intrusion*: is the intentional insertion of EM energy **(EME)** into transmission paths in any manner to deceive operators or to cause confusion.
- *Electromagnetic jamming* is deliberate radiation, reradiation, or reflection of EME to prevent or reduce an enemy's effective use of the **EMS** and with the intent of degrading or neutralizing the enemy's combat capability.
- *Electromagnetic pulse* is EM radiation from a strong electronic pulse [Directed energy weapons (DEW)] that may couple with electrical or electrical systems to produce damaging current and voltages. (Wolff, 2022)Chapters 9-11 in *DRONE DELIVERY OF*

CBNRECy – DEW WEAPONS Emerging Threats of Mini-Weapons of Mass Destruction and Disruption (WMDD) expertly cover the subject. (Nichols & Sincavage, 2022)

- *Electronic probing* is intentional radiation designed to be introduced into the devices and systems of potential enemies to learn the operational capabilities of the devices and systems.
- *Cyber or electronic 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) (Nichols & Sincavage, 2022)

Electronic protection measures (EP): EP measures fall into six categories: (Wolff, 2022)

EM hardening: actions are taken to protect personnel, facilities, and or equipment by blanking, filtering, attenuating, grounding, bonding, and shielding against undesirable effects of EME.

Electronic masking: controlled radiation of EME on friendly frequencies to protect the emissions of friendly communications and electronic systems against enemy **EWS** measures and **SIGINT** without significantly degrading the operation of friendly systems.

Emission control: sensitive and controlled use of **EM**, acoustic, or other emitters to optimize command and control **(C2)** capabilities while minimizing the following for operations security **(OPSEC):** 1) detection by enemy sensors; 2) mutual interference among friendly systems; 3) enemy interference with the ability to execute a military deception plan. (Wolff, 2022)

EMS management: planning, coordinating, and managing joint use of the EMS through operational, engineering, and administrative procedures.

Wartime reserve modes: characteristics and operating procedures for sensors, communications, navigation aids, threat recognition, weapons, and countermeasures systems that will contribute to military effectiveness if unknown to or misunderstood by opposing commanders before they are used but could be exploited or neutralized if known in advance. (Wolff, 2022)

EM compatibility: the ability of systems, equipment, and devices that use the EMS to operate in their intended environments without causing or suffering unacceptable or unintentional degradation because of electromagnetic radiation **(EMR)** or response. (Wolff, 2022) This is an extremely important concept and is exploited by the use of

UAS against USN assets in the South China Seas (**SCS**.) (Nichols & al., 2020)

ISR – Intelligence, Surveillance, and Reconnaissance [3]

Intelligence, surveillance, and reconnaissance operations **(ISR)** are used to collect information about the enemy, terrain, weather, and other aspects of the Area of Operation **(AO)** that will affect friendly combat operations. (Global Security.Org, 2022)

The Army has conducted reconnaissance and surveillance tasks since its inception. The production of *intelligence* (the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning an enemy force or area of operation) has always been critical to successfully accomplishing the mission. ISR is the term currently applied to combined arms enabling operation that combines previously described as *reconnaissance and surveillance (a maneuver or collection task)* with the *production and dissemination of intelligence (a staff task).* ISR is a constant, continuous, and optimized operation that focuses on the collection of relevant information that is analyzed to create intelligence to support the commander's and or leader's situational understanding and the operational cycle. (Global Security.Org, 2022)

ISR Systems and Technology from Space

MIT gives an interesting purview of their mission for ISR from space. They see it as "Creating Technology To Provide Vital Tactical Information." They conduct "R&D in advanced sensing, signal and image processing, decision support technology, and high-performance embedded computing to provide systems capable of gathering reliable intelligence, surveillance, and reconnaissance information." (MIT R&D, 2022) It is this purview that the authors see from the user POV to develop "earth traces" from space capable of yielding unique information on non-military technologies such as agriculture management, crop rotation, global food supply, tree and fire zone management, and cattle management.

Eichelberger Collective Detection (ECD) Definitions / Counter Spoofing Concepts

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:

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

Eq. 3-1

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 Ớ (N log N) time. [4](Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019)

Like classical GPS receivers, coarse-Time Navigation (CTN) is a snapshot receiver localization technique that measures sub-millisecond satellite ranges from correlation peaks. (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 combines all the available information and decides only at the end of the computation. 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.

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, ellipsoid, equator, meridian longitude, latitude, geodetic latitude, geocentric latitude, and geoid. [5]

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

Navigation Data is the data transmitted from satellites, which includes orbit parameters to determine the satellite locations, timestamps of signal transmission, atmospheric delay estimations, and status information of the satellites and GPS as a whole, such as an accuracy and validity of the data. (IS-GPS-200G, 2013) [6]

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)

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

Scope

Looking at the definitions above, the EW and ECD spheres are huge and encompass many different sciences. Chapter 3 focus will be on space electronic warfare with a limited scope and a specific emphasis on spoofing. We are trying to get a sense of the technologies and challenges. Jamming will be briefly presented only as a precursor attack to a spoofing attack. There are plenty of learning seminars available by SMEs like Rhode & Schwartz and fundamental textbooks to inform the reader. (Wolff, 2022) (Adamy D. , EW 101: A First Course in Electronic Warfare, 2001) (Adamy D. L., Space Electronic Warfare, 2021) (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., 2004)[7] [8]

Decibel Math

EW calculations are done using "dB" math. It allows manipulation of very large numbers such as transmitted signal strength and very small numbers such as received signal strength. Numbers expressed in decibels (or dB) form are logarithmic and follow the rules.[9] This permits the comparison of values that may differ in many orders of magnitude. It is important to understand that any value expressed in decibel units is a ratio converted to a logarithmic form. (Adamy D. , EW 101: A First Course in Electronic Warfare, 2001)

To Convert To Decibel Form (base 10 log)

Ratio (in dB) = 10 log (Linear Ratio)

Eq. 3-2

Example: convert 2 (the ratio of 2 to 1) to decibel form.

$10\log(2) = 3dB$ (rounded)

convert 1/2 (the ratio of 1 to 2) to decibel form.

$10\log(0.5) = -3dB$ in EW, link loss and antenna calculations this is a useful factor.

A reverse way of looking at the process or converting back to a nonlogarithmic form is:

Antilog (logarithm number) = linear number in place of 10 (logarithmic number)

So, antilog (3/10) = 2. See (Adamy D. , EW 101: A First

Course in Electronic Warfare, 2001) or (Adamy D. L., 2004) or (Adamy D. L., Space Electronic Warfare, 2021) for many examples of nauseating details and helpful tables for common usage.

Plane Trig /Equations

To solve problems of elevation and azimuth of look angles associated with Earth Satellites, three-dimensional (3-D) angular relationships are solved with Plane and Spherical Trigonometry. Plane Trigonometry deals with triangles in a plane. The important relationships are:

Plane Trigonometry:

The Law of Sines: $a/\sin A = b/\sin B = c/\sin C$

Eq. 3-3

Note: Lower case letters represent the lengths of a triangle's side, and upper-case letters are their associated angles opposite the corresponding side.

$$a^2 = b^2 + c^2 - 2bc\ cos A$$

Eq. 3-4

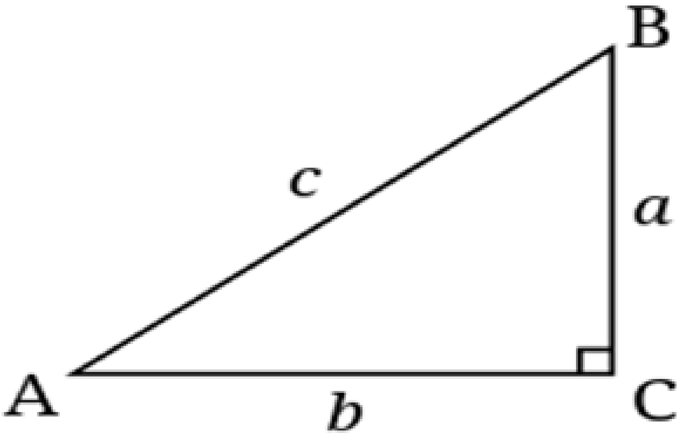
The Law of Cosines for Angles: $A = b\cos C + c\cos B$

Eq. 3-5

A right triangle is a plane triangle with a 90° angle. All triangles fall under the above rules.

Right Triangle: 2-dimensional defined, also known as a Plane Triangle.

Figure 3-1 Right Triangle



Source: (Adamy D. L., Space Electronic Warfare, 2021)

Spherical Trigonometry:

The Law of Sines for Spherical Triangle:

$$\sin a / \sin A = \sin b / \sin B = \sin c / sinC$$

Eq. 3-6

The Law of Cosines for Sides:

$$\cos a = \cos B \cos C + \sin B \sin C \cos a$$

Eq. 3-7

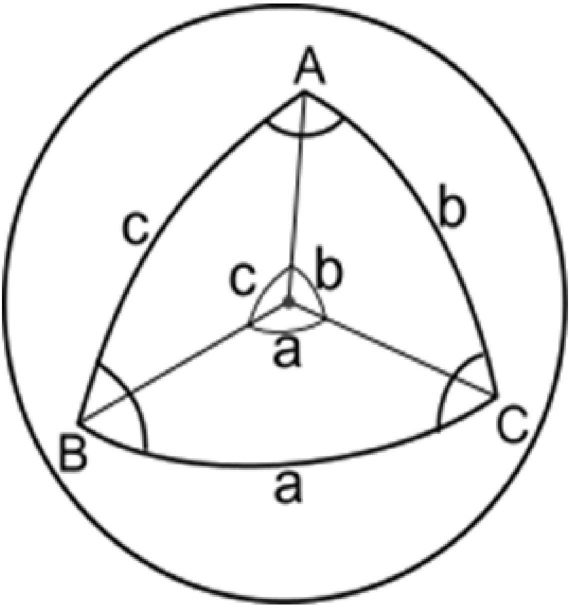
The Law of Cosines for Angles:

$$\cos A = -\cos B \cos C + \sin B \sin C \cos a$$

Eq. 3-8

Spherical Triangle: Formed by 3 great circles that pass through a common center point.

Figure 3-2 Triangle on a Sphere

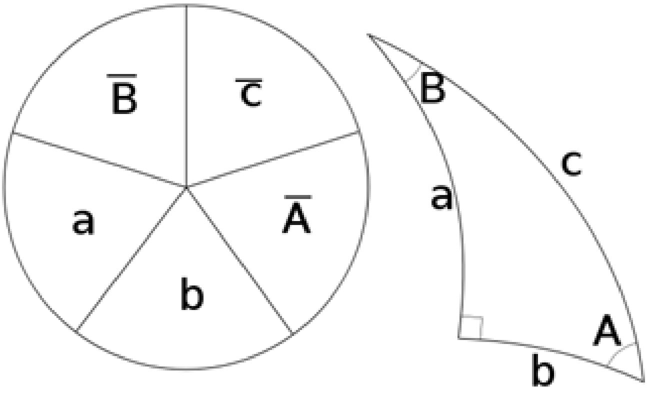


Source: (Adamy D. L., Space Electronic Warfare, 2021)

Napier's Rules:

Right spherical triangles allow the use of simplified spherical trigonometric equations using Napier's rules.

Figure 3-3 Napier's Rules for Right Spherical Triangles



Source: Author modification of Figure 2.6 in (Adamy D. L., Space Electronic Warfare, 2021)

Rules for Napier's right spherical triangles

$\sin a = \tan b \cot B$ Eq. 3-9

$\cos A = \cot c \tan b$ Eq. 3-10

$\cos c = \cos a \cos b$ Eq. 3-11

$\sin a = \sin A \sin c$ Eq. 3-12

Orbital Mechanics

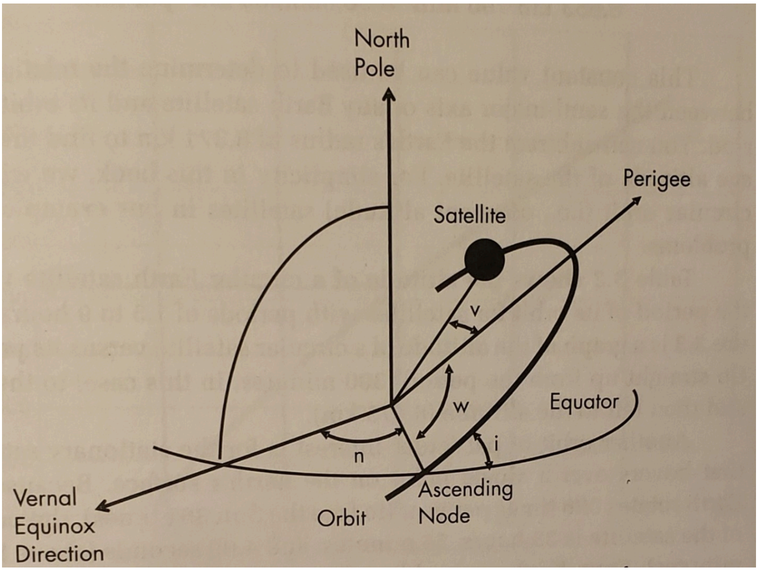
Spherical and Elliptical geometry explain Orbital Mechanics. The difficulty trying to understand Spherical Triangles versus Plane Triangles is because Spherical Triangles are 2-dimensional, taking place on a sphere rather than a plane. An example would be looking at a map and drawing a line from one point to the other, *r* but in reality, the space between is actually curved. Spherical Trigonometry takes the curvature of the earth into account. This is known as the Keplerian ephemeris. The Ephemeris elements of Spherical Triangles can be seen in Table 3-1.

Table 3-1
Earth Satellite Ephemeris

	Ephemeris Value	**Significance**
a	Semi-major Axis	Size of the Orbit
e	Eccentricity	Shape of the Orbit
i	Inclination	Tilt of orbit relative to the equatorial plane
Ω-θ = n	Right ascension of the ascending node	Longitude at which the satellite crosses the Equator going north
w	Argument of Perigee	Angle between ascending node and perigee
v	True anomaly	Angle between perigee and the satellite Location in the Orbit

Note: Apogee = a(1-e) Source: (Adamy D. L., Space Electronic Warfare, 2021)

Figure 3-4 The Ephemeris defines the satellite's location with six factors.



Source: Courtesy of (Adamy D. L., Space Electronic Warfare, 2021)

From the orbital elements, it is possible to compute the position and velocity of the satellite.

Kepler's Third Law states the relationship between the size of the orbit and its period is defined by:

$$a^3 = CP^2 \qquad \text{Eq. 3-13}$$

where: a = the semi-major axis of the orbit ellipse, C is a constant, and P = the orbit period.

Example: If a Satellite circles the Earth every 1.5 hours and has an altitude of 281.4-km-high (or a radius from the center of the Earth of 6,653 km, then *C* is calculated as; 6,653 km3/ 90 min2 = 36,355.285 km per min2

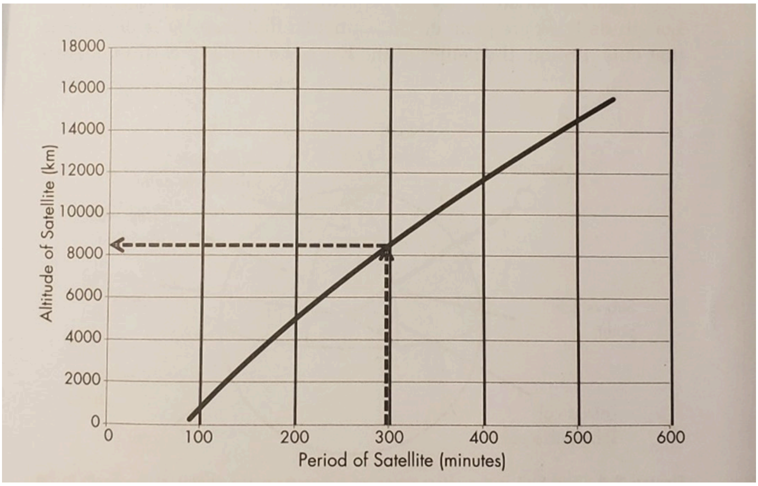
Table 3-2 Shows the altitude of a circular Earth satellite versus the period of its orbit for satellites with periods of 1.5 hours to 9 hours.

Altitude and Semi-Major Axis of Circular Orbits Versus the Satellite Period

p(min)	h(km)	α(km)	p(min)	h(km)	α(km)
90	281	6652	330	9447	15818
105	1001	7372	345	9923	16294
120	1688	8059	360	10392	16763
135	2346	8717	375	10854	17225
150	2980	9351	390	11311	17682
165	3594	9965	405	11761	18132
180	4189	10560	420	12206	18577
195	4768	11139	435	12646	19017
210	5332	11703	450	13081	19452
225	5883	12254	465	13510	19881
240	6422	12793	480	13936	20307
255	6949	13320	495	14357	20728
270	7466	13837	510	14773	21144
285	7974	14345	525	15186	21557
300	8473	14844	540	15595	21966
315	8964	15350	–	–	–

Source: (Adamy D. L., Space Electronic Warfare, 2021)

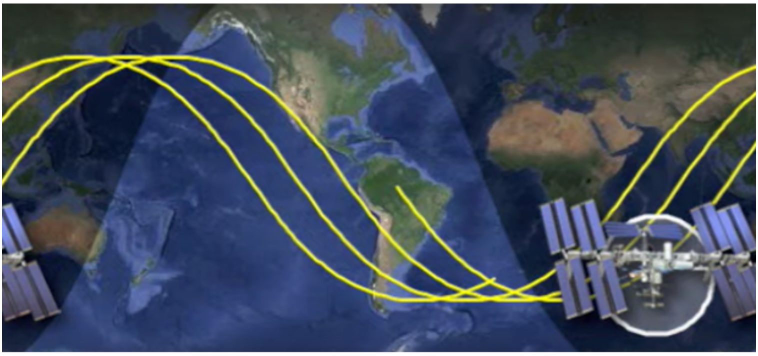
Figure 3-5 Altitude of a Circular Satellite is a Function of its Orbital Period



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

EARTH TRACES

Figure 3-6 Earth traces of synchronous satellites as they travel in sine wave over a global map

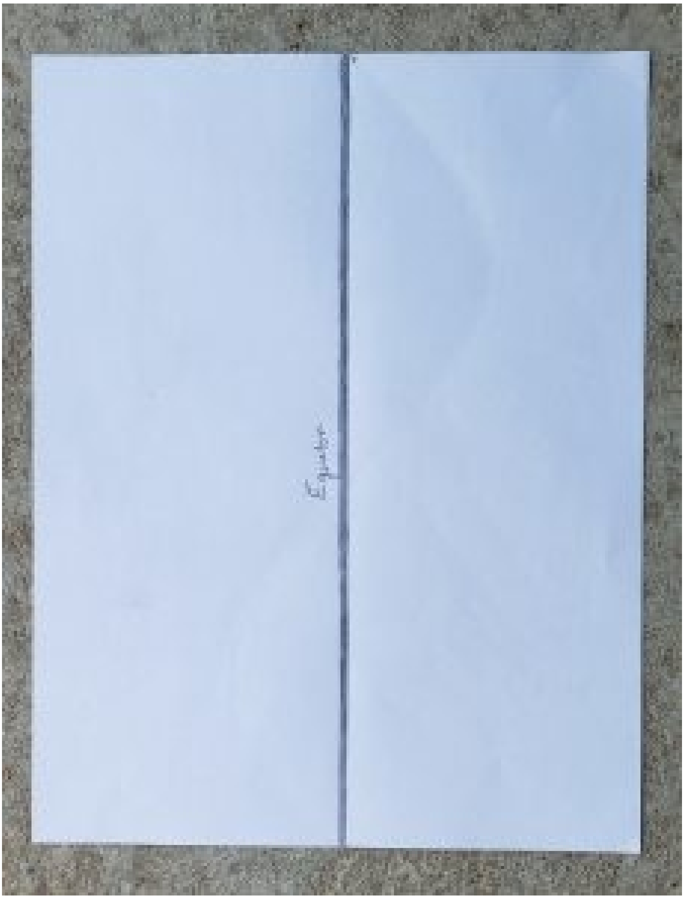


Source: (CYFO: A, 2018)

If you have ever wondered why satellites look like they travel in a sine-wave along a global map, you are not alone. It seems counterintuitive; however, there is an easy explanation for this. First, remember that a global is not a flat surface. Although the above map is in 2-dimensions and Earth traces of a satellite are represented in a sine wave, making them look as though they do not travel in a straight line. Why are they represented this way?

If we take a piece of paper, draw a straight line in the center, and label it as the equator, we will find out that it is the only straight line on a 2-dimensional map.

Figure 3-7 Representation of the Equator on a 2-dimensional paper



Source: Hand drawn by co-author Mai, R. (2022)

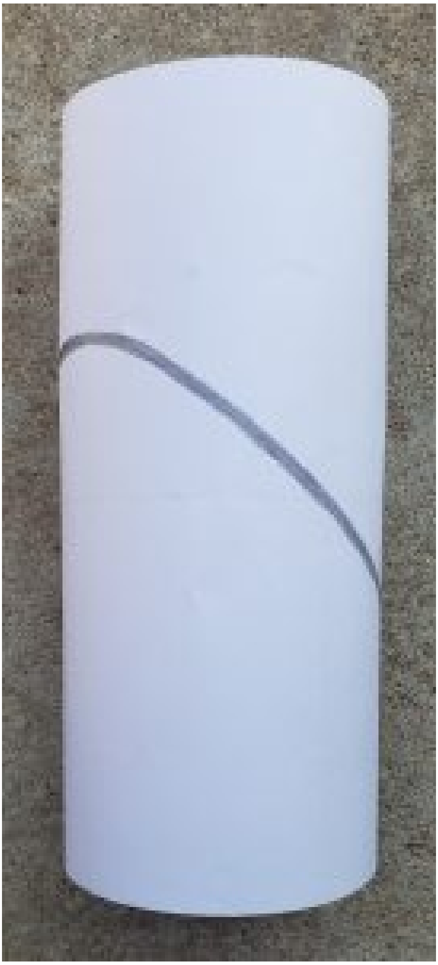
Now, as we fold the piece of paper into a circle, we see that the line creates a circle. It does not create the sine wave that we see in the first map above.

Figure 3-8 Representation of the Equator on a circular rolled 3-dimensional paper.

Source: Hand drawn by co-author Mai, R. (2022)

However, by working backwards through this problem, by drawing a circle on the folded paper in any other inclination, we do not have a result that creates a straight line.

Figure 3-9 Representation of any inclination as a sine wave on circular rolled 3-dimensional paper- represent a satellite's Earth traces.

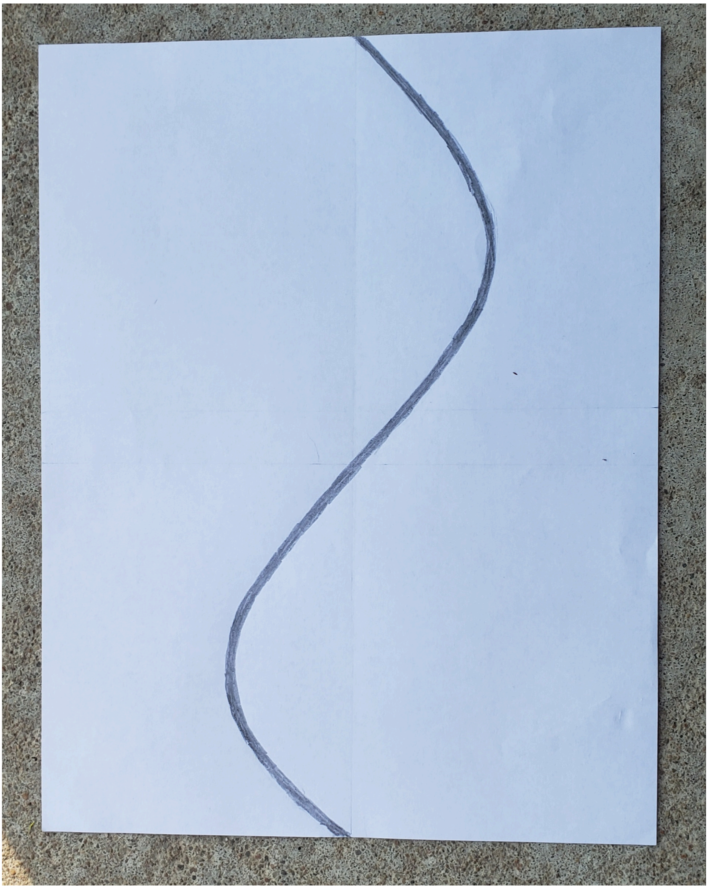


Source: Hand drawn by co-author Mai, R. (2022)

Instead, a sine wave is formed when unfolded and laid flat, just like in the picture above. This is how a sine wave is formed when trying to represent a satellite Earth traces in 2-dimensional form. Even though the satellite travels in a straight line when circling a globe. To represent its travel in 2 dimensions, this is the result. It is true for all angles other than the equator.

When unfolded, you can see where the sine wave is created.

Figure 3-10 ***The Earth trace is the locus of latitude and longitude of the SVP as the satellite moves through its orbit.***



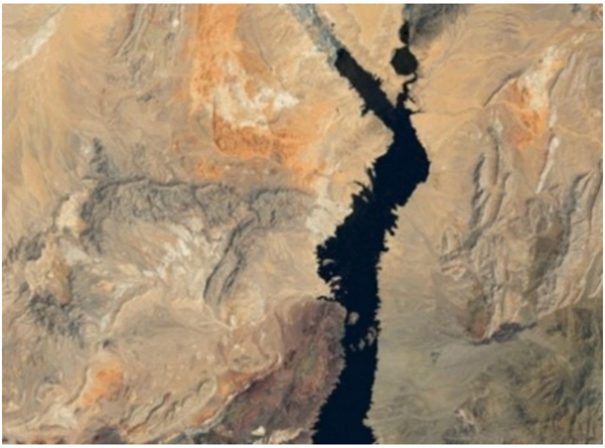
Source: Hand drawn by co-author Mai, R. (2022)

LOOK ANGLES

The Earth trace is the *locus of latitude and longitude of the SVP as the satellite moves through its orbit*. Note: The SVP is the point on the Earth's surface directly below the satellite. This point intersects the line from the center of the Earth to the satellite with the surface of the Earth. LEO (low earth orbits) determines the moment-to-moment area of the Earth that the satellite sees. It also allows us to calculate the look angles and range of the satellite from a specified point on (or above) the Earth at any specified time.

A recent example of a satellite monitoring Lake Meade water loss since 2000, looking towards the SVP. It shows before and after.

Figure 3-11 Lake Meade before water loss 2000 Figure 3-12 Lake Meade after water loss 2021

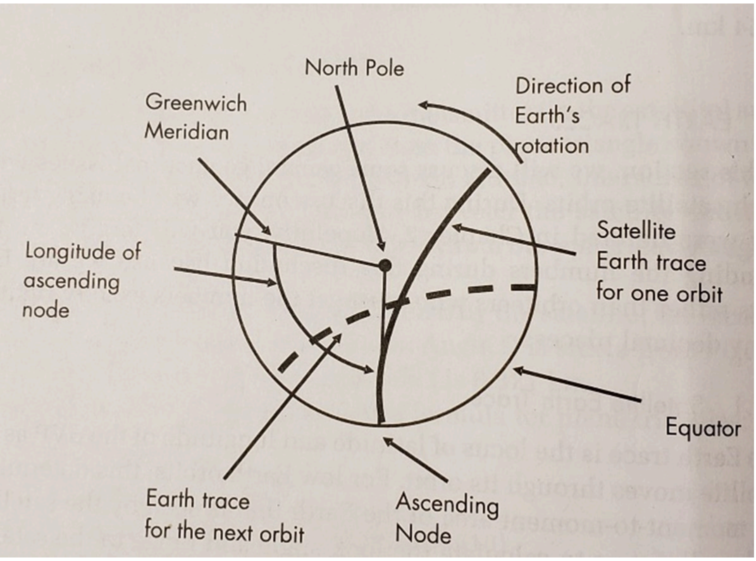


Source for Figure 3-11 & 3-12: (Data: USGS/NASA Landsat, 2021)

Using the six elements of Ephemeris (defined earlier in the chapter) the exact location of a satellite can be calculated at any time. For example, the Earth trace of a satellite with a 90-minute orbital period will move West by 22.56 longitude degrees for each subsequent orbit.

Example: (90-minute orbital Period / 1463 sidereal day, minutes) x 360 deg = 22.56 deg

Figure 3-13 Earth trace of the satellite is the path of the SVP over the Earth's surface in Polar view.

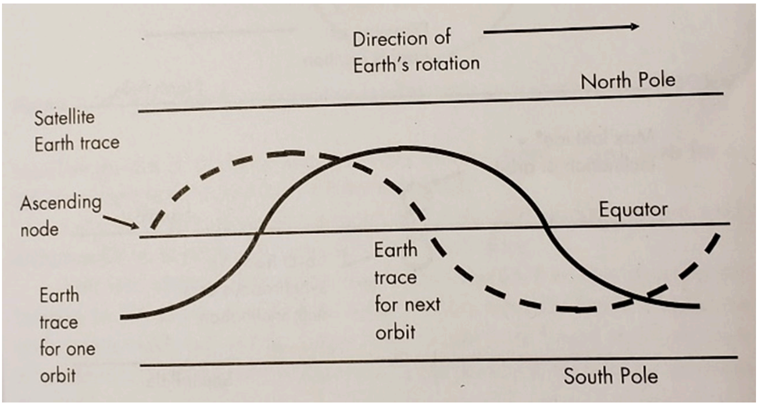

North Pole
Greenwich Meridian
Direction of Earth's rotation
Longitude of ascending node
Satellite Earth trace for one orbit
Equator
Earth trace for the next orbit
Ascending Node

Source: Courtesy of (Adamy D. L., Space Electronic Warfare, 2021)

Where: (SVP = Sub-vehicle point) and is the intersection of a line from the center of the Earth to the satellite with the Earth's surface

The Earth area over which a satellite can send or receive signals to and from the Earth-based stations during each orbit depends on the altitude of the satellite and the beam width and orientation of antennas on the satellite. If a satellite is placed in polar orbit, its orbit has 90˚ inclination and will therefore eventually provide complete coverage of the surface of the Earth.

Figure 3-14 Earth trace of a satellite is the path of the SVP over the Earth's surface in equatorial view.

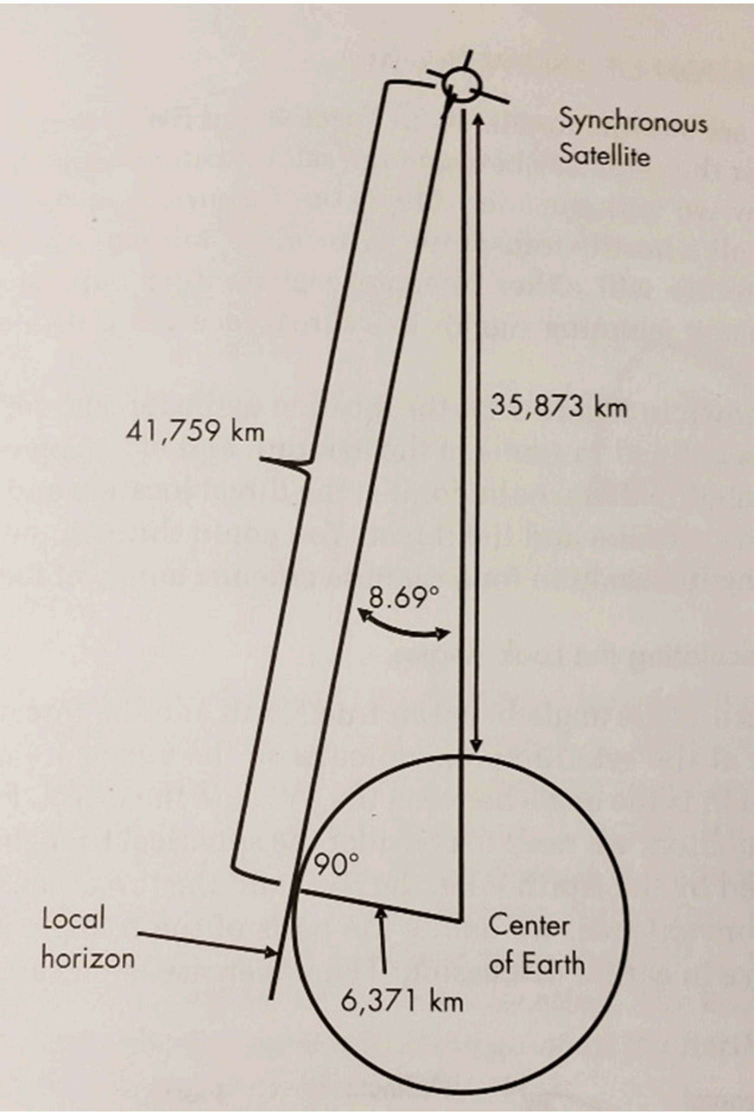


Source: Courtesy of (Adamy D. L., Space Electronic Warfare, 2021)

A synchronous satellite has an SVP that stays in one location on the Earth's surface. This requires that its orbital period be one sidereal day (i.e., 1,436 minutes). Another requirement for a fixed SVP is that the orbit has an 0° inclination. That would place it directly on the border.

Figure 3-15 Example calculation: Maximum Range to a synchronous satellite on the horizon is 41,759 km by

Kepler's Laws. Link loss for a 2 GHz signal would be from 189.5 to 190.9 dB



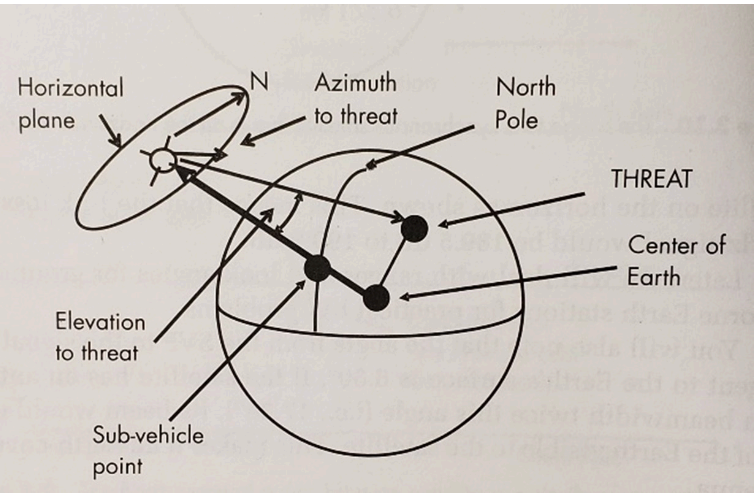
Source: Courtesy of (Adamy D. L., Space Electronic Warfare, 2021)

Figure 3-15 shows a sample calculation of the range of a synchronous satellite based on a semi-major axis of 42,166 km. "In a circular orbit, the satellite's height will be 35,795 km. The maximum range can be calculated from the Earth surface station (ESS) to the synchronous satellite with a circular orbit. The diagram is a planer triangle in the plane containing the ESS, satellite, and center of Earth. The ESS sees the satellite at 0 deg elevation. The minimum and maximum range values for the satellite to the ground link are 35,795 km and 41,682 km. The shorter range applies if the satellite is directly overhead, and the maximum range is for the satellite to the horizon as shown." (Adamy D. L., Space Electronic Warfare, 2021)

Location of Threat to Satellite

The location of a threat from the satellite is defined in terms of the azimuth and elevation of a vector from the satellite that points at the threat location and the range between the satellite and the threat. The vector points information for a satellite antenna aimed at the threat. An EW system on the satellite will either intercept signals from a threat transmitter or transmit jamming signals to a threat receiver at the considered location.

Figure 3-16 The azimuth and elevation angle from the nadir defines the direction of a threat to a satellite.



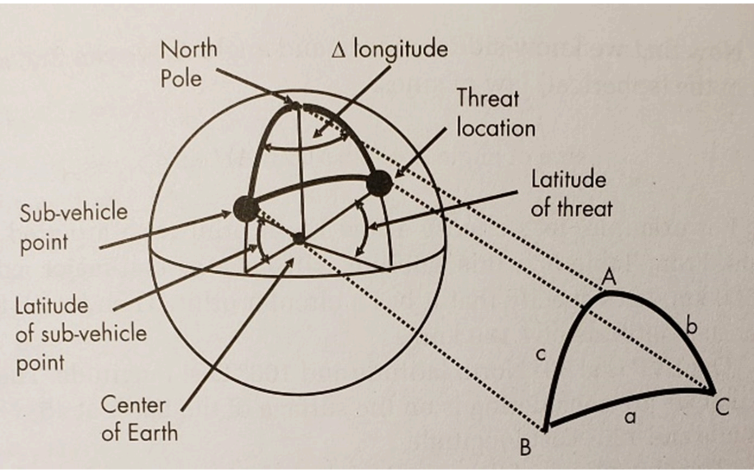
Source: Courtesy of (Adamy D. L., Space Electronic Warfare, 2021)

Where: the *azimuth* is the angle between true North and the threat location in a plane at the satellite perpendicular to the vector from the SVP. The *elevation* is the angle between the SVP and the threat. The *nadir* is defined as the point on the celestial sphere directly below an observer.

Calculating the Look Angles:

For the azimuth calculation, we need to consider the spherical triangle.

Figure 3-17 A spherical triangle is formed between the North Pole, the SVP, and the Threat location.



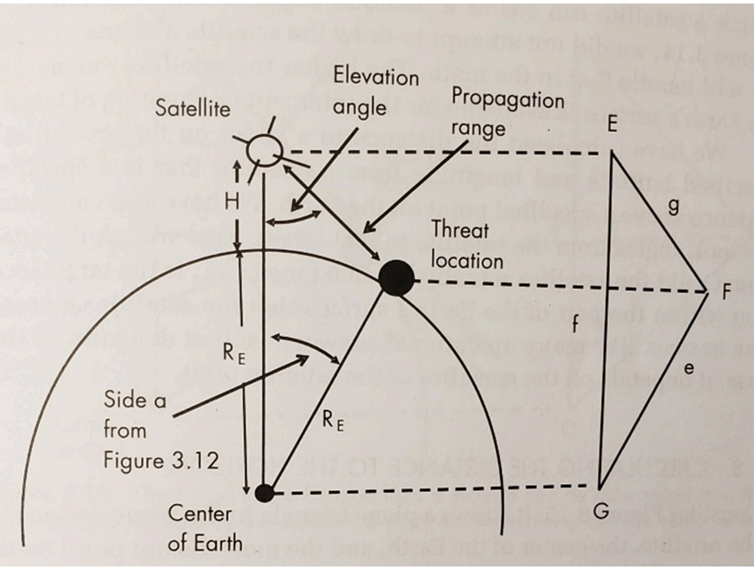
Source: Courtesy of (Adamy D. L., Space Electronic Warfare, 2021)

The elevation from the nadir and range to a threat from a satellite can be determined from the plane triangle defined by the satellite, the threat, and the center of the Earth. For example, Set E is at the satellite, F is at the threat, and G is at the center of the Earth. Side e is the radius of the Earth (6,371 km). Side f is the semi-major axis (the radius of the Earth plus the satellite altitude = 10,560 km), angle G is side a from the spherical triangle above (21.57°), and side g is the propagation distance between the satellite and the threat.

The law of cosines for plane triangles is:

$$g^2 = e^2 + f^2 - 2ef\cos(G) \qquad \text{Eq. 3-14}$$

Figure 3-18 The elevation from the nadir and range to a threat from a satellite can be determined from the plane triangle defined by the satellite, threat, and the center of the Earth.



Source: Courtesy of (Adamy D. L., Space Electronic Warfare, 2021)

EMS

Chapter 8 Designing UAS Systems for Stealth in *Unmanned Aircraft in the Cyber Domain*, 2nd ed. **(Nichols R. K.-P., 2019)** the author's introduced the Electromagnetic Spectrum in relationship to battlefield dimensions and stealth signatures for unmanned aircraft systems **(UAS)**. We will start with a short replay of this information because the coverage was instructive.

Designing a UAS for Stealth

Stealth means "to resist detection." Stealth applies to the air vehicle and materials visible to the enemy plus the internal sense and avoid systems **(SAA)** that control / create noise, heat, electromagnetic emanations, and changes in light. For intelligence, reconnaissance, and surveillance **(ISR)** platforms and missions, the UAS systems must be undetected in operation. "It is desirable not to alert the enemy (military) or criminals (police) to the ISR operation." It can be assumed that the enemy is using counter-UAV [10]operations and weapons. Stealth design protects the air vehicle from these counter – UAV measures. Stealth in civilian operations results in minimal environmental disturbances. (Austin, 2010)

Detection Signatures

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)

Noise (acoustic) [16 m-2 cm, or 20 – 16000 Hz]
Optical (visible) [0.4 – 0.7 um]
Infrared (thermal) [0.75 um – 1 mm]

RADAR (radio) [3 mm – 3 cm]" (Austin, 2010)

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)

A student might look at the answers above and ask what the significance is? Let's take a short sojourn down the EMS lane. Military planners used to think about ground, sea, and air. Space came later. Now there is a "fifth realm," the electromagnetic spectrum **(EMS).** For EMS, we think in terms of ***frequency.*** Enhancing our ability to communicate using the EMS significantly changes how we conduct warfare. (Adamy D. -0., 2015) (Adamy D. L., Space Electronic Warfare, 2021)

Radio communications and wireless transmissions using tuned transmitters and the information explosion of the internet were the heart of the warfare revolution. The certainty of intercepting radio communications and radar signals and the ability to locate transmitters significantly impacted military operations. Intercept, jamming, spoofing, emitter location, message security, and transmission security became fundamental to warfare. The basic destructive capabilities (energy) employed in warfare have not changed greatly (fast-moving projectiles, significant overpressure, heat, and sound).

However, the ways they are employed have changed significantly through the use of the EM Spectrum (EMS). Now, we guide the destructive energy of weapons towards their intended targets using the EMS in many ways. Also, the EW specialist uses EMS to prevent those weapons from hitting their intended targets. Sometimes the destruction of communications capability by an enemy is the goal.

The battlespace, which once had only four dimensions (latitude, longitude, elevation, and time [before radio]), now has a fifth dimension: frequency. (Adamy D. -0., 2015) See Table 3-2 Battlespace Dimensions.

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 the capacity for data transfer of electrical communications systems. 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.

Table 3-3 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
		Vulnerability to Spoofing[11]

Source: (Adamy D. -0., 2015) Reprinted from Table 8-1 in (Nichols R. K.-P., 2019)

Note the addition of a new and powerful threat vector – Spoofing.

A closer transmitter will better receive a signal and can usually locate the transmitter more accurately. Once we depend on inputs from multiple receivers, the network becomes central to our war-making ability. [Think UAS Team collaboration.] We have now entered net-centric warfare. (Adamy D. -0., 2015) Net-Centric warfare was the brainchild of John Arquilla and David Ronfeldt of the National Defense Research Institute. See: (Ronfeldt, 1966)

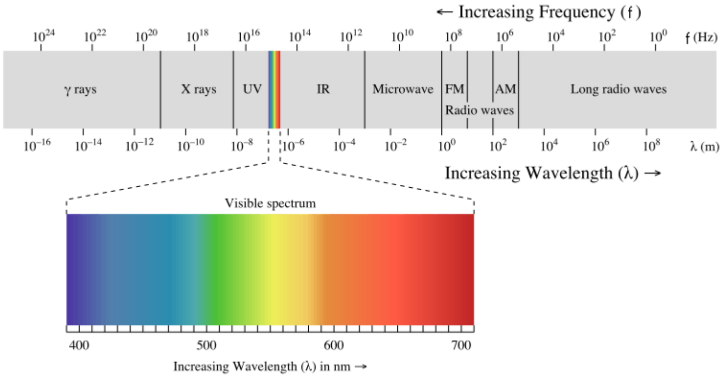
Thinking again about a team or swarm of UAS, the low-hanging fruit target is US communications. (Nichols R. K., 2020)We depend on connectivity in everything we do: daily lives, social interactions, business, manufacturing, government, transportation, computers, and warfare, to name just a few in the extensive list. *Connectivity is any technique for moving information from one location or player to another.* Consider the economic impact of shutting our critical infrastructure (banking, air transportation, etc.). Damaging the connectivity of the system is real damage. We measure connectivity in terms of information flow. In warfare, this is called Information Operations **(IO).** Fundamental to IO is the *frequency* at which the information is transmitted or received.

Returning to the topic of stealth concerning UAS design, we note the intelligence, surveillance, reconnaissance, and weapons payload-delivery functions of UAS. These are all IO operations, and frequency is at the heart of their success against or denial by the enemy. (Nichols R. K.-P., 2019)

Electromagnetic Spectrum (EMS)

The German company, Tontechnic-Rechner-Sengpielaudio **(TRS)** has put together some clever tools for conversions of wavelength to frequency (and vice versa) "for Acoustic Waves (sound waves) and Radio Waves and Light waves in a vacuum." (TRS, 2018) Start with Figure 3-19 EMS. Note the inverse relationship between frequency, **f,** and wavelength L (lambda – Greek).

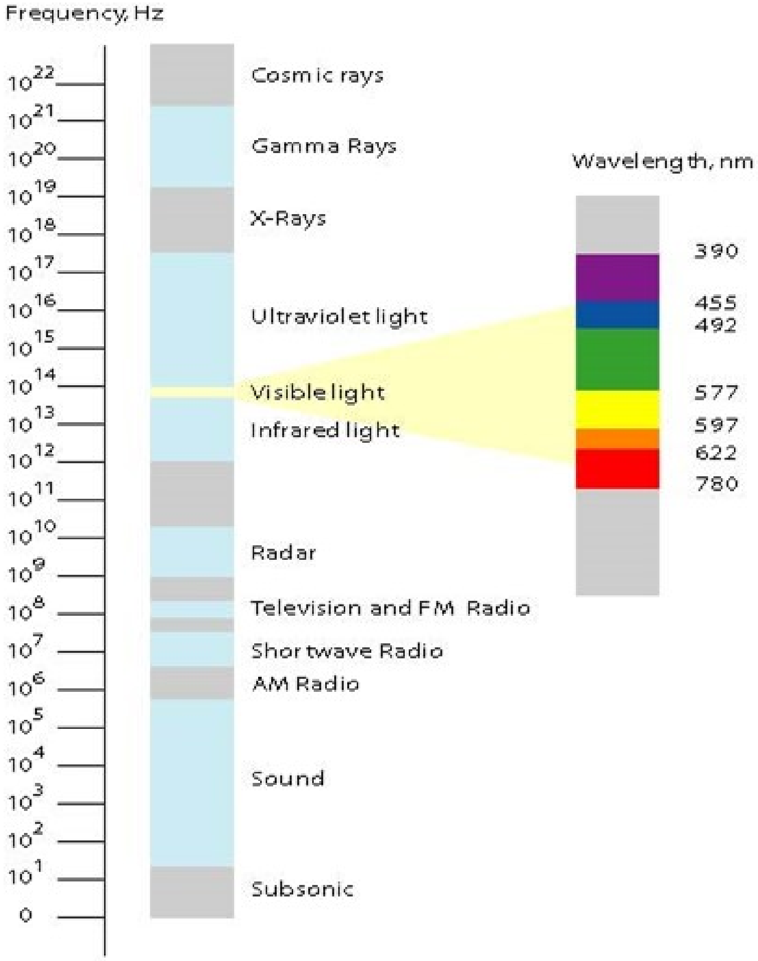
Figure 3-19 EMS



Source: (TRS, 2018) Reprinted from Figure 8-1 in (Nichols R. K.-P., 2019)

Note also how small the visible spectrum is as part of the enormous EMS. Figure 3-20 shows some of the EMS functions.

Figure 3-20 EMS Functions



Source: (TRS, 2018) Reprinted from Figure 8-2 in (Nichols R. K.-P., 2019)

Figure 3-21 shows the conversion of sound and acoustic wave period to frequency and back. (Adamy D. -0., 2015) Figure 3-22 shows the Sound EMS regions (Adamy D. -0., 2015)

Figure 3-21 Conversion for sound and acoustic wave period to frequency and back

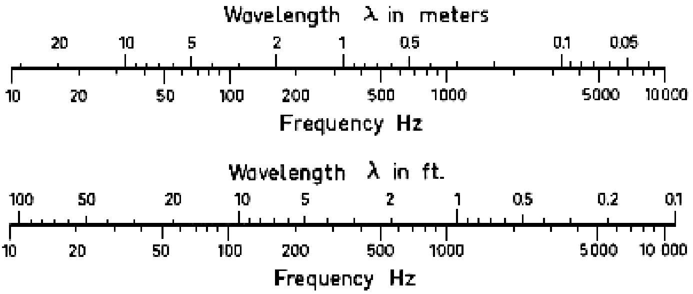
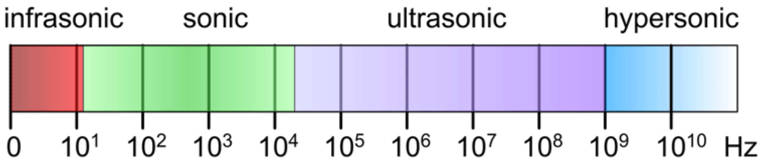


Figure 3-22 Sound EMS Regions



Source for Figures 3-21 & 3-22: (TRS, 2018)

Acoustic waves and Sound Waves in Air

Sound waves are EMS waves that propagate vibrations in air molecules. The 1986 standard speed of sound, **c**, is 331.3 m/s or 1125.33 ft/s at a temperature, T = 0 degrees Celsius." (TRS, 2018)

The formulas and equations for sound are:

$$c = Lf;\ \ L = c\ /f = cT;\ \ f=c\ /L \qquad \text{Eq. 3-15}$$

where: T = time-period or cycle duration and **T = 1/ f** and **f = 1 / T,** T in sec, frequency is in Hertz = Hz =1/ s; wavelength, L is in meters, m. The wave speed or speed of sound, c, is meters/sec, m/s. (TRS, 2018)

Noise

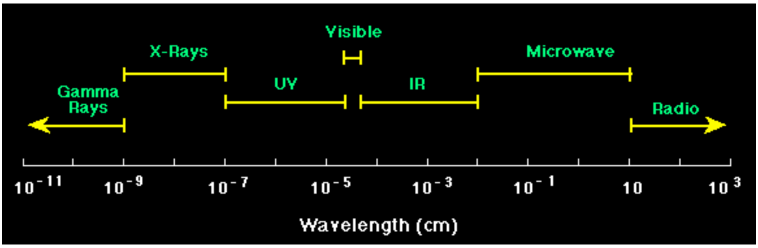
Austin states that the design limit for UAS Stealth for acoustic (noise) or sound waves is "[16 m-2 cm, or 20 – 16000 Hz]." (Austin, 2010) Use the TRS converter. {Basis: Speed of sound c = λ × f = 343 m/s at 20°C} for 16 m L = 21.4375Hz. This compares to the Austin value of 20 Hz. For the 2 cm = 0.02 m, the resulting valued for f = 17650 Hz. This is above the 16,000 Hz limit from Austin. This might be due to the 20-degree Celsius basis difference. This tells the UAS designer that the upper end of noise – Stealth acceptability of 17,150 Hz. **The Stealth range is 20 Hz – 17,150 Hz.**

Radio Waves and Light Waves in a Vacuum

The formulas and Equations for radio and light waves in a vacuum are the same. However, the constant c is different. Lower-case c is the speed of light waves and the speed of radio waves in a vacuum. The speed of light in free space (vacuum) is the speed at which electromagnetic waves propagate, including light waves." (TRS, 2018) Instead of the speed of sound in air, the speed of light c is 299,792,458 m/s (or 983,571,056 ft/s.) needs to be used in the formulas as the speed of propagation. Wave frequency in Hz = 1/s and wavelength in nm = 10 (**-9) m. (TRS, 2018)

Radio waves and microwave radiation are both forms of energy known as Electromagnetic Radiation (**EMR**). Sunlight contains other EMR forms: ultraviolet, infrared (heat) waves, and visible light waves. These EMRs spread in a vacuum at the speed of light ~ 300 000 km/s as electromagnetic radiation." (TRS, 2018) The propagation speed of electrical signals via optical fiber is about 9/10 of c or ~270 km/s. "Copper as a medium is worse slowing the propagation speed c, to ~200, 000 km/s." (TRS, 2018) Sound is also shown on the EMS chart but has no electromagnetic radiation. "Sound pressure is the deviation from local ambient pressure (sound pressure deviation) caused by a sound wave – mainly in air." (TRS, 2018) Wavelength is sometimes given in Angstrom units. 1 A = 10 (**-10) m = 0.1 nm. See Figure 3-23 EMS Reduced.

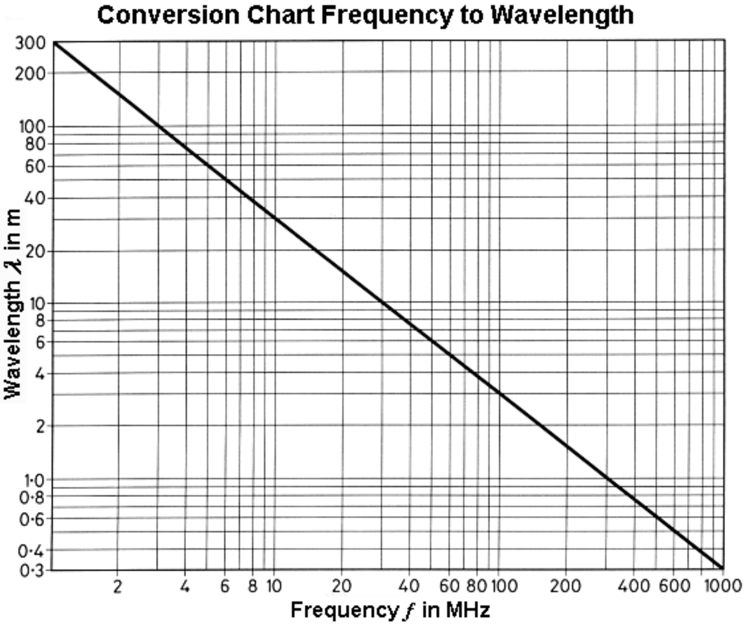
Figure 3-23 EMS Reduced



Source: (TRS, 2018)

The EMS includes visible light, gamma rays, microwaves, and radio waves. They differ by wavelength. (TRS, 2018) Figure 3-24 contains a conversion chart for radio and light waves in a vacuum.

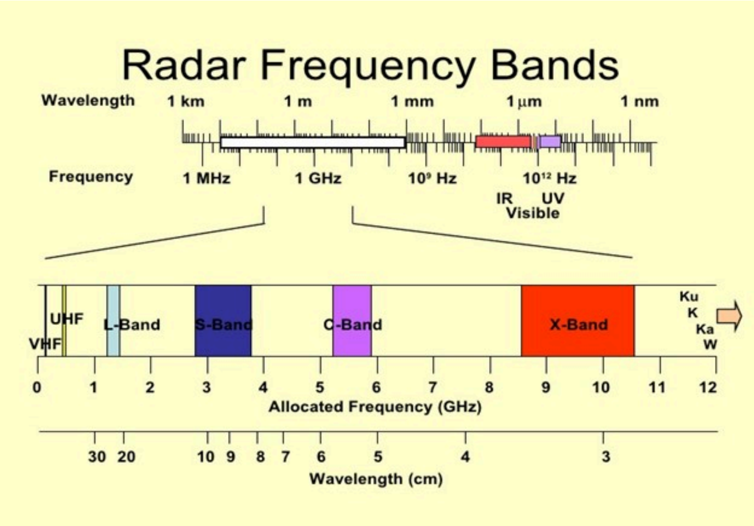
Figure 3-24 Conversion Chart – Frequency to Wavelength Radio and Light Waves in a Vacuum [12]



Source: (TRS, 2018)

We have covered noise, optical, and infrared stealth signatures. RADAR is not as simple without another trip down RADAR lane. RADAR was extensively discussed and written about in the 20th century. It is certainly one of the most influential inventions in the last century, arguably more relevant than the cellphone. Our concern is to "paint" or recognize the UAS signature from a distance, i.e., SPACE. If we can "see" the hostile UAS coming, it can be tracked, disabled, destroyed, intercepted, and "turned" to a new waypoint or objective.

Figure 3-25 RADAR Frequency Bands (ITU, 2019)

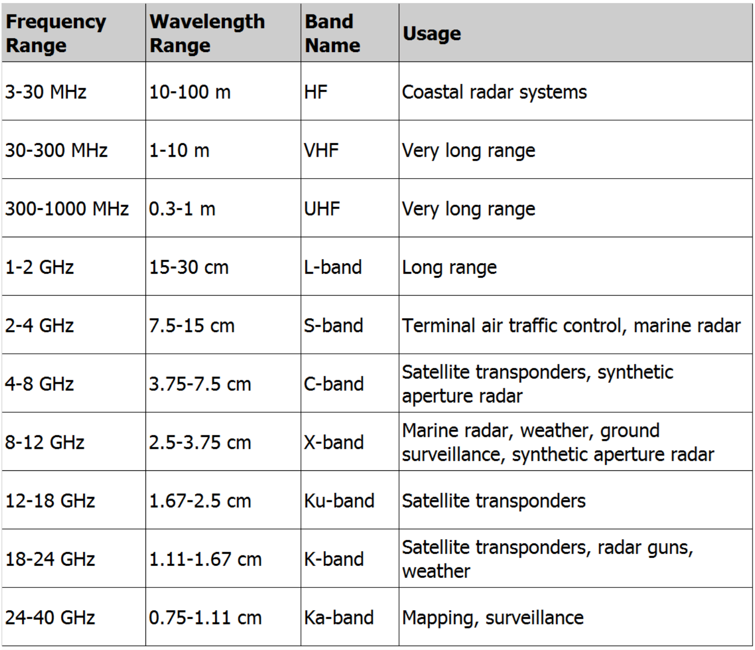


Source: (ITU, 2019) Reprinted from (Nichols R. K.-P., 2019)

RADAR / EW / Range Equation

From Austin, we know that the upper frequency for a UAS RADAR signature is 0.03 m = 3 cm. This is approximately 10 GHz frequency. See Figure 3-25. RADAR is usually thought of in terms of **Frequency Bands**. See Figure 3-26 RADAR Bands and their Usage. These are consistent with the (Wolff, 2022) presentation.

Figure 3-26 RADAR Bands



Frequency Range	Wavelength Range	Band Name	Usage
3-30 MHz	10-100 m	HF	Coastal radar systems
30-300 MHz	1-10 m	VHF	Very long range
300-1000 MHz	0.3-1 m	UHF	Very long range
1-2 GHz	15-30 cm	L-band	Long range
2-4 GHz	7.5-15 cm	S-band	Terminal air traffic control, marine radar
4-8 GHz	3.75-7.5 cm	C-band	Satellite transponders, synthetic aperture radar
8-12 GHz	2.5-3.75 cm	X-band	Marine radar, weather, ground surveillance, synthetic aperture radar
12-18 GHz	1.67-2.5 cm	Ku-band	Satellite transponders
18-24 GHz	1.11-1.67 cm	K-band	Satellite transponders, radar guns, weather
24-40 GHz	0.75-1.11 cm	Ka-band	Mapping, surveillance

Sources: (ITU, 2019) (Wolff, 2022) Modified from Figure 8-3 in (Nichols R. K.-P., 2019)

Radio propagation theory is key to understanding Space Electronic Warfare (EW) and its role in detecting a UAS approaching a target. If we understand how radio signals propagate, we can then intercept, jam, spoof or protect in a logical progression. (Adamy D. -0., 2015) [13] (Nichols R. K., 2020)

RADAR is Radio Detection and Ranging. It uses radio waves and their propagation in the EMS to determine the battlespace elements for an approaching

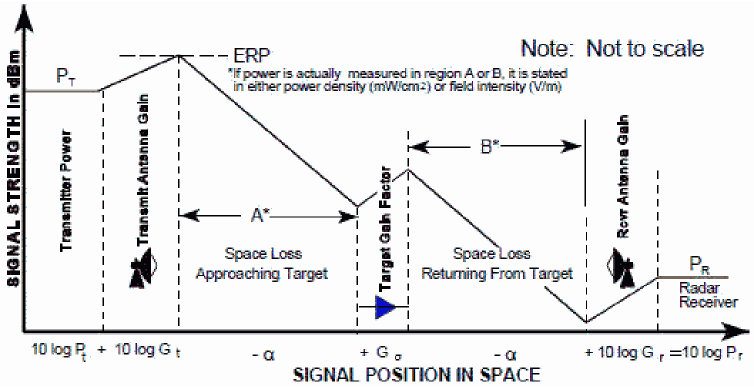
aircraft, UAS, ship, submarine, or any moving vehicle. We are only interested in two equations to understand the RADAR (radio) signature of a UAS. They are the link equation and the RADAR Range Equation; both are presented without derivation. "*The operation of every type of RADAR, military communications, signals intelligence, and the jamming system can be analyzed in terms of individual communications links." (Adamy D. -0., 2015)* A Link includes one radiation source, one receiving device, and all events to the electromagnetic energy as it travels from source to receiver. (Adamy D. -0., 2015) (Adamy D. L., Space Electronic Warfare, 2021)

Sources and receivers can take on many forms. When a radar pulse reflects off the skin of a UAS or airplane, the reflecting mechanism is a transmitter. It obeys the same laws that apply to a walky-talky when pushing the transmit button. Yet there is no power source and no circuitry to fore reflection. (Adamy D.-9. , 1998)

One–Way Link Equation

The basic communication link, known as a **one-way link**, consists of a transmitter, receiver, transmitting and receiving antennas, and propagation losses between the two antennas along the path. (Adamy D. L., Space Electronic Warfare, 2021) See Figure 3-27 Path Through One-Way Link.

Figure 3-27 Path Through One-Way Link



Sources: (Adamy D. L., Space Electronic Warfare, 2021)

The diagram shows signal strength in dBm and increases and decreases of signal strength in dB. Figure 3-27 shows the Line-of-Sight link. The transmitter and receivers can electronically see each other. However, there are interferences/ exceptions. The link must not be too close to water, land, severe weather, or asymmetric non-line-of-sight propagation factors. To calculate the received signal level (in dBm), add the transmitting antenna gain (in dB), subtract the link losses (in dB), and add the receiving antenna gain (in dB) to the transmitter power (in dBm).

(Adamy D. L., Space Electronic Warfare, 2021)

A simple example of the link equation in dB format is:

Transmitter Power (1 Watt) = + 30 dBm

Transmitter Antenna Gain = +10 dB

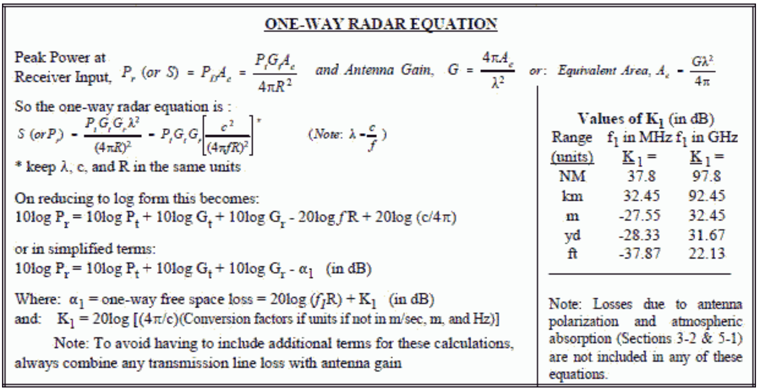
Spreading loss = 100 dB

Atmospheric loss = 2 dB

Receiving Antenna Gain = +3 dB

Received Power = 30 dBm + 10 dB – 100 dB – 2 dB +3 dB = – 59 dBm (Adamy D.-9. , 1998)

Figure 3-28 One–Way RADAR Equation



ONE-WAY RADAR EQUATION

Peak Power at Receiver Input, P_r (or S) $= P_{D}A_e = \frac{P_t G_t A_e}{4\pi R^2}$ and Antenna Gain, $G = \frac{4\pi A_e}{\lambda^2}$ or: Equivalent Area, $A_e = \frac{G\lambda^2}{4\pi}$

So the one-way radar equation is :

$$S \ (or\, P_r) = \frac{P_t G_t G_r \lambda^2}{(4\pi R)^2} = P_t G_t G_r \left[\frac{c^2}{(4\pi f R)^2}\right]^* \qquad (Note: \lambda = \frac{c}{f})$$

* keep λ, c, and R in the same units

On reducing to log form this becomes:

$10\log P_r = 10\log P_t + 10\log G_t + 10\log G_r - 20\log fR + 20\log (c/4\pi)$

or in simplified terms:

$10\log P_r = 10\log P_t + 10\log G_t + 10\log G_r - \alpha_1$ (in dB)

Where: α_1 = one-way free space loss = $20\log (f_1 R) + K_1$ (in dB)

and: $K_1 = 20\log [(4\pi/c)$(Conversion factors if units if not in m/sec, m, and Hz)]

Note: To avoid having to include additional terms for these calculations, always combine any transmission line loss with antenna gain

Values of K_1 (in dB)

Range (units)	f_1 in MHz K_1 =	f_1 in GHz K_1 =
NM	37.8	97.8
km	32.45	92.45
m	-27.55	32.45
yd	-28.33	31.67
ft	-37.87	22.13

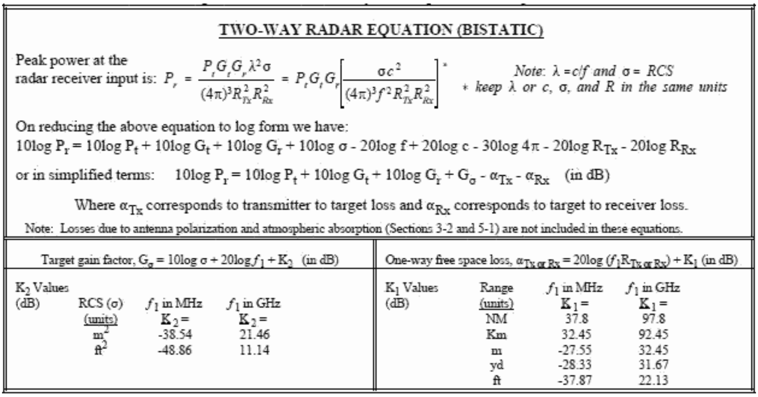
Note: Losses due to antenna polarization and atmospheric absorption (Sections 3-2 & 5-1) are not included in any of these equations.

Source: Wikipedia RADAR Images

Effective Range

What is the maximum range that a RADAR can “see” a UAS in any form: individual, group, team, or Swarm? The RADAR range equations can estimate the ***maximum distance to detect a UAS***. The smaller the UAS, the less reflective area is present to “return “a radar pulse back to its transmitter source. Figures 3-28 and 3-29 demonstrate the one-way and two-way (return trip) for determining the maximum range of a RADAR unit. The received power is equal to receiver sensitivity at the maximum link range. Receiver sensitivity is the smallest signal (lowest power strength) it can receive and still provide the specified output. (Adamy D. , EW 101 A First Course in Electronic Warfare, 2001)

Figure 3-29 Two Way RADAR Equation (Bi-Static)



TWO-WAY RADAR EQUATION (BISTATIC)

Peak power at the radar receiver input is: $P_r = \frac{P_t G_t G_r \lambda^2 \sigma}{(4\pi)^3 R_{Tx}^2 R_{Rx}^2} = P_t G_t G_r \left[\frac{\sigma c^2}{(4\pi)^3 f^2 R_{Tx}^2 R_{Rx}^2}\right]^*$

Note: $\lambda = c/f$ and σ = RCS

* keep λ or c, σ, and R in the same units

On reducing the above equation to log form we have:

$10\log P_r = 10\log P_t + 10\log G_t + 10\log G_r + 10\log \sigma - 20\log f + 20\log c - 30\log 4\pi - 20\log R_{Tx} - 20\log R_{Rx}$

or in simplified terms: $10\log P_r = 10\log P_t + 10\log G_t + 10\log G_r + G_\sigma - \alpha_{Tx} - \alpha_{Rx}$ (in dB)

Where α_{Tx} corresponds to transmitter to target loss and α_{Rx} corresponds to target to receiver loss.

Note: Losses due to antenna polarization and atmospheric absorption (Sections 3-2 and 5-1) are not included in these equations.

Target gain factor, $G_\sigma = 10\log \sigma + 20\log f_1 + K_2$ (in dB)

K_2 Values (dB) RCS (σ) (units)	f_1 in MHz K_2 =	f_1 in GHz K_2 =
m^2	-38.54	21.46
ft^2	-48.86	11.14

One-way free space loss, $\alpha_{Tx\ or\ Rx} = 20\log (f_1 R_{Tx\ or\ Rx}) + K_1$ (in dB)

K_1 Values (dB) Range (units)	f_1 in MHz K_1 =	f_1 in GHz K_1 =
NM	37.8	97.8
Km	32.45	92.45
m	-27.55	32.45
yd	-28.33	31.67
ft	-37.87	22.13

Source: Wikipedia Two-Way RADAR Range Equation images

If the received power level is at least equal to the receiver's sensitivity, communication takes place over the link. The amount of design *signal delta* over the minimum receiver sensitivity is called the margin. Figures 3-28 and 3-29 show the derivations (in normal and dB forms) of the RADAR Ranging Equations for limited environments. Other forms of the basic RADAR Ranging Equation, derivations, definition of terms, and examples of radar units for surveillance, tracking, and jamming applications can be found in Toomay's simplified reference. (Toomay, 1982) Readers interested in the RADAR units for mariners (picking up a hostile UAS over a ship) can refer to Monahan's (Monahan, 2004) or Burch's references. (Burch, 2015) Detailed RADAR equations in terms of orbital geometry and spherical relationships are found in (Adamy D. L., Space Electronic Warfare, 2021)

Example

Given the operating frequency of 100 MHz, the atmospheric and normal terrestrial losses are minimal. Assume the transmitter output power, Pt = 10 watts. [About double the normal marine VHF set.] The transmitting gain antenna, GT, is +10dB, the receiving antenna gain, GR, is +3 dB, and the design receiver sensitivity, Sens = – 65 dBm. {If we find that the received power level (say -59 dBm is at least equal to the sensitivity, then the communication takes place. The margin in this example would be 6 dB higher}. Assume line-of-sight between the two antennas. Calculate the maximum range we can see to the hostile UAS, not using Stealth techniques to reduce the radar visibility. Let PR = received power in dBm. Let d = distance in km. Setting Sens = PR = -65 dBm. Convert to dB math. Plug in the values and solve for 20 log (d). [Logs are base 10, not base e}

$$Sens = -65dBm = P_R = P_T = G_T - 32.4 - 20\log(f) - 20\log(d) + G_R$$

$$20\log(d) = P_T + G_T - 32.4 - 20\log(f) + G_R - Sens$$

And

$$P_T = 10W = +40dBm, G_T = 10dB, G_R = +3dB, [20\log(f = 100] = +40dB$$

$$20\log(d) = +40 + 10 - 32.4 - 40 + 3 + 65 = 45.6$$

$$D = antilog(20\log(d))$$

$$D = antilog(20\log(d)/20) = Antilog(45.6/20) = Antilog2.28 = 190.54km = 118.6miles$$

We can see the UAS (multiple with a bead on the leader) at 119 miles from our radar transmitter.

We have come full circle back to the question of designing a UAS for stealth and to get closer to the target. (Nichols R. K.-P., 2019) Discuss detailed detectability, stealth, and acoustic, visual, thermal, and RADAR/radio signature reductions. We return to Space.

Propagation Loss Models

The one-way link equation gives the received power PR in terms of the other link components (in decibel units). It is:

$$P_R = P_T + G_T - L + G_R$$

Eq. 3-16

Where:

P_R – received signal power in dBm

P_T – transmitter output power in dBm

G_T – transmitter antenna gain in dBm

L – link losses from all causes as a positive number in dBm

G_R – receiver antenna gain in dBm

In linear (nondecibel units), this formula is:

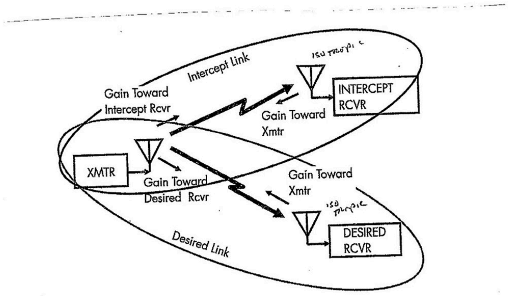
$$P_R = (P_T G_T G_R)/L$$

Eq. 3-17

It is assumed that all link losses from propagation are between isotropic antennas (unity gain, 0-dB gain). (Adamy D. L., Space Electronic Warfare, 2021)

When a communication signal is intercepted, there are two links to consider: the transmitter to intercept the receiver link and the transmitter to desired receiver link. Refer to Figure 3-30.

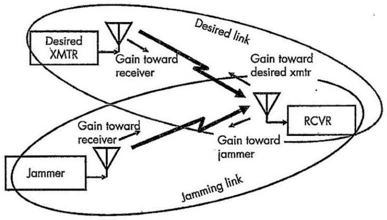
Figure 3-30 Intercepted Communication Signal



Source: Reprinted from Figure 4-3 courtesy of (Adamy D. L., Space Electronic Warfare, 2021)

When a communication signal is jammed or spoofed, there is a link from the desired transmitter to the receiver and a link from a jammer or spoofer to the receiver. (Adamy D. L., Space Electronic Warfare, 2021) [14] Refer to 3-X

Figure 3-31 Jammed / Spoofed Communications Signal



Source: Reprinted from Figure 4-4 courtesy of (Adamy D. L., Space Electronic Warfare, 2021)

Propagation Loss Models

(Adamy D. L., Space Electronic Warfare, 2021) presents several propagation loss models within the atmosphere based on a clear or obstructed path and Fresnel zone distance. Refer to Table 3- These models are LOS (free space loss or spreading loss), two-ray propagation for phase cancellation, and KED (knife-edge loss). Adamy also considers atmospheric, rain, and fog losses.

Table 3-4 Selection of Appropriate Propagation Loss Model

Clear propagation path	Low frequency, wide beams near the ground	Link longer than Fresnel-zone distance	Use two-ray model
		Link shorter than Fresnel-zone distance	Use LOS model
	Hight-frequency, narrow-beams	Far from ground	Use LOS model
Propagation path obstructed by terrain.		Calculate additional loss from the KED model	

Source: Reprinted from Table 4.1 courtesy of (Adamy D. L., Space Electronic Warfare, 2021)

When radio transmission and propagation is to or from an Earth satellite, there are special considerations due to the nature of space, losses due to extreme long range, and the geometry of the links. The formula gives the *received power at the receiver*:

$$P_R = ERP - L + G_R$$

Eq. 3-18

Where:

P_R – received signal power in dBm

ERP– the effective radiated power, in dBm

L – losses from all causes between transmitting and receiving antennas in dBm

G_R – receiver antenna gain in dBm

The total path loss to or from a satellite includes LOS loss, atmospheric loss, antenna misalignment loss, polarization loss, and rain loss. (Adamy D. L., Space Electronic Warfare, 2021) [15]

Satellite Links

Satellites are, by nature, remote from the ground and must be connected by links. Uplink and downlink geometry is a complex set of calculations related to satellite position, North Pole, longitudes, latitudes, sub-vehicle points **(SVP)**, Center of Earth, ground station, Equator, Greenwich Meridian, Azimuth to the ground station, satellite movement in the horizontal plane, satellite payloads, radar bore sights, and hostile target detection, all wrapped up in complex orbital and spherical geometry calculations. (Adamy D. L., Space Electronic Warfare, 2021) spends four challenging chapters on this subject. We will assume that Keplerian ephemeris, Napier's rules, and the Laws of Sines, Cosines for sides and angles haven't been overruled by Executive Order (EO), which leads us to a discussion of Link vulnerability to EW. [16]

Link Vulnerability to EW: Space-Related Losses, Intercept (Jamming) & Spoofing

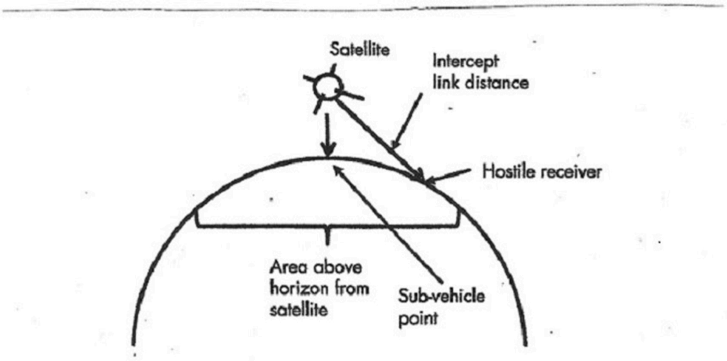
Satellites are from Earth but present excellent loss of signal **(LOS)** from a large part of the Earth's surface. They are highly susceptible to three kinds of hostile activity. Signals from satellites can be intercepted, and strong hostile transmissions can be jamming signals, interfering with uplink or downlink signals to prevent proper reception. They can also be spoofing signals that cause the satellite to interpret them as functional commands that are harmful or transmit useless positional data. (Adamy D. L., Space Electronic Warfare, 2021) This section and the following will focus heavily on spoofing and the downlink interpretation of false signals in GNSS/GPS/ADS-B receivers.

Figure 3-32 shows a successful intercept of a satellite signal. Successful intercept gives the hostile receiver a high-quality signal to recover important information. A ground-based jammer operating against a satellite uplink transmits to the link receiver in the satellite. The ground station and the jammer must be above the horizon from the satellite. The received signals are intended for the receiver in the satellite control station (GCS) or other authorized receiver. There is a separate link to any hostile receiver. (Adamy D. L., EW 103: Tactical Battlefield Communications Electronic Warfare, 2009) (Adamy D. L., Space Electronic Warfare, 2021)

Successful spoofing places a strong enough signal into a satellite link receiver to cause the satellite or its payload to accept it as a valid command. Command spoofing could cause the satellite to perform a maneuver that ends the mission or put the payload in an unusable state. (Adamy D. L., Space Electronic Warfare, 2021)

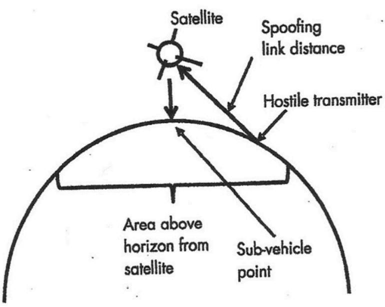
Figure 3-33 shows a successful spoofing of a satellite signal. A ground-based spoofer operating against a satellite uplink transmits to the link receiver in the satellite. The ground station and the jammer must be above the horizon from the satellite.[17]

Figure 3-32 Intercept



Source: Figure 3-32 Modified from Figure 7.1 Courtesy of (Adamy D. L., Space Electronic Warfare, 2021)

Figure 3-33 Spoofing



Source: Figure 3-33 Modified from Figure 7.2 Courtesy of (Adamy D. L., Space Electronic Warfare, 2021)

Space-Related Link Losses

Any attack on a satellite link may involve single or multiple links. Each link is subject to transmission losses, including LOS, atmospheric, antenna misalignment, rain, and polarization losses.

An *intercept link* is separate from the intended command and data links. It goes from the satellite's link transmitter (onboard or at GCS) to a hostile receiver. The quality of the intercept is judged by the Signal to Noise (S/N) ratio achieved in the hostile receiver. (Adamy D. L., Space Electronic Warfare, 2021)

A *spoofing link* goes from the hostile transmitter to a satellite link receiver. This receiver is generally on the satellite. The spoofing signal's purpose is to cause it to function improperly, but if the spoofer is in the GCS, the purpose is to invalidate the date – especially localization data. (Adamy D. L., EW 104: EW against a new generation of threats, 2015)

Jamming of any satellite link is communications jamming. Jamming effectiveness is defined in terms of the *Jamming-to-Signal ratio (J/S)* that it causes. It is calculated from the following formula:

$$J/S = ERP_J - ERP_S - LOSS_J + LOSS_S + G_{RJ} - G_R$$

EQ. 3-19

Where:

J/S= jamming-to-signal ratio in decibels

ERP_J = effective radiated power (ERP) of jamming transmitter toward the target receiver in dBm

ERP_S = ERP of the desired signal toward the receiver in dBm

$LOSS_J$ = transmission loss from the jammer to target a receiver in dBm

$LOSS_S$ = transmission loss from transmitter to target a receiver in decibels

G_{RJ} = gain of receiving antenna in the direction of a jammer in decibels

G_R = gain of receiving antenna toward transmitter in decibels

The last two terms cancel each other if the target receiver has a non-directional antenna.

(Adamy D. L., Space Electronic Warfare, 2021) in his textbook, he presents and solves detailed examples of intercepting, jamming, and spoofing uplinks and downlinks.[18]

We now discuss spoofing in detail and its implications concerning navigation and location services. We will focus on a particularly promising anti-spoofing technology known as ECD.

GPS/GNSS/ADS-B SPOOFING

Two issues are discussed: 1) GPS spoofing detection and mitigation for GNSS / GPS using the ECD algorithm, and 2) GPS spoofing of ADS-B systems.[19] **Recognize that 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.** 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**. But a much better technology is available to Detect, Mitigate and Recover Spoofed satellite signals –**

even those with a precursor Jamming attack. It is called ECD.

ECD: EICHELBERGER COLLECTIVE DETECTION

This section covers the brilliant value-added research by Dr. Manuel Eichelberger on the detection, mitigation, and recovery of GPS spoofed signals. (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019) ECD implementation and evaluation show that with some modifications, the robustness of collective detection (CD) can be exploited to mitigate spoofing attacks. (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019) shows that multiple locations, including the actual one, can be recovered from scenarios where several signals are present. [20] [21]

ECD does not track signals. It works with signal snapshots. It is suitable for snapshot receivers, a new low-power GPS receiver class. (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. In general, 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.

Qualitative Risk Assessment Opinion based on FAA SRM Reference Guidelines (FAA, 2018) (FAA, 2021) (FAA, 2019)

After reviewing data, papers, and reports regarding the Severity, Likelihood, and Risks associated with spoofing GNSS/ GPS signals, there are two schools of thought. Before 2015, transmitting fake GNSS/GPS signals was a qualitative – unlikely [Table 3-C *Remote*] (FAA, 2018) risk and a niche issue. After 2015, the world changed considerably. Low-cost SDR RF signal generators combined with an awareness that spoofing was a powerful disruption technique and availability of COTs precipitated a sharp increase in incidents ranging from amateur to researcher generated to professional crook to the nation-state. The Ling and Qing demonstration of the SDR signal spoofer at DEFCON 2015 plus the 2013 spoofing of the 213′ motor yacht White Rose of Drach's by Humphreys' team set the stage for significant spoofing incidents to follow. (T.E. Humphrees, 2008)

Two organizations report the spoofing risks quite differently. These are the FAA and US Navy. The FAA is concerned with aircraft and UAS. It considers the severity of signal spoofing threat to be *Major* [Table 2 -3] (FAA, 2018) because of substantial damage to the aircraft vehicle and physical distress or injuries to persons *without loss of life*. Depending on circumstances, FAA sees the Likelihood as *Probable* – especially for UAS. [Table 4-B]. (FAA, 2018) The US Navy sees the spoofing threat quite differently. It considered the spate of incidents in 2016 in Moscow, the Black Sea in 2017, the Port of Shanghai in 2019, and the loss of 20 sailors in the South China Seas in 2017 involving incidents with the USS McCain and USS Fitzgerald colliding with commercial vessels Alnic MC and ACX. The US Navy sees the spoofing severity as *Catastrophic* [Table 2-1] because of multiple fatalities, loss, and/or severe damage to ships and defensive aircraft. Further, the US Navy's view appears to be that the Likelihood is *Probable* [Table 3-B]. (FAA, 2018) Depending on the view, spoofing can be considered at Risk Levels *Yellow or Red* [*Medium to High*], i.e., medium acceptable risk to unacceptable risk. This is based on the number of researchers and analysts studying / reporting/ conventions on GNSS/GPS spoofing countermeasures since 2018.

Using FAA SRM Guidelines, signal spoofing on UAS /ADS-B systems is above average likelihood (***probable -> frequent***) and **severe** [*Yellow bordering on Red or in terms of the severity qualitative scale three -> 2*]. (FAA, 2019)

Risk Assessment Spoofing Classes

Risk Assessment for spoofing threats into four classifications: *Part 107 Operations, BVLOS, Urban Areas, and*

Near Airports. Because of Federal guidelines and licensing requirements, Part 107 Operations specifies a near pristine Risk level or The Best-Case Scenario. Because the UAS is not limited to a specified space and may cross the visual horizon, BVLOS represents an elevated UAS spoofing threat and risk. Urban area operations represent a difficult case for spoofing with increased Severity of consequences—urban areas present difficulty in enacting countermeasure to a spoofing attack. Humans and equipment are at risk. Near Airports represents the Worst-Case scenario with the highest Severity and Likelihood Probability. There are globally reported UAS – aircraft and UAS – ship spoofing incidents that present serious consequences to human life. In all four classifications, spoofing is **Probable**. **Both FAA and USN consider spoofing a real and escalating threat**. **It no longer represents a remote or niche possibility.** (Kahn & M. Mohsin, 2021) (Nichols R. K., 2020) (M.L. Psiaki & Humphreys, 2016)

Dependence on GPS and vulnerability [22]

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 incorporated into many applications (aircraft, ship, car /truck navigation; train routing and control; cellular network, stock market, and power grid synchronization) that make a "rich" target for spoofing a receiver's 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 underway in the US since 2020. The A/C determines 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. 2017 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 for exchanging communication data packets between ground antennas and mobile handsets in the same network cell. Also, all neighboring cells of the network 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 at all 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 the signal power and delays for each satellite individually. (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019)

Before discussing E*CD – 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. [23]

GPS SIGNAL

The GPS system consists of control, space, and user segments. The space segment contains the 24 orbiting satellites. The network monitor stations, GCS, and antennas comprise the control segment. The third and most important are the receivers, which comprise 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) Signals from different satellites may be distinguished and extracted from background noise using code division multiple access protocols (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.[24] (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. [25] GPS receiver locates the set of available satellites. This is achieved by correlating the received signal with the satellites'. 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 start to 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. ToFs 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. [26] 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. [27]

A-GPS (Assisted GPS) – Reducing the Start-Up Time

Assisted GPS (A-GPS) drastically reduces the start-up time by fetching the navigation data over the Internet, commonly by connecting via a cellular network. Data transmission over cellular networks is faster than decoding 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 can be estimated along with their expected Doppler shifts. With A-GPS, the receiver still needs to extract the HOW timestamps from the signal. However, these timestamps are transmitted every six seconds, which translates to how long it takes the A-GPS receiver 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 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 directly related to the sub-milliseconds unambiguously; the deviation may be no more than 150 km from the correct values. [28] [29] 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. [30] 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 ranges to the satellite modulo 1 ms, 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 combines all the available information and decides only at the end of the computation. [31] 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* 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 ones. (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019) ECD achieves median errors under 19 m on the TEXBAT dataset, which is the de facto reference dataset for testing GPS anti-spoofing algorithms. (Ranganathan & al., 2016) (Wesson, 2014) The ECD approach uses only a few milliseconds of raw GPS signals, so-called snapshots, for each location fix. This enables offloading of the computation into the Cloud, which allows knowledge of observed attacks. [32] 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

Because of the overwhelming dependence on GPS in every sector, ranging from civilian to military, researchers have been trying desperately to find a complete solution to the spoofing threat. To understand that ECD (following sections) is a brilliant departure from past efforts, it is necessary to briefly cover the prevailing common wisdom. Haider and Khalid 2016 published an adequate survey of spoofing countermeasures up through the end of 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 towards the GPS receiver. It was performed successfully by Los Almos 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 and detection do not synchronize simulator signals is easy.

In the *intermediate spoofing attack*, the spoofing component consists of a GPS receiver to receiver 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 using an IMU. (Humphreys & al., 2008)

In *sophisticated spoofing attacks*, multiple receiver-spoofer devices target the GPS receiver from different angles and directions. In this scenario, the angle-of-attack defense against GPS spoofing in which the reception angle is monitored to detect spoofing fails. The only known defense successful against such an attack is cryptographic authentication. (Humphreys & al., 2008) [33]

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)

(Haider & Khalid, 2016), present findings based on six innovative research papers that cover spoofing countermeasures. These are:

1. Multi-test Detection and Protection Algorithm against Spoofing Attacks on GNSS Receivers (Jovanovic & Botteron, 2014)
2. GPS Spoofing Countermeasures (Warner & Johnston, 2003)
3. An Asymmetric Security Mechanism for Navigation Signals (Kuhn, 2015)
4. A Cross-layer defense mechanism against GPS spoofing attacks on PMUs in Smart Grid (Fan & al., 2015)
5. Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing (Magiera & Katulski, 2015)
6. GPS Spoofing Detection via Dual-Receiver Correlation of Military Signals(Psiaki & al., 2013)

A-F Analysis (Haider & Khalid, 2016)

(Haider & Khalid, 2016) present two tables that show the criteria used to evaluate each technique to find the most effective GPS spoofing CM and present the analysis of A-F with specific criteria. From their tables, 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 protect against sophisticated 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!

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). Historical spoofing research focuses primarily on the detection of singular SPS source attacks. ECD's hallmark is to focus on mitigation, correction, and recovery attending to multiple spoofing signals on multiple satellite attack surfaces.

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 vast 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. The tide will turn.[34]

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 authentic 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 by a moving receiver. (M.L. Psiaki & Humphreys, 2016) For signal erasure to be feasible, the spoofer needs to know the receiver location more accurately than the GPS L1 wavelength, which is 19 cm. 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) In all other types of spoofing attacks, including signal replay and multiple transmission antenna implementations, the original signals are still present, 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 [35]

ECD uses an iterative signal damping technique with spoofing signals similar to SIC. SIC removes the strongest received signals one by one to find the weaker ones that have 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 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 signal-to-noise ratio (SNR) of the satellite signal acquisition results. ECD algorithms achieve a better SNR than classical receivers and can 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 the authentic signals. [36] (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019)

There is a more powerful and subtle attack on the jammed signal. The spoofer can send a set of satellite signals with adjusted power levels and synchronized 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*. In such an attack, the original and counterfeit signals are nearly identical 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 all the 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)

Regarding the 4th point, Spoofing and multi-path 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 a consistent localization solution at the receiver. To detect spoofing and multipath signals, classical receivers can be modified to track an arbitrary number of signals per satellite instead of only one. (S.A.Shaukat & al., 2016) In such a receiver, the set of authentic signals – one signal from each satellite – would have to be correctly identified. 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 overlapping (synced) signals for some location hypotheses do not accumulate a significant likelihood. 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

Compared to exhaustively enumerating all the location hypotheses in the search space, a fast CD leveraging branch and bound algorithm is employed to reduce the computational load. (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 discusses acquisition, receiver implementation, and experiments using the TEXBAT database. [37] [38]

One of the key points under the receiver implementation concerns the correlation of C/A codes. [39]

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 highly depends 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)[40]

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 [41]

Strohmeier et al. (Strohmeier, 2015) and Nichols et al. (Nichols R. K.-P., 2019) have both outlined a set of security requirements for piloted aircraft and unmanned aircraft, respectively. Here are the combined security requirements for the ADS-B system in sync with the standard information security paradigm of the CIA:

- Data integrity [42]

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 be able to 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 actual owner (correct a/c) of the message.

- 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 information 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) [43]

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 that no cryptographic mechanism is implemented in the ADS-B protocol. (Airports Authority of India, 2014) [44]

ADS-B COTS

ADS-B receivers are available in COTS at affordable prices. The receiver can track ADS-B capable a/c flying within a specific range of the receiver. The number of ADS-B tracking gadgets for all media is growing yearly. They can be used to hack the systems on UAS. (Nichols R. K.-P., 2019)

Shared Data

Due to the COTS availability of ADS-B receivers, private and public parties share real-time air traffic information on a/c on the Internet. Some 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)

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) on the a/c. Therefore, ADS-B aircraft surveillance is dependent on 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 on-board 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 vulnerability of the system*. **The system inherits 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 with the intention to harm the a/c. This can be done with more sophisticated traffic and signal analysis using available sources such as Mode S and ASDS-B capable open-source GNU Radio modules or SDR. Eavesdropping is a violation of confidentiality and compromises system security. (Busyairah, 2019)

Data-Link Jamming

Data-link jamming is an act of deliberate / non-deliberate blocking, jamming, or causing interference in wireless communications. (R.K. Nichols & Lekkas, 2002) Deliberate jamming using a radio jammer device aims to disrupt information flow (message sending /receiving) between users within a wireless network. 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 critical safety 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) [45] Not only is ADS-B prone to jamming, but so is SSR. (Adamy D. , EW 101: A First Course in Electronic Warfare, 2001)[46]

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 range of the ground station.

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 WAM/MLAT and SSR interrogation. 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).[47] 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. [48]

ADS-B Signal Spoofing

ADS-B signal spoofing attempts to deceive an ADS-B receiver by broadcasting fake ADS-B signals structured to 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 of 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). [49]

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 be made to 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 and 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.

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) Ochin & 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 spoofers; [50] GNSS interference modalities; complementary countermeasures like INS; [51] GNSS jamming techniques; GNSS meaconing; and detailed sections on cloud-based GNSS positioning. Modern satellite navigation uses NO-Request range measurements between the navigation satellite and the user. The information about the satellite coordinates given to the user is included in the navigation signal. The way of 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 proceeds to mathematically define 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 daily. The accessories necessary for the manufacture of systems for GNSS "jamming" and "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

Space is the new frontier of electronic warfare (EW), intelligence, and reconnaissance. Signals are the soul of EMS. Space is also the place to view the earth in large "earth traces." These views can help military and agricultural planners make better decisions on protecting the United States and managing (increase) global food supply, land usage, irrigation, and health. The same information for diametrically different uses. Chapter perused:

- Key definitions in EW, satellite systems, and ECD countermeasures
- A look at space calculations and satellite threats using plane and spherical trigonometry to explain orbital mechanics
- A brief review of EMS, signals, RADAR, Acoustic, and UAS Stealth principles,
- Signals to/from satellites and their vulnerabilities to Interception, Jamming, and Spoofing,
- The promising ECD technology countermeasure to spoofing can detect, mitigate, and recover fake and genuine signals. All ADS-B vulnerabilities and threats mentioned in Chapter 3 are amenable to ECD mitigation if sufficient computing horsepower is available.

Chapter 3 should prepare students for deeper dives into the fascinating world of space technologies.

References

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/: https://www.gps.gov/systems/gps/performance/accuracy/#problems

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

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

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

Adamy, D. L. (2004). *EW 102 ASecond Course in Electronic Warfare.* Norwood, MA: 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*.

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: https://www.microsemi.com/document-portal/doc_download/133615-timing-sync-for-lte-tdd-lte-a-mobile-networks

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

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). Pittsburg, PA: IPSN.

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

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 Detection. *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

CYFO: A, M. (2018, Nov 4). *CYFO Why Satellite Orbits Look Like Waves on Maps.* Retrieved from https://www.youtube.com: https://www.youtube.com/watch?v=JyfEffMrglI

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.

Data: USGS/NASA Landsat. (2021). *Wipe-shows-water-loss-in-Lake-Mead-2000-2021.-Two-versions.* Retrieved from https://stock.adobe.com/video/: https://stock.adobe.com/video/Wipe-shows-water-loss-in-Lake-Mead-2000-2021.-Two-versions.-Data%3A-USGS%2FNASA-/454218719?as_campaign=TinEye&as_content=tineye_match&epi1=454218719&tduid=3ccffe944195c552a79f6ba937c7a9c9&as_channel=affiliate&as_campclass=red

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

FAA. (2018, April 27). *FAA Safety Management.* Retrieved from https://www.faa.gov/: https://www.faa.gov/regulations_policies/handbooks_manuals/aviation/risk_management/media/20180427_FAASRMGuidance5StepProcess_signed_508.pdf

FAA. (2019). *ATO-SMS-Manual.* Retrieved from https://www.faa.gov/: https://www.faa.gov/air_traffic/publications/media/ATO-SMS-Manual.pdf

FAA. (2021). *SRM Safety Management Quick Reference Guide.* Washington: FAA Manual Sections 3.5.4 & ff.

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.

Fletcher, H. a. (1933). Loudness, its definition, measurement, and calculation. *Journal of the Acoustical Society of America*, 5, 82-108.

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.

Global Security.Org. (2022, July 16). *Chapter 3 Intelligence, Surveillance, and Reconnaissance Planning.* Retrieved from https://www.globalsecurity.org/: https://www.globalsecurity.org/military/library/policy/army/fm/3-21-31/c03.htm

Goward, D. (April 21, 2020). GPS circle spoofing was discovered in Iran. *GPS World*.

GPSPATRON. (2022, July 9). *GNSS Interference in wildlife.* Retrieved from GPSPATRON.com: https://GPSPATRON.com/gnss-interference-from-wildlife/

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.

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

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

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/

ITU. (2019, July 19). *ARTICLE 2 – Nomenclature – Section I – Frequency and Wavelength Bands.* Retrieved from ITU Radio Communication Edition 2008: https://web.archive.org/web/20111001005059/ http://life.itu.int/radioclub/rr/art02.htm

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.

Kahn, S. Z., & M. Mohsin, &. W. (2021, May 7). On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions. *Comp Sci*, p. 507 ff.

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

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.

MIT R&D. (2022, July 16). *ISR SYSTEMS AND TECHNOLOGY.* Retrieved from https://www.ll.mit.edu/r-d/isr-systems-and-technology: https://www.ll.mit.edu/r-d/isr-systems-and-technology

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

Nichols, R. K. (2020). *Counter Unmanned Aircraft Systems*

Technologies & Operations. Manhattan, KS: www.newprairiepress.org/ebooks/31.

Nichols, R. K., & Sincavage, S. M. (2022). *DRONE DELIVERY OF CBNRECy – DEW WEAPONS Emerging Threats of Mini-Weapons of Mass Destruction and Disruption (WMDD).* Manhattan, KS: New Prairie Press #46.

Nichols, R. K.-P. (2019). *Unmanned Aircraft Systems in the Cyber Domain, 2nd Edition.* Manhattan, KS: 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.

Ochin, E., & Lemieszewski, &. L. (2021). Chapter 3 Security of GNSS. In G. P. PETROPOULOS, & &. P. SRIVASTAVA, *GPS and GNSS Technology in the Geosciences* (pp. 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*, pp. 223-234.

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.

Ronfeldt, J. A. (1966). *The Advent of Netwar.* Santa Monica, CA: RAND.

Rosen, S. (2011). *Signals and Systems for Speech and Hearing (2nd ed.).* New York City: BRILL. p. 163.

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.

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

Strohmeier, M. (2015). On the security of the automatic dependent surveillance-broadcast protocol. *IEEE Communications Surveys & Tutorials*, 17:1066-1087.

A 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.

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

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

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/sysytems/gps

Warner, J. S., & Johnston, R. (2003). GPS Spoofing Countermeasures. *Journ of Security Administration*. Retrieved

from https://www.semanticscholar.org/paper/GPS-Spoofing-Countermeasures-Warner-Johnston/36e17f723bff8d429aca4714abe54500a9edaa49

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

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

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

Wolff, C. (2022). *Radar and Electronic Warfare Pocket Guide.* Munich, Germany: Rhode & Schwarz.

1026. Ng & Gao, G. (2016). Mitigating jamming & meaconing attacks using direct GPS positioning. *In Position, Location & Navigation Symposium (PLANS) IEEE/ION*, 1021-1026.

Endnotes

[1] Definitions taken from (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019), (Wolff, 2022), (Nichols R. K.-P., 2019) and (Nichols & Sincavage, 2022)

[2] Since 1998, Christian Wolff has maintained the educational website www.radartutorial.eu

[3] ISR defined from the USA Army POV only.

[4] Ớ = Order of magnitude; dot = dot product for vectors

[5] All these systems are discussed in Chapter 2 of (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019)

[6] Each satellite has a unique 1023-bit PRN sequence, plus some current navigation data, D. Each bit is repeated 20 times for better robustness. Navigation data rate is limited to 50 bit / s. This also limits sending timestamps every 6 seconds, 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.

[7] Professor Adamy has about 50+ years of experience and as a SME has written an accelerated set of textbooks EW 101-104

to define the entire EW playing field. The author had the pleasure of studying under this accomplished researcher, practitioner, lecturer, and author.

[8] This chapter is a testament to (Adamy D. L., Space Electronic Warfare, 2021) work. It is impossible to summarize his experience and knowledge, so we have used sections of his technical teachings for our students.

[9] To multiply linear numbers, add their logarithms; to divide linear numbers, subtract their logarithms; to raise a linear number to the *n*th power, multiply its logarithm by n; and to take the *n*th root of a linear number, divide its logarithm by n.

[10] UAS and UAV are used synonymously. V=vehicle.

[11] Spoofing is added to the table by author based on his work with ECD and inferred from (Adamy D. L., EW 104: EW against a new generation of threats, 2015) , (Adamy D. L., Space Electronic Warfare, 2021) & (Nichols & Sincavage, 2022)

[12] Some useful factors: 1 Terahertz (THz) = 10**3 GHz = 10**6 MHz = 10 **12 Hz; and

1 nm = 10 (**-3) um (micron-meter) = 10 (**-6) mm (millimeter)= 10(**-9) m

1-micron, um = m / 1000000 (1 millionth of a meter).

[13] Adamy has written five stellar references on EW, use of dB

logarithmic mathematics to solve EW equations for strength, gains, losses, radars, interceptors, jamming technologies, current threats, defense systems and more for the reader to research and enjoy. (Adamy D. -0., 2015)

[14] Spoofing affects the same path as a jammer.

[15] (Adamy D. L., Space Electronic Warfare, 2021) covers all these losses in nauseating detail. From a ChE POV (ye author) they are a just a total system loss regardless of root causes. One number. EEs and RADAR engineers will find this statement heresy.

[16] Author sarcasm.

[17] Spoofing is often accompanied by a precursive jamming operation. (Nichols R. K., 2020)

[18] There are important numbers for space EW calculations: A solar day is 24 hours or 1440 minutes. The sideral day is 23.9349 hours or 1436.094 minutes. Kepler's third law is a3 = C x P2 where C= 36,355,285 km3 per min2 . Radius of earth is 6,371 km. The earth is proportionally a smooth sphere and can be assumed as a perfect sphere in orbital calculations. Synchronous satellite period is 23 hours and 56 minutes. The 12-hour satellite is 20,241 km high. Synchronous altitude is 35,873 km. Its range to the horizon is 41,348 km. The width of

the earth from a synchronous satellite is 17.38 degrees. These all make excellent bar bets.

[19] Aircraft signal transfer is not the only means to localize indoor signals. HAPs, WiFi, Ultrasound, Light, Bluetooth, RFID. Sensor fusion and GSM all have a place in the decision-making process.

[20] Experiments based on the TEXBAT database show that a wide variety of attacks can be mitigated. In the TEXBAT scenarios, an attacker can introduce a maximum error of 222 m and a median error under 19 m. This is less than a sixth of the maximum unnoticed location offset reported in previous work that only detects spoofing attacks. (Ranganathan & al., 2016)

[21] According to SPSPATRON.com, GNSS Spoofing in Anti-Drone Systems is the most common application of GNSS spoofing. The anti-drone system simulates the coordinates of the nearest airport. The commercial drone is either landing or trying to fly to the takeoff point. There are different usage scenarios here. Sometimes only GPS is spoofed, and the other constellations are blocked. Sometimes GLONASS + GPS are spoofed. There are also different scenarios in terms of the duration of use. Automatic systems generate a fake signal within minutes. Sometimes a spoofer is activated for many hours. (GPSPATRON, 2022) ECD can handle this and other forms of signal spoofing.

[22] The author translated part of (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019) reference from the original German.

[23] The author has nicknamed Dr. Manuel Eichelberger's brilliant doctorial research, ECD. ECD is Dr. Manuel Eichelberger's advanced implementation of CD to detect and mitigate spoofing attacks on GPS or ADS-B signals

[24] This is a key point. CD reduces this timestamping process significantly.

[25] Data is sent on a carrier frequency of 1575.42 MHz (IS-GPS-200G, 2013)

[26] GPS satellites operate on atomic frequency standard, the receivers are not synchronized to GPS time.

[27] Because the receiver must decode all that data, it has to continuously track and process the satellite signals, which translates to high energy consumption. Furthermore, the TTFF on startup cost the user both latency and power.

[28] The deviation is defined as the time offset multiplied by the speed of light plus the location distance.

[29] For those who insist on SI / metric, 1 km = ~ 0.62 mi (miles)

[30] Data bit flips can happen. The normal practice is 2 milliseconds of sample time.

[31] 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)

[32] Cloud offloading also makes ECD suitable for energy-constrained sensors.

[33] (Nichols & al., 2020) have argued the case for cryptographic authentication on civilian UAS /UUV and expanded the INFOSEC requirements.

[34] Author opinion.

[35] This is a key section to understanding the beauty of ECD. The entire SIC algorithm and ECD implications is found in detail in (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019) p81-ff.

[36] 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.

[37] See (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019) Sections 6.5 – 6.7 pages 84-94.

[38] 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 **V**, time discretization, averaging over likely hypotheses, hypothesis **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)

[39] This is accomplished in the acquisition stage of a GPS receiver. The received signals is correlated with the C/A codes.

[40] (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.

[41] 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]

[42] Please note the word “should.” Hackers just love this word.

[43] Wireless networks present few obstacles to access and can

easily be attacked by open-source software. (R.K. Nichols, 2020)

[44] This is still true in legacy systems. Newer implementations have additional protections. UAS systems are notoriously weak in terms of security.

[45] 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 subset of the larger problem.

[46] 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 D. , EW 101: A First Course in Electronic Warfare, 2001)

[47] This might have been true in 2011, however a decade of change, growth, cost-effective COTS, and state sponsored hackers says that this observation is severely dated. (Author comment)

[48] 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)

[49] This is a headache to say the least. Consider a SWARM

of 100 + UAS bursting onto the controller's screen at a busy airport.

[50] DIY – Do it yourself

[51] INS- an inertial navigation system is composed of motion sensors (accelerometer, gyrometer, and magnetometer) allowing determination of the absolute movement of a platform. Using this information and knowledge of the last position, it is possible using dead reckoning to provide an estimation of position, velocity, and time of the platform after spoofing or jamming detection.

4.

MANUFACTURING IN SPACE (JACKSON & JOSEPH)

Student Learning Objectives:

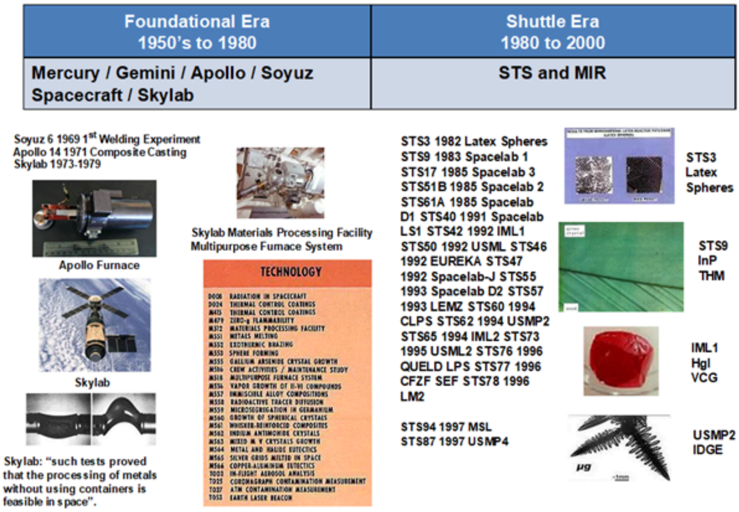
- The student will learn the potential of manufacturing in space, on Earth and on the International Space Station (ISS).
- The student will learn the potential of manufacturing replacement parts in space, recycling in space, printing spacecraft and use of resources on planetary surfaces.
- The student will learn the difference between circular economics and sustainability and the need for manufacturing in space as an application of circular economic principles.

Introduction

Manufacturing in space is becoming a strategic aspect of endeavor that aims to produce materials that cannot be manufactured on Earth for a variety of reasons and where their processing damages the Earth's environment. Prior missions to establish a scientific basis for manufacturing in space developed in the 1950s with the foundations of studying materials in microgravity environments commencing with the Mercury and Gemini programs progressing to welding and casting in space during the Apollo and Skylab era (Figure 4-1). The Space Shuttle and Mir enterprises progressed the initial work with the Spacelab and the International Space Station (ISS). The focus was on the processing of materials without containers, welding, and crystal formation (solidification), and in fact, all the characteristics needed to realize additive manufacturing as a process to be used in space (Volz 2014).

In recent years, a US government-led consortium known as 'America Makes' is fully supported by NASA (www.nasa.gov) and is creating initiatives associated with 'in-space manufacturing' with NASA leading the charge on all aspects of manufacturing in space (https://www.americamakes.us/). Parallel development of manufacturing in space is also occurring in the European Union (EU) as part of the strategic agenda of the EU focusing on additive manufacturing for the aerospace sector (http://www.rm-platform.com/).

Figure 4-1 Long Duration Microgravity Materials Science Research



Foundational Era 1950's to 1980	Shuttle Era 1980 to 2000
Mercury / Gemini / Apollo / Soyuz Spacecraft / Skylab	STS and MIR

Soyuz 6 1969 1st Welding Experiment
Apollo 14 1971 Composite Casting
Skylab 1973-1979

Apollo Furnace

Skylab

Skylab: "such tests proved that the processing of metals without using containers is feasible in space".

Skylab Materials Processing Facility
Multipurpose Furnace System

TECHNOLOGY

D008	RADIATION IN SPACECRAFT
D024	THERMAL CONTROL COATINGS
M415	THERMAL CONTROL COATINGS
M479	ZERO-g FLAMMABILITY
M512	MATERIALS PROCESSING FACILITY
M551	METALS MELTING
M552	EXOTHERMIC BRAZING
M553	SPHERE FORMING
M555	GALLIUM ARSENIDE CRYSTAL GROWTH
M516	CREW ACTIVITIES / MAINTENANCE STUDY
M518	MULTIPURPOSE FURNACE SYSTEM
M556	VAPOR GROWTH OF II-VI COMPOUNDS
M557	IMMISCIBLE ALLOY COMPOSITIONS
M558	RADIOACTIVE TRACER DIFFUSION
M559	MICROSEGREGATION IN GERMANIUM
M560	GROWTH OF SPHERICAL CRYSTALS
M561	WHISKER-REINFORCED COMPOSITES
M562	INDIUM ANTIMONIDE CRYSTALS
M563	MIXED III-V CRYSTALS GROWTH
M564	METAL AND HALIDE EUTECTICS
M565	SILVER GRIDS MELTED IN SPACE
M566	COPPER-ALUMINUM EUTECTICS
T003	IN-FLIGHT AEROSOL ANALYSIS
T025	CORONAGRAPH CONTAMINATION MEASUREMENT
T027	ATM CONTAMINATION MEASUREMENT
T053	EARTH LASER BEACON

STS3 1982 Latex Spheres
STS9 1983 Spacelab 1
STS17 1985 Spacelab 3
STS51B 1985 Spacelab 2
STS61A 1985 Spacelab
D1 STS40 1991 Spacelab
LS1 STS42 1992 IML1
STS50 1992 USML STS46
1992 EUREKA STS47
1992 Spacelab-J STS55
1993 Spacelab D2 STS57
1993 LEMZ STS60 1994
CLPS STS62 1994 USMP2
STS65 1994 IML2 STS73
1995 USML2 STS76 1996
QUELD LPS STS77 1996
CFZF SEF STS78 1996
LM2

STS94 1997 MSL
STS87 1997 USMP4

STS3
Latex
Spheres

STS9
InP
THM

IML1
HgI
VCG

USMP2
IDGE

Source: Courtesy of NASA.

The EU's focus is primarily on materials, technology, engineering, and the circular economy/sustainability via the Fraunhofer Institutes (AM Sub-Platform 2013, EU Powder Metallurgy Association 2014). The European Space Agency (ESA) is focused of additive manufacturing in space to develop replacement parts for the ISS. The EU's Additive Manufacturing Aiming Towards Zero Waste and Efficient Production of High-Tech Metal Products (AMAZE) project involved in-space applications as a core area across the whole of the EU (https://cordis.europa.eu/project/id/313781). ESA is funding in situ additive manufacturing on planetary habitats such as the Moon and asteroids using methods developed in the US. However, the development of manufacturing standards in space and international cooperation between space agencies needs to be established to eliminate duplication owing to the cost of manufacturing in space (Volz 2014).

Manufacturing standards

At least 10,000 ASTM standards (www.astm.org) have been developed for product safety, quality, market access, trade, and consumer confidence. The International Organization Standardization (ISO) (www.iso.org), is also developing technical product standards. Standards specifically for additive manufacturing are being jointly developed by Committee F42 of the ASTM and Technical Committee 261 of ISO.

The variation in standards is in areas of terminology, processes and materials, test methods, and design and data formats. The development of standards by ASTM/ISO for in-space applications are qualification and certification methods, design guidelines, test methods for characterizing raw materials, test methods for mechanical properties of additively manufactured parts, material recycling guidelines, standard protocols for testing, standard test artifacts, and requirements especially for additively manufactured parts (Prater et alia 2019).

Harmony of standards

Considering general manufacturing, standards are already established for Earth-based processing. ASTM has specific terminology for fundamental additive manufacturing. The seven categories given for additive manufacturing technologies under ASTM Standard F2792-12A are vat photopolymerization, material extrusion, material jetting, binder jetting, powder bed fusion, sheet lamination, and direct-energy deposition. However, for terrestrial manufacturing, standards will need to be established prior to large scale in-space additive manufacturing activities (Nafisi et al. 2022).

Manufacturing on Earth

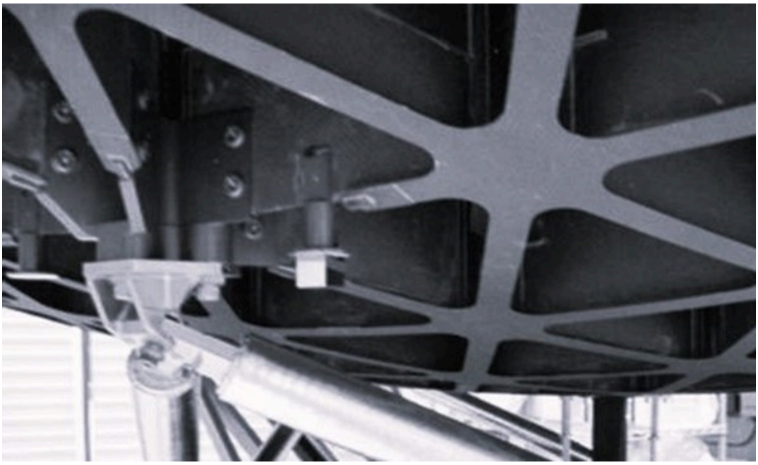
Manufacturing applications (especially additive) are increasing for many aerospace applications. Lockheed Martin additively manufactured waveguide brackets for microwave communication components for NASA's Juno spacecraft launched in 2011 (Figures 4-2 and 4-3). Other parts are being manufactured using additive manufacturing techniques such as rocket engine injectors, entire jet engines, components of engines, CubeSats and small satellites (Schmuland et al. 2013, Gradl et al. 2022).

Figure 4-2 The Juno spacecraft includes additively manufactured space system components

Source: Courtesy of NASA/JPL (https://www.jpl.nasa.gov/)

The Fused Deposition Modeling (FDM) technique is, and additive manufacturing process used by Aurora Flight Sciences to manufacture drone systems and components with active sensors embedded into 3D-printed wings and printed heat exchangers using novel materials (Gradl et al. 2022). Airbus is using 3D printing techniques to produce fully functional metallic prototype of the airframe and propulsion system for a drone aircraft and there are many other examples that show additive manufacturing/printing is able to create complex shapes that are difficult to produce with traditional casting or machining processes (Patankar 2018, Gradl et al. 2022).

Figure 4-3 Additively manufactured waveguide brackets for the Juno spacecraft



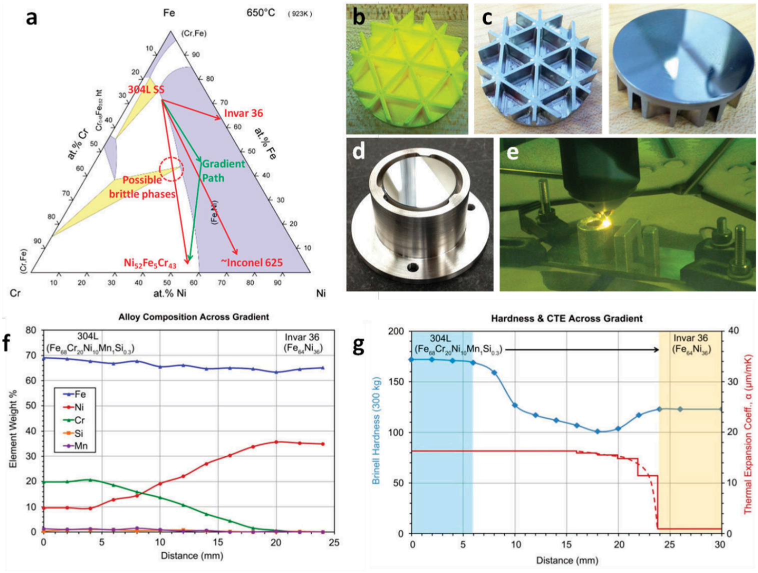
Source: Courtesy of Lockheed Martin *(www.lockheedmartin.com).*

Additive manufacturing creates high value materials and combinations of materials to direct specific product material properties with gradient coatings. NASA's Jet Propulsion Laboratory (JPL) is using printing technology to create gradient structures focusing on specific physical characteristics, rigidity, and/or electrical and thermal properties (Hoffman et alia 2013) that are tailored for performance under various structural load and temperature conditions (https://www.jpl.nasa.gov/). The gradient-metallic alloy mirror assembly developed at JPL is a perfect example of using printing techniques to create gradient engineered materials (Figure 4-4).

The components manufactured this way illustrate how components can be enhanced when exposed to the harsh and complex physical conditions of space (Bhudiya et al. 2022). Additive manufacturing creates less waste compared to traditional manufacturing processes and cost savings are significant (Volz 2014). However, there are still issues with the process owing to the microstructural integrity and reliability. Research in the form of hybrid additive manufacturing systems that combine additive manufacturing with direct-writing technologies that allow embedded structures to be produced in three dimensions. The integration of electronics with 3D printed structures allows flexibility for use in complex environments in space.

Figure 4-4 (a) An isotherm of the Fe-Ni-Cr ternary phase diagram showing different gradient compositions. The lines represent composition gradients between 304L stainless steel and Invar 36, a simplified Inconel 625 alloy and NiFeCr alloy; (b) An isogrid mirror fabricated using a 3D plastic printer; (c) a fabricated part using laser-engineered net shaping (LENS). The mirror surface of Invar 36 and the isogrid backing is a gradient alloy that transitions from Invar 36 to stainless steel; (d) A gradient alloy mirror assembly with a metal-coated glass mirror attached to the Invar side of the assembly using epoxy;

(e) Test samples of a Ti-V gradient alloy being fabricated by LENS; (f) The compositions of the gradient mirror assembly in (d), and (g) hardness and thermal expansions across the gradient mirror assembly. *(http://www.techbriefs.com/component/content/article/5- ntb/ tech-briefs/materials/17446.*



Source: Images courtesy of NASA/Jet Propulsion Laboratory/California Institute of Technology).

The benefits of manufacturing ground-based aerospace applications are significant. However, certain disadvantages need to be addressed for use in space environments and include the cost of operation (equipment, maintenance, and materials); machine performance (size, speed, reliability, repeatability, and reproducibility); and availability/use of materials in space environments.

Manufacturing of space devices on Earth

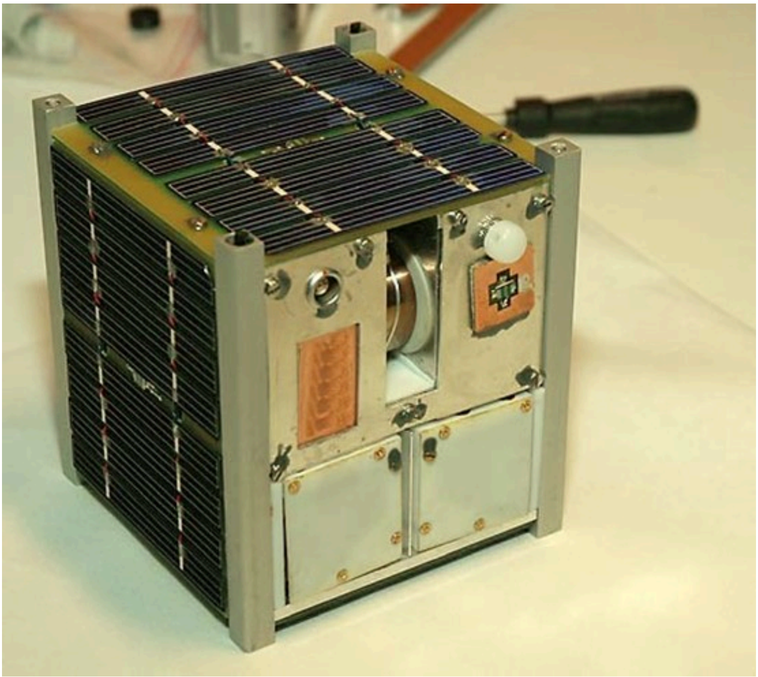
The first use of additive manufacturing techniques for space applications is the development of CubeSats (https://www.cubesat.org/), the first being launched into low Earth orbit (LEO) in 2003. There are more than 4000 of these small (10 cm × 10 cm x 10 cm) satellites have now been placed in LEO (nanosats.eu, 2022). An example of an additively manufactured CubeSat is shown in Figure 4-5. The low cost and simplicity of CubeSats is highly advantageous for developing space science on the small scale. CubeSats were built using traditional spacecraft technologies and are built with a wide range of assemblies and external features produced using additive manufacturing materials/processes. The features produced can control on-board systems including power, communications, propulsion systems, thermal control, attitude control, digital systems, and instrumentation (Russell 2017).

PrintSat (http://www.ssel.montana.edu/printsat.html) was built to demonstrate the manufacture of space structures and mechanisms in a university environment. The satellite structure is composed of polyamide carbon-filled structures used for terrestrial applications. The payload elements include a single-chip hybrid radiation micro dosimeter, load cells, and a surface resistivity sensor to measure the surface resistivity of its nickel plating. The system was designed by students of the Space Science and Engineering Laboratory using standard engineering software and hardware. Flight testing was conducted to NASA standards then launched aboard a small vehicle known as Super Strypi as part of Sandia's space program (www.sandia.gov). This type of space education is clearly achievable using standard equipment/software and associations with government laboratories and agencies.

Manufacturing construction in space

Manufacturing assembly in space started at the beginning of the space program. The effort involved the integration of large and complex components such as space station modules, rather than manufacturing of sub-assemblies/components in space. Space operations required launching fully integrated spacecraft or connecting sub-assemblies in orbit with robots and with human support. Structures and objects were made on the ground and launched into space and assembled using conventional methods. The Soviet space program performed in-orbit welding, and in-space welding has been studied by a US aerospace contractor. NASA employed supporting technologies associated with welding processes and the ISS was an assembly and integration project that was manufactured on Earth. However, there were attempts at in-space manufacturing of construction materials in the mid- 1970s, when NASA built the 'Space Fabrication Demonstration System' capable of assembling triangular aluminum trusses. The system was tested at NASA Marshall Space Flight Center (MSFC) in Alabama, where NASA considered using lunar regolith or Martian soil for the construction of structures. However, the project did not continue.

Figure 4-5 NCUBE2 CubeSat integrated with the ESA satellite SSETI-Express

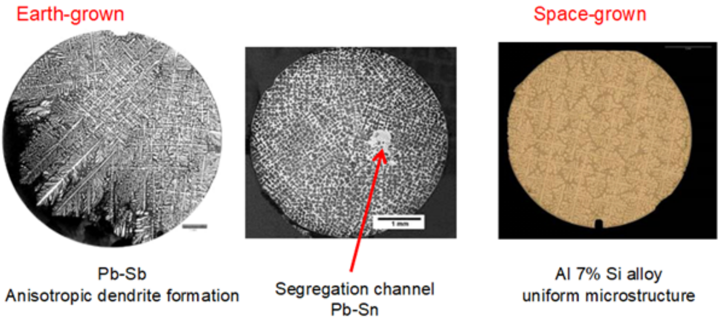


Source: Courtesy of Bjørn Pedersen, NTNU, Norway.

Materials science and manufacturing aboard the ISS

The development of materials science aboard the ISS has prompted the development of using additive manufacturing processes in space (Momeni et al. 2022). Initial studies on microgravity showed that diffusion-controlled growth is the dominant mechanism of solidification promoting uniform microstructures as shown in Figure 4-6. Figure 4-6 shows the differences between anisotropic dendrite formation in Pb-Sb alloys and segregation channels in Pb-Sn alloys grown on Earth to those formed in space. Space grown alloys show uniform microstructure due to reduced thermal and solute convection flows (Volz 2014).

Figure 4-6 Microgravity Reduces Thermal and Solute Convection (Volz 2014)

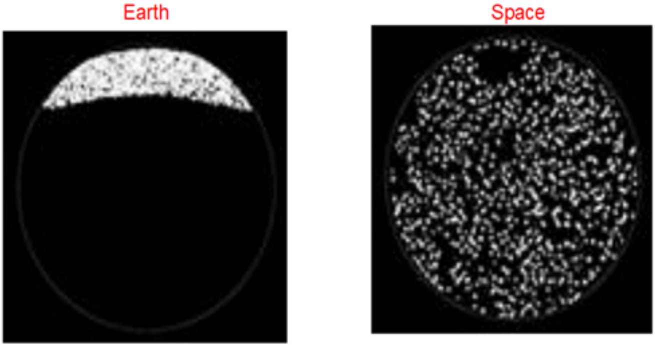


Source: Courtesy of NASA.

Microgravity also minimizes sedimentation and buoyancy of mixed materials, which promotes uniform particle distributions that leads to understanding of coarsening mechanisms and sintering (Figure 4-7) (Volz 2014). The systems used on the ISS to conduct materials science experiments focus on the use of a materials science glovebox, a SUBSA vertical gradient furnace with transparent growth zone, a PFMI low temperature furnace for solidification and remelting of transparent materials and a CSLM quench furnace for studying coarsening in metals (Figure 8).

In addition to the equipment on the ISS shown in Figure 4-8, a Low Gradient Furnace (LGF) and a Solidification Quench Furnace (SQF) also operate on the materials science rack on the ISS with cartridges provided by ESA (Figure 4-9). These pieces of equipment provide the laboratory equipment needed to understand the basics of manufacturing in space (Volz 2014).

Figure 4-7 Microgravity Minimizes Sedimentation and Buoyancy (Volz 2014)



Source: Courtesy of NASA.

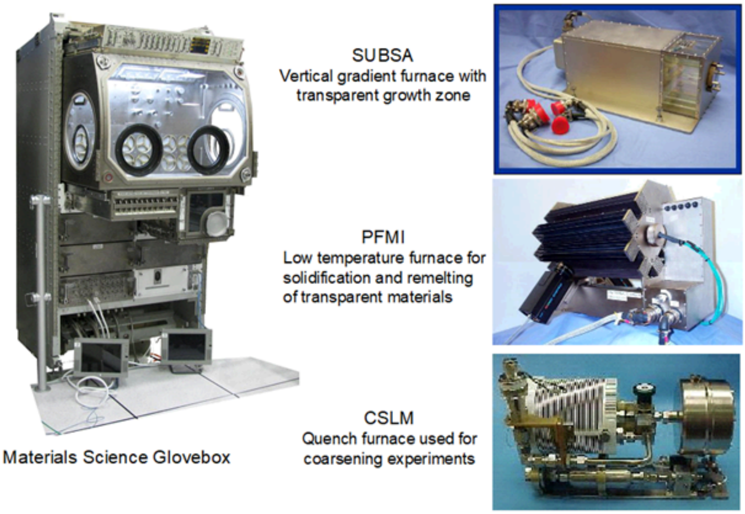
In 1999, Cooper and Griffin of NASA MSFC helped publish a report that referred to direct manufacturing and stated that in remote locations such as the Moon or Mars, direct fabrication (manufacturing) could be used to produce items on location (NRC 2000). The report explained how additive manufacturing in microgravity space demonstrated the benefits of the fused deposition modeling (FDM) technique to quickly produce replacement components or repair broken hardware on the Space Shuttle (SS) or on the International Space Station (ISS).

Cooper and Griffin conducted many laboratory experiments and KC-135 low-gravity aircraft experiments to demonstrate the capability of FDM equipment to fabricate in a microgravity environment. Cooper and Griffin developed a hardware implementation plan using FDM for further experiments aboard the ISS. They proposed using an ISS FDM device with a 10 cm × 10 cm × 10 cm working volume, total mass of approximately 45-65 kg, physical envelope of 0.45 m × 0.5 m × 0.6 m using peak power of 300 W with an air cooling of 150 W (Cooper and Griffin 2003).

Additive manufacturing holds the potential to extend traditional manufacturing capabilities to physical scales currently unobtainable with current spaceflight hardware construction practices (Korkut and Yavuz 2022). Manufacturing in space allows construction of structures and subsystems fully optimized to operate in the zero-gravity environment with volume-to-mass efficiencies that may revolutionize future approaches to design (Prater et alia 2018, 2019).

Figure 4-8 Materials Science Facilities on the ISS:

Materials Science Glovebox (MSG) Facilities (Volz 2014)

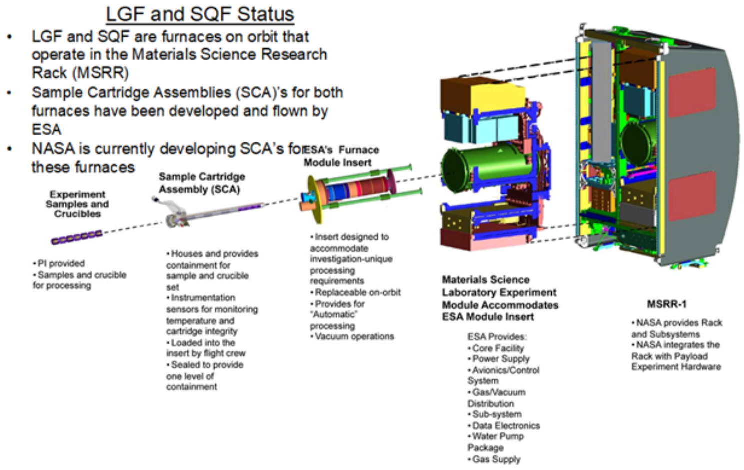

SUBSA
Vertical gradient furnace with transparent growth zone
PFMI
Low temperature furnace for solidification and remelting of transparent materials
CSLM
Quench furnace used for coarsening experiments
Materials Science Glovebox

Source: Courtesy of NASA

Manufacturing in Space

Manufacturing in space is a very useful way of creating replacement parts and systems. The percentage of hardware failures on the International Space Station (ISS) involve polymeric and composite materials (~ 30%) that can be repaired using additive manufacturing techniques on board the ISS. NASA has developed several ways to achieve this. Contracts with ‘Made In Space, Inc.’ (www.madeinspace.us) to provide extrusion-based additive manufacturing in microgravity environments on board the ISS were granted. Once printed, an optical scanner is used to verify the integrity of parts made with a view to create procedures to use metals and combinations of materials (Prater et alia 2019).

Figure 4-9 Materials Science Facilities on the ISS: Low Gradient Furnace (LGF) & Solidification Quench Furnace (SQF) (Volz 2014)



LGF and SQF Status

- LGF and SQF are furnaces on orbit that operate in the Materials Science Research Rack (MSRR)
- Sample Cartridge Assemblies (SCA)'s for both furnaces have been developed and flown by ESA
- NASA is currently developing SCA's for these furnaces

Experiment Samples and Crucibles

- PI provided
- Samples and crucible for processing

Sample Cartridge Assembly (SCA)

- Houses and provides containment for sample and crucible set
- Instrumentation sensors for monitoring temperature and cartridge integrity
- Loaded into the insert by flight crew
- Sealed to provide one level of containment

ESA's Furnace Module Insert

- Insert designed to accommodate investigation-unique processing requirements
- Replaceable on-orbit
- Provides for "Automatic" processing
- Vacuum operations

Materials Science Laboratory Experiment Module Accommodates ESA Module Insert

ESA Provides:

- Core Facility
- Power Supply
- Avionics/Control System
- Gas/Vacuum Distribution
- Sub-system
- Data Electronics
- Water Pump Package
- Gas Supply

MSRR-1

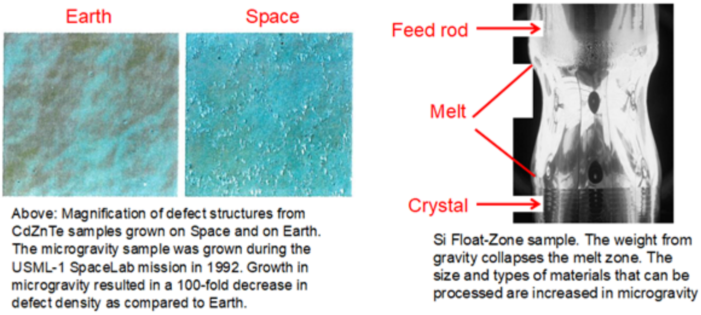
- NASA provides Rack and Subsystems
- NASA integrates the Rack with Payload Experiment Hardware

Source: Courtesy of NASA.

In addition to additive manufacturing, other forms of traditional manufacturing are envisaged such as container-less melting of metals (Figure 4-10), mixing of liquids for pharmaceutical production and the bulk solids processing of liquids and solids. Additive manufacturing in space presents new opportunities for recycling. Recycling material on the ISS has a significant impact on ISS operations. Traditionally, astronauts assign waste to robotic spacecraft (Russian Progress and the Orbital Sciences' Cygnus) for disposal. This is achieved by detaching from the ISS and burning up in the upper atmosphere of the Earth. However, using recycled materials would eliminate that operation. Component/system creation and recycling allows one to launch feedstock to ISS instead of hardware (Prater et alia 2018).

The microgravity environment enables accurate measurements of material properties such as viscosity and surface tension, facilitates nucleation studies, increases the size of crystals that can be grown container-less and reduces defect densities from contact with container walls (Figure 4-10).

Figure 4-10 Microgravity Allows Container-less Processing to Manufacture Items (Volz 2014)



Above: Magnification of defect structures from CdZnTe samples grown on Space and on Earth. The microgravity sample was grown during the USML-1 SpaceLab mission in 1992. Growth in microgravity resulted in a 100-fold decrease in defect density as compared to Earth.

Si Float-Zone sample. The weight from gravity collapses the melt zone. The size and types of materials that can be processed are increased in microgravity

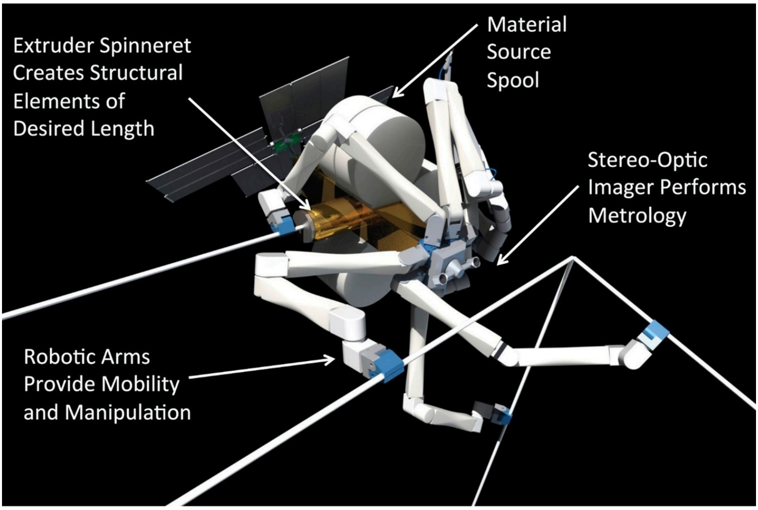
Source: Courtesy of NASA.

Manufacturing hardware enables the production of low-mass systems thereby reducing launch and storage burdens. Antennas, booms, and panels are designed for launching and their size and shape are limited in addition to their functionality and scale. Manufacturing in space and orbital construction enable deployment of systems that do not conform to weight and volume constraints. Systems include mirrors, gossamer structures, antennas and arrays, reflectors, trusses and much more (Kovalchuk et al. 2022).

Tethers Unlimited (https://www.tethers.com/) is a company that provides launchable materials in the form of spools of thread to form large truss-based structures such as solar arrays and antennas in space. Other applications such as star shades to block light/heat from stars allow space-based telescopes to image exoplanets around stars. The use of a large spider-like robot that can extrude long beams of thread and join large structures together is highly attractive for space exploration activities and is known as 'SpiderFab' (Figure 4-11).

Additive manufacturing in space enables the production of entire subsystems and systems including the production, assembly, and launch of sensor-based CubeSats from the ISS and other platforms in orbit (Stewart et al. 2022). In-space satellites deployed as swarms are not inconceivable. The Automated Manufacturing Facility on the ISS and CubeSat platforms could provide swarms of satellites. The swarm could have a range of capabilities and act as a fully functional satellite system.

Figure 4-11 'SpiderFab' is a combination structural elements and multi-dexterous robots that can control and manipulate structural elements

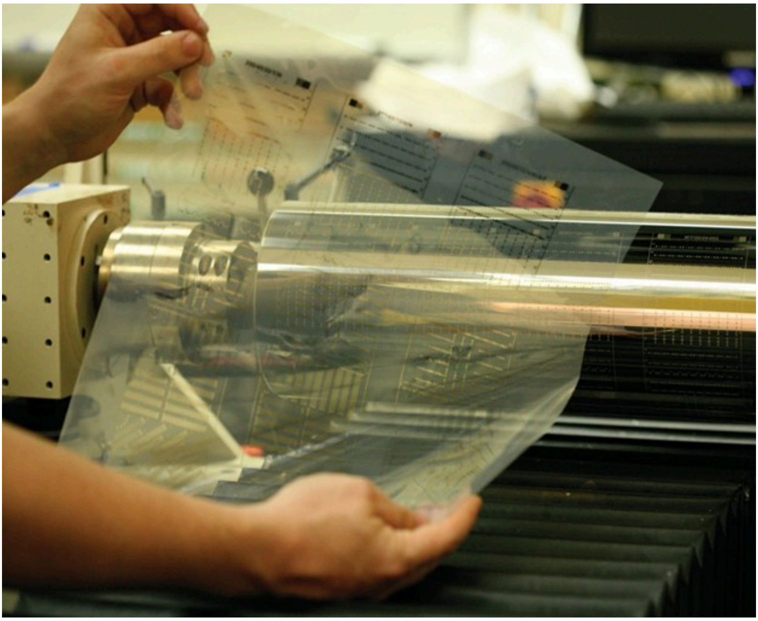

Extruder Spinneret Creates Structural Elements of Desired Length
Material Source Spool
Stereo-Optic Imager Performs Metrology
Robotic Arms Provide Mobility and Manipulation

Source: Courtesy of Tethers Unlimited.

The concept of a fabrication laboratory (fab lab) was developed at the Massachusetts Institute of Technology. A typical fab lab is equipped with flexible manufacturing systems and would be able to manufacture what is needed without providing it from Earth. Free-flying fab labs for manufacturing in space is a distinct possibility (Warner 2017).

Additive manufacturing techniques such as printing can be applied to subsystems and complete systems such as spacecraft (Kovalchuk et al. 2022). Sub-systems can be deposited on a transparent sheet of plastic with electronic components printed to collect environmental information in space or within a planet's atmosphere (Figure 12). Roll-to-roll printing is a technology that can revolutionize manufacturing in space and allows the integration of mechanical and electrical systems. The technique can produce flexible electronics that can sense a variety of conditions prevalent in space.

Figure 4-12 A two-dimensional printed spacecraft being developed at the Jet Propulsion Laboratory

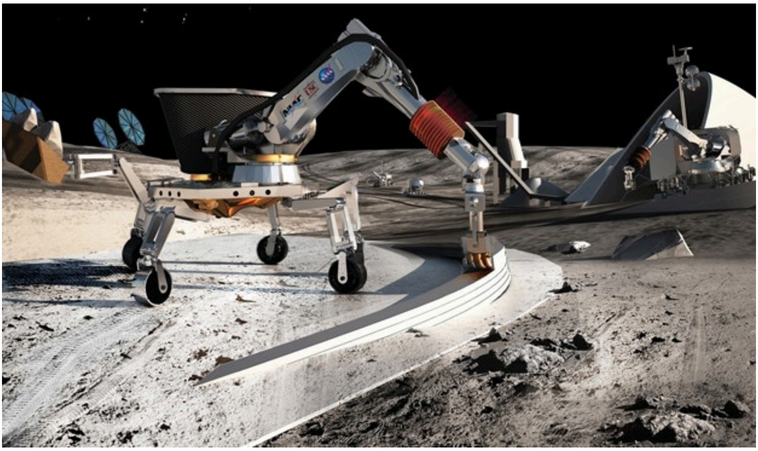


Source: Courtesy of PARC, a Xerox company;

(http://gigaom.com/2013/08/20/nasa-wants-to-print-a-spacecraft-but-first-its-printing-the-electronics/).

When considering manufacturing on planets, the availability of construction materials in space on asteroids or surfaces of planets allows one to use manufacturing processes to build settlements without having to launch expensive and prefabricated materials out of Earth's orbit (Stewart et al. 2022). Lunar regolith (simulated moon soil) could be used to construct pressurized habitats or other infrastructure needed to live on other planets such as landing pads, roads, walls, buildings for protection against thermal radiation on the Moon (Figure 4-13).

Figure 4-13 A robot on the Moon using "contour crafting" to build up a structure, layer by layer



Source: Courtesy of USC.

Contour crafting can create landing pads on the Moon using simulated lunar regolith. Simulated lunar regolith is being manufactured at the University of Central Florida's Center for Lunar and Asteroid Surface Science (https://sciences.ucf.edu/class/exolithlab/#:~:text=Located%20in%20Orlando%2C%20Florida%2C%20Exolith,asteroid%20regolith%20(soil)%20simulants) and aims to practice building structures on Earth prior to building on the Moon. Contour crafting extrudes a building material layer-by-layer to build structures. ESA has developed a similar technology called D-Shape Printing to build Moon-based habitats (https://www.esa.int/ESA_Multimedia/Images/2013/01/D-Shape_printer).

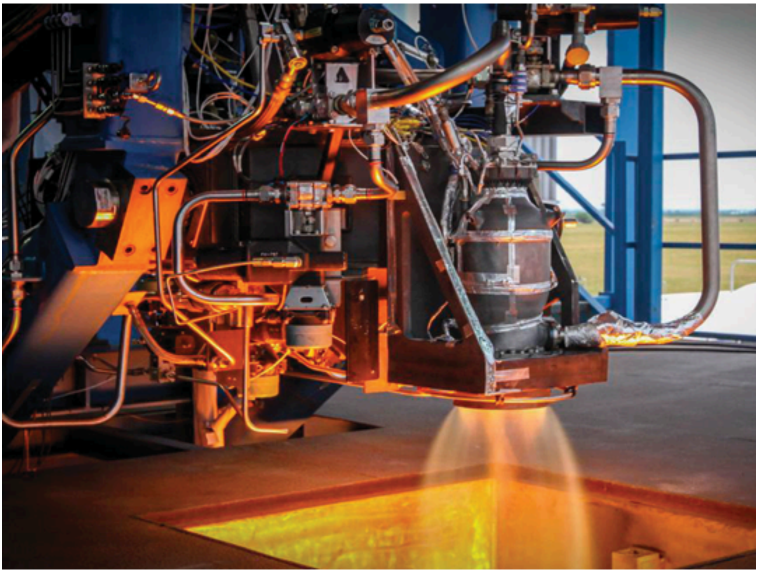
Launch vehicles transporting materials for additive manufacturing activities in space can provide volume densities > 100 x, producing spacecraft in orbit or in a space-based manufacturing center tailored to operate in a microgravity environment such as the Moon. However, there are still many challenges and hurdles to overcome to realize the concept of manufacturing in space.

Challenges of Manufacturing in Space

For homogenous and heterogeneous material mixtures used in space, new physics-based models of manufacturing processes are required to predict material properties and design the correct material compositions (Owens et al. 2016). An understanding of basic physics will create predictive modeling techniques that will allow engineers to know functional properties of systems of parts (Figure 4-14).

New methods are needed for in-process monitoring and closed-loop feedback of sensors enabling non-destructive evaluation and defect detection. Also, different processing approaches can change the properties of systems due to thermal effects depending on the energy source, density, and environment (Owens 2017).

Figure 4-14 SuperDraco rocket engine uses an additively manufactured Inconel thrust chamber



Source: Courtesy of SpaceX.

Printers create parts by fusing solid sheets or by using a laser to heat and/or polymerize. The total volume required to print dominates the build time. The time to print an object also depends on the resolution. The complexity of the design and the application of the part will affect time required to manufacture it. CubeSats can be constructed in weeks if printing is required for complex subsystems. Printing in space will require less mass due to the reduced gravity but is difficult to predict build time without knowing the resolution required and the impact of environment on the process (Prater et al. 2018).

The manufacturing of complex, multi-material, and multi-functional parts involving embedding a circuit board, motor, or other sub-assembly into the process when and where it needs to be integrated can be done easily for ground-based systems. To manufacture a functional satellite in orbit it is likely to require research into additive manufacturing specifically focused on that function and the environment it operates (Figure 4-15).

Figure 4-15 Lockheed Martin's Advanced Extremely High Frequency Communications Satellite manufactured with additive processes on the Earth

Source: Courtesy of Lockheed Martin Corporation.

Manufacturing spacecraft on Earth through the use of additive manufacturing process requires developments in each of the spacecraft subsystem areas (Prater 2019). Developments in electronics and optical manufacture will require mirrors and optics to be fabricated using photolithographic and surface science techniques that will be more accurate than additive manufacturing processes (Cooper and Griffin 2003). This will require transitioning all types of manufacturing processes to the space environment.

Manufacturing in space can be conducted in a pressurized and climate-controlled environment or provided in an unpressurized vacuum of space. The location of the manufacturing will be affected by the microgravity environment will be a concern and the vacuum and thermal environment will need to be considered when understanding the physics of additive manufacturing processes such as casting, welding, and printing. Electron beam processing has been developed for use in high vacuum environments. It is an energy source that can be adapted to melt and fuse materials and could be useful in the space environment (Bagwell 2018).

The current technologies used on Earth that thrive in vacuum will require further study to understand the effect of zero-gravity or microgravity on manufacturing processes and the properties of the manufactured article (Cooper and Griffin 2003). In the absence of gravity, surface tension forces become dominant forces of system function and processes that rely on the control of fluid or flow conditions will need further understanding. Reduced gravity environments will affect processing parameters and functional integrity of the manufacturing item or system (Marsh 2018).

The lack of gravity will affect the design of handling and support systems for products. Earth based processes all function at 1g within thermally controlled environments. Also, zero/micro gravity environments generate floating debris that has the potential to interfere with the manufacturing process (Moraguez et alia 2019). However, new drives will have to be designed to avoid debris damage and to integrate robotic interactions with manufacturing processes in the absence of gravity to constrain manufactured parts/systems. Microgravity environments might create new opportunities for improving manufacturing systems and processes (Moraguez et alia 2019).

Thermal environments in space include a lack of convection currents that will affect the processes of manufacturing that will be subjected to the thermal loads of solar, albedo (measure of the diffuse reflection of solar radiation out of total solar radiation), and the Earth's infrared during orbit (Kurk 2017). The operation and performance of manufacturing systems including dimensional accuracy of the product/system will be affected. Shielding may have to be of paramount importance for such operations in space (Huebner 2018).

The creation of stable in-space manufacturing platform is needed to survive and operate in the space environment. The ISS provides a platform for the development of manufacturing processes in a space-based environment. ISS also has a materials science aspect that allows physics-based manufacturing to take place and can be validated too (Norfolk 2018). Clearly, the existence of the ISS is important to the further development of manufacturing in space, but a lunar manufacturing base would provide the economies of scale needed to explore and mine ores on planets such as Mars.

Manufacturing in space is far more of a systems engineering issue compared to manufacturing on Earth (Boling 2019). The supporting infrastructure and environments are not trivial in space compared to Earth and there is a much greater reliance on reusing, recycling, and remanufacturing scarce resources. The circular economy is considered vital to developing any manufacturing system in space and its importance on Earth and in space cannot be overstressed.

Manufacturing in Space and the Circular Economy

Circular versus linear economic model

The current linear consumption model practiced on Earth is one of raw material extraction, production, use, and disposal dominates the global economy. Today, we clearly see that this linear model has led to serious unintended global consequences from resource depletion to global waste, spanning all industrial sectors, from plastics to the built environment. In the current linear economic model, we take, make, and waste products. In contrast with the 'take-make-waste' or linear model is the circular economy. The ideas behind the circular economy include keeping products in use, eliminating waste and pollution by design, and aiming to help nature.

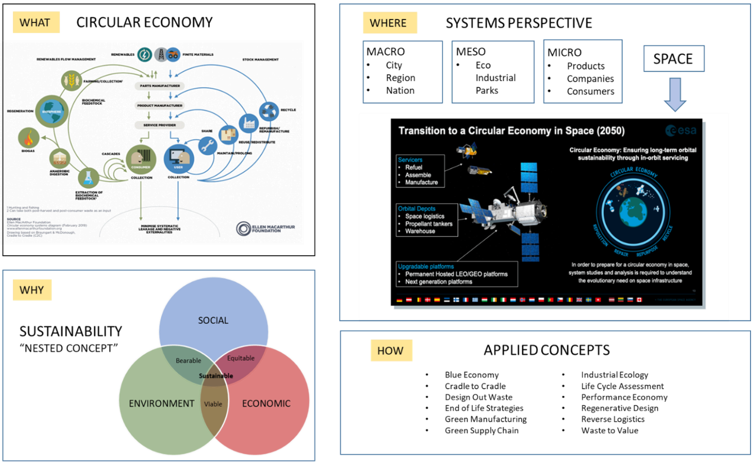
In some industries, such as automobile production and commodity aluminum products, circular design principles have been successfully introduced, while in others such as plastics products or the built environment, progress towards circularity has been painfully slow. For example, the growth in the construction sector to house our growing population leads to extraction of construction minerals exceeding 10 billion metric tons annually, and the construction industry alone could be responsible for up to 60% of the remaining carbon budget (Muller, 2013). This industry currently favors the use of products such as composite wood materials that do not degrade such that 38 million tons are landfilled annually in the US alone (U.S. EPA, 2015; Fischer-Kowalski, 2011). In contrast to linear models, circular economy (CE) aims to decouple economic growth from resource consumption by cycling products and materials back into production, either by returning materials to generate new products, or by releasing benign substances to the environment through degradation. CE principles are based on the efficient use of resources and eliminating waste from product life cycles; a truly circular economy keeps material in continuous use by design. The overall adoption of CE principles has been incremental at best – especially in the US – because the market fails to account for externalities (i.e., full environmental costs) and owing to a lack of truly circular designs to replace conventional analogs (EMF, 2017). Bocken (2016) states that CE product design is underpinned by closing and slowing resource loops. Closing resource loops involves either creating products and components that can be easily and safely absorbed by the biosphere or creating items that while they cannot be released to the ecosystem, can be easily recycled to high value uses. As such, closing loops involves: (a) design for a biological cycle, (b) design for a technological cycle, and (c) design for disassembly and reassembly. Designing for slowing resource loops includes design for longer life and product life extension. In the design for longer life, one aims to create more robust products with longer viable service lives, while also creating designs to which consumers become emotionally attached. Product life extension can be achieved through several strategies: (a) design for ease of maintenance and repair, (b) design for upgradability and adaptability, (c) design for standardization and compatibility, and (d) design for dis- and re-assembly.

Circular economy versus sustainability

A circular economy, as defined in the Save Our Seas 2.0 Act, refers to an economy that uses a systems-focused approach and involves industrial processes and economic activities that are restorative or regenerative by design, enable resources used in such processes and activities to maintain their highest value for as long as possible, and aim for the elimination of waste through the superior design of materials, products, and systems (including business models). It is a change to the model in which resources are mined, made into products, and then become waste. A circular economy reduces material use, redesigns materials to be less resource intensive, and recaptures "waste" as a resource to manufacture new materials and products.

A framework is developed to present CE in Figure 4-16 that intends to identify and segregate CE from its surrounding ecosystems similar to a framework used by Nobre (2021). The framework, inspired by the 5W1H concept – *What, Where, Why, When, Who and How*, allows readers to separate the main research objective – “*what is CE?*” – from “*why it is important*”, “*where it applies to*” and “*how it can be implemented*”. Ellen MacArthur’s ‘Butterfly’ circular economy system diagram in Figure 4-16 illustrates the continuous flow of technical and biological materials through a circular economy. The closed loop paradigm has started to garner even more attention now that the United Nations (UN) has integrated CE practices to achieve its Sustainable Development Goals (SDGs) by 2030.

Figure 4-16 Circular economy definition framework



Source: United Nations (UN) has integrated CE practices

While the terms ‘Circular Economy’ and ‘Sustainability’ are increasingly gaining traction with academia, industry, and policymakers, the similarities and differences between both concepts remain ambiguous. The Brundtland Commission provided the most commonly accepted definition of sustainability as “development that meets the needs of the present without compromising the ability of future generations to meet their own needs” (Brundtland, 1987).

The most noticeable work on CE has been by the Ellen MacArthur Foundation. The Foundation acts as a collaborative hub for businesses, policy makers, and academia. The CE concept has gained traction with policymakers, influencing governments and intergovernmental agencies at the local, regional, national, and international level. Germany was a pioneer in integrating the Circular Economy into national laws, as early as 1996, with the enactment of the “Closed Substance Cycle and Waste Management Act” (Su et al., 2013). This was followed by Japan’s 2002 “Basic Law for Establishing a Recycling-Based Society” (METI, 2004), and China’s 2009 “Circular Economy Promotion Law of the People’s Republic of China” (Lieder and Rashid, 2016). Supranational bodies have also incorporated circular economy concerns – most notably the EU’s 2015 Circular Economy Strategy (European Commission, 2015).

The modern understanding of the term Circular Economy seems to have emerged more recently than that of sustainability. While the Circular Economy is traced back by

EMF (2013) to different schools of thought like cradle-to-cradle and industrial ecology, the concept of sustainability is considerably older (Mantel, 1990) and was institutionalized by environmental movements and supranational bodies, especially after the publication of the Brundtland report in 1987. Table 1 summarizes the identified differences between the two concepts of Circular Economy and Sustainability.

Applying the circular economy in space

According to a well-known OECD's definition, the space economy "comprises a long value-added chain, starting with research and development actors and manufacturers of space hardware (e.g., launch vehicles, satellites, ground stations) and ending with the providers of space-enabled products and services to final users" (OECD, 2007, online).

The traditional approach to space industry was to divide the sector into two segments: one upstream, which includes launch systems, ground operations and satellite manufacturers and the other downstream, related to all providers of satellite communication services to the consumers (OECD, 2007). This distinction, which came into existence in the 1990s during the marked increase in the commercialization of satellite services around the world, is still popular, irrespective of the fact that the sector itself has moved on both for turnover and as a paradigm jump. The space industry went through a cycle development, each of which presenting widely different characters and actors (OECD, 2016, 2019). Cycle 4 characterized by both the popularization and the globalization of space has seen the emergence of a different kind of downstream activities, mainly handled by private companies and supported by the on-going digital revolution, has now been completed. The new Cycle 5, started in 2018 and expected to last until 2033, will be determined by an ever-increasing availability of data, and, among other things, by the widespread adoption of CE principles. Cycle 5 is characterized by growing uses of satellite infrastructure outputs; global monitoring; new space activities; and robotics missions (Paladini, 2021).

Paladini et al (2021) propose a framework integrating circular economy, Space Sector, and Industry 4.0. The cornerstone of Industry 4.0 conceptualization mandates that, while its nine innovation-enabler fundamental pillars ((i.e., Big Data & AI, Horizontal &Vertical Integration, Cloud Computing, AR, IoT, Additive Manufacturing and 3D Printing, Autonomous Robot, Simulation, Cyber-Security (Russmann et al., 2015)) make smart systems possible, it is only when they are all used together that Industry 4.0 unleashes all its potential (Sap, 2020; Haskel and Westlake, 2018). Space system Cycle 5, has already brought a series of new actors on the world scene and a different set of procedures at all levels, taking the sector away from the traditional upstream and downstream divide and steering it toward a different configuration, in an increasingly overlapping series of value chains whose potential for spillovers to other sectors are far higher. The adoption of incremental technologies, including data analytics, additive manufacturing, and robotics, had the net effect of reducing those material costs and production times, changing dramatically the way both private and public operators plan their missions. In one of the trends that is certainly going to keep growing is the way private process innovators are changing the sector, followed by the incumbents, especially in additive manufacturing (Russell, 2017; EOS, 2016) already identified as one of the cardinal points of CE applications to industry. Space X's reusable rockets and adaptation of experiences and data from high-volume industries (Space X, 2021; OECD, 2019), such as the automotive industry, are just the beginning.

Other innovations that have already made their appearance in the area of space manufacturing includes extensive 3D printing (e.g., Space X rockets and RocketLab engines), a growing reliance on 'off-the-shelf' components within supply chains, and the Cubesat revolution of low-cost and low-impact satellites, which have become the tool of choice of small organizations and educational institutions.

Applying circular economy principles in space for manufacturing

- Efforts in the US

NASA's In-Space Manufacturing (ISM) project seeks to develop the materials, processes, and manufacturing technologies needed to provide an on-demand manufacturing capability for deep space exploration missions. The ability to manufacture, repair and recycle some parts on demand rather than launch them from earth has the potential to reduce logistics requirements on long duration missions and enhance crew safety.

ISM can provide on-demand fabrication, repair, and recycling for critical systems, habitats, and mission logistics and maintenance (both in-transit and on-surface). This can provide cost savings by decreasing launch mass. Risk is reduced by decreasing the need for pre-produced spares and/or over-designing systems for reliability. ISM is developing these capabilities by using new technologies being developed terrestrially and modifying them for use in the space environment.

In-Space Manufacturing shows immense potential to achieve gains in logistics reduction by (a) reducing the number of spare parts and orbital replacement units which much be up massed and (b) enabling the recycling of materials which would otherwise be nuisance materials (scrap/trash) or consumables (Owens, 2016; Owens, 2017). The "make it, don't take it" philosophy represents a fundamental paradigm shift from traditional logistics models, which rely on the change out of orbital replacement units (stowed on the ISS) rather than repair of a unit at the component level. The implementation of ISM on future space mission thus depends on design of exploration systems which are accessible and intended to be repaired rather than simply changed out with an identical full-scale unit stored on-orbit.

The work under the recycling/reuse component of the In-Space Manufacturing portfolio focuses on reuse of plastics and packaging materials through (a) manufacturing technology development for (i) recycling and (ii) printing with recycled materials and (b) development of materials which are intended to be reused and recycled.

- Efforts in the EU

European Space Agency (ESA) is looking to foster the implementation of a 'circular economy' in space by **recycling, refurbishing, repurposing, and reusing by 2050.** In this case, a circular economy means "*ensuring long-term orbital sustainability through in-orbit servicing.*"

The first step toward these goals has been taken through a series of ESA studies carried out with European industry under the umbrella title of 'On-Orbit Manufacture, Assembly and Recycling' (OMAR). These studies identified some key advantages that this revolutionary new space ecosystem could have, including:

- Reduction in launch mass by taking advantage of material, equipment or even entire assets that are already in orbit.

- Reduction in raw materials that are required to be extracted on ground by recycling critical raw materials that are already in orbit.
- Decrease in development times as the assets can be developed and tested directly in orbit.
- Development of key technologies and capabilities that currently cannot be achieved because satellites are constrained by the dimensions and capabilities of launchers.

To transition from OMAR studies to a circular economy, the Agency is considering presenting a proposal at the ESA Ministerial Council (end-2022) to place contract(s) with service provider(s) and customer(s) to perform In-Orbit Servicing covering some or all services listed below:

Cooperative Attitude and Orbit Control System (AOCS) takeover: lifetime extension for a customer spacecraft by providing the needed propulsion/actuation capabilities.

Assembly: Assemble, manipulate and/or disassemble (take apart) spacecraft parts from or into a satellite/vehicle.

Refurbishment: Rehabilitation or servicing of a spacecraft by replacing current aged or non-functional parts by new, equivalent ones.

Manufacturing: Manufacturing of spacecraft parts in orbit starting from raw material and/or basic components coming from Earth and/or from in-orbit recycling.

Refueling: Re-supply of propellant to a spacecraft already in space.

Future Possibilities

The future possibilities associated with manufacturing in space are tremendous and varied including planetary mining and manufacturing, asteroid mining and manufacturing, and manufacturing in orbit around planets and satellites of planets. The challenges are great and a great deal of understanding the physics of manufacturing processes is needed in addition to the integration of systems to minimize waste and effort. The space environment allows us to develop materials that cannot be made on Earth owing to gravity or environmental constraints. There is a vast amount of knowledge that we simply do not know about manufacturing in space environments that will occupy the minds of young scientists and engineers for decades to come.

Questions

1. Describe the concept of 'manufacturing in space'.
2. How does the microgravity environments affect the structure of materials and how they are manufactured into parts, components, systems, and sub-systems?
3. What are manufacturing standards and how are they harmonized?
4. Describe the type of equipment used on the

International Space Station (ISS) to study the effects of microgravity on the properties of materials.

5. How does 'Circular Economy' fit into the concept of sustainability?
6. What are the three pillars of sustainability? What happens when only two out of the three pillars are achieved?
7. How is circularity applied in the space sector?
8. Compare and contrast the US's and the EU's circularity efforts in the area of manufacturing in space.
9. Why is manufacturing in space different to manufacturing on Earth? Compare and contrast the differences.
10. Why is the application of systems engineering principles critical to manufacturing in space?

References

"Acoustical Signature Analysis for In-Situ Monitoring and Quality Control for In-Space

Manufacturing." MetroLaser, Inc. Small Business Innovative Research (SBIR) abstract. 2018. < https://www.sbir.gov/sbirsearch/detail/1559789>

AM Sub-Platform, 2013 Additive Manufacturing: Strategic Research Agenda, Version 2, http://www.rm-platform.com/linkdoc/AM_SRA_ FINAL-V2.pdf.

Anderson, Janet. “NASA to Demonstrate Refabricator to Recycle, Reuse, Repeat.” NASA Press Release. 14 November 2018. < https://www.nasa.gov/mission_pages/centers/marshal l/images/refabricator.html>

Bagwell, Roger. “Additive Manufacturing of PEEK and Fiber-Reinforced PEEK for NASA Applications and Custom Medical Devices.” Proceedings of the National Space and Missile Materials Symposium, Henderson, NV. June 2018.

“Automated In-Process Quality Control of Recycled Filament Production and FDM Printers.” Cornerstone Research Group. Small Business Innovative Research (SBIR) abstract. 2018. < https://www.sbir.gov/sbirsearch/detail/1559745>

Bhundiya, H.G., Royer, F. & Cordero, Z. Engineering Framework for Assessing Materials and Processes for In-Space Manufacturing. J. of Materials Eng and Perform, 2022, 31, 6045–6059. https://doi.org/10.1007/s11665-022-06755-y

Bocken, N.M.P., de Pauw, I., Bakker, C., van der Grintern, B., *Product design and business model strategies for a circular economy*. J. Industr. Prod. Eng., 2016. 33(5): p. 308-320.

Boling, Rich. “3D Printer for Human Tissue Now Available for Research Onboard the ISS National Laboratory.” ISS National Lab. 13 August 2019. < https://www.issnationallab.org/blog/3d-printer-for-human-tissue-now-available-for-research-onboard-the-iss-national-laboratory/>

Brundtland, G.H., 1987. *Our common future: Report of the 1987 World Commission on Environment and Development*. United Nations, Oslo.

Brussels. Lieder, M., Rashid, A. *Towards circular economy implementation: a comprehensive review in context of manufacturing industry*, 2016, J. Clean. Prod. 115, 36–51.

"CRISSP Custom Recyclable International Space Station Packaging." Small Business Innovative Research (SBIR) abstract. 2017. www.sbir.gov/sbirsearch/detail/1148879

Cooper K. and Griffin M., Microgravity Manufacturing Via Fused Deposition, NASA TM-2003-212636 (https://ntrs.nasa.gov/citations/20030067856).

Ellen MacArthur Foundation (EMF), 2013. Towards the Circular Economy, vol.1. Isle of Wight.

Ellen MacArthur Foundation. Barriers policy can overcome. 2017 (cited 9 August 2022).

European Powder Metallurgy Association, "European Additive Manufacturing Group (EAMG)," http://www.epma.com/european- additive-manufacturing-group, accessed March 11, 2014

European Commission. Closing the loop – An EU action plan for the Circular Economy, Com (2015) 614 communication from the commission to the European parliament, the council, the European economic and social committee, and the committee of the regions.

"Feedback Sensors for Closed Loop In-Space Manufacturing." Cybernet Systems Corporation. Small

Business Innovative Research (SBIR) abstract. 2018. < https://www.sbir.gov/sbirsearch/detail/1559783>

Fischer-Kowalski, M., et al., "Methodology and Indicators of Economy-wide Material Flow Accounting". 2011. 15(6): p. 855-876.

Geissdoerfer, M. and Savaget, P. and Bocken, N.M.P. and Hultink, E.J. *The circular economy – a new sustainability paradigm?* Journal of Cleaner Production., 2017, 143. pp. 757-768.

Gradl, P., Tinker, D.C., Park, A. et al. Robust Metal Additive Manufacturing Process Selection and Development for Aerospace Components. J. of Materials Eng and Perform, 2022, 31, 6013–6044. https://doi.org/10.1007/s11665-022-06850-0

Haskel, J., Westlake, S., 2018. Capitalism without Capital: the Rise of the Intangible Economy. Princeton University Press, Princeton, New Jersey

Hofmann D., Borgonia J., Dillon D., Suh E., Mulder J., and Gardner P., "Applications for Gradient Metal Alloys Fabricated Using Additive Manufacturing," NASA Technical Brief, Jet Propulsion Laboratory, October 1, 2013, http://www.techbriefs.com/component/ content/article/17446.

Huebner, Lawrence. "Archinaut Technology Development: Ground-Based Results for External In-Space Additive Manufacturing and Assembly." Proceedings of the National

Space and Missile Materials Symposium, Henderson, NV. June 2018.

"In-Space Manufacturing (ISM) Multi-material Fabrication Laboratory (FabLab)." Broad Agency Announcement. 11 April 2017. www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=8a6ebb526d8bf8fb9c6361cb8b50c1f8&_c view=1

"In Situ Monitoring and Process Control." Made in Space. Small Business Innovative Research (SBIR) abstract. 2018. < https://www.sbir.gov/sbirsearch/detail/1559743>

"In Situ Monitoring of In-Space Manufacturing by Multi-Parameter Imaging." LER Technologies. Small Business Innovative Research (SBIR) abstract. 2018. https://www.sbir.gov/sbirsearch/detail/1559833>

Kim, H. Wu, D.I. Moon, M.L. Seol, B. Kim, D.I. Lee, J.W. Han, and M. Meyyappan. "Carbon nanotube Based Gamma Ray Detector." ACS Sensors. Volume 4, 2019, pp. 1097-1102.

Korkut, V., Yavuz, H. In-Space Additive Manufacturing Based on Metal Droplet Generation Using Drop-on-Demand Technique. J. of Materials Eng and Perform, 2022, 31, 6101–6111. https://doi.org/10.1007/s11665-022-06865-7

Kovalchuk, D., Melnyk, V. & Melnyk, I. A Coaxial Wire-Feed Additive Manufacturing of Metal Components Using a Profile Electron Beam in Space Application. J. of Materials Eng and Perform, 2022, 31, 6069–6082. https://doi.org/10.1007/s11665-022-06994-z

Kurk, Andy. "Sintered Inductive Metal Printer with Laser

Enhancement." Proceedings of the National Space and Missile Materials Symposium, Palm Springs, CA. June 2017.

Mantel, K., 1990. Wald und Forst in der Geschichte. M. & H. Schaper, Hannover.

Marsh, Doug. "The VULCAN Advanced Hybrid Manufacturing System." Proceedings of the National Space and Missile Materials Symposium, Henderson, NV. June 2018.

METI, 2004. Handbook on Resource Recycling Legislation and 3R Initiatives. Tokyo: Japanese Ministry of Economy, Trade, and Industry.

Momeni, K., Neshani, S., Uba, C. et al. Engineering the Surface Melt for In-Space Manufacturing of Aluminum Parts. J. of Materials Eng and Perform, 2022, 31, 6092–6100. https://doi.org/10.1007/s11665-022-07054-2

Moraguez, M., O. DeWeck, and T. Prater."Suitability of Manufacturing Processes for In-Space Manufacturing of Spacecraft Components." Proceedings of the 70th International Astronautical Congress, Washington, D.C. 2019.

Muhlbauer, Rachel. "Food-safe, skin contact-safe, and medical device 3D printing for manned space missions." Proceedings of the National Space and Missile Materials Symposium, Palm Springs, CA. June 2017.

Muhlbauer, Rachel. "Metal Advanced Manufacturing Bot Assembly (MAMBA) Process." Small Business Innovative

Research (SBIR) abstract. 2017. http://sbir.nasa.gov/SBIR/abstracts/17/sbir/phase1/SB IR-17-1- H7.02-9710.html

Müller, D.B., et al., *Carbon Emissions of Infrastructure Development*. Environmental Science & Technology, 2013. 47(20): p. 11739-11746.

Munther, D.I. Moon, B. Kim, J.W. Han, K. Davami, and M. Meyyappan, "Array of Chemiresistors for Single Input Multiple Output (SIMO) Variation-Tolerant All Printed Gas Sensor" Sensors and Actuators, Volume 299 pp. 1269-71. 2019.

Nafisi, S., Hofmann, D., Gradl, P. et al. Space and Aerospace Exploration Revolution: Metal Additive Manufacturing. J. of Materials Eng and Perform, 2022, 31, 6011–6012. https://doi.org/10.1007/s11665-022-06929-8

Nobre, G. C., Tavares, E. The quest for a circular economy final definition: A scientific perspective, Journal of Cleaner Production, Volume 314, 2021.

Norfolk, Mark. "Solid State Metal Manufacturing for International Space Station (ISS).", Proceedings of the National Space and Missile Materials Symposium, Henderson, NV. June 2018.

NRC, Microgravity Research in Support of Technologies for the Human Exploration and Development of Space and Planetary Bodies, National Academy Press, Washington, D.C., 2000, pp. 99-100.

OECD, 2007. The Space Economy at a Glance. OECD, Paris.

OECD, 2016. Space and Innovation. OECD, Paris.

OECD, 2019. The Space Economy in Figures: How Space Contributes to the Global Economy. OECD, Paris.

Owens, A., O. C. de Weck, W. Stromgren, W. Cirillo, and K. Goodliff. "Supportability Challenges, Metrics, and Key Decisions for Human Spaceflight."Proceedings of the American Institute of Aeronautics and Astronautics (AIAA) SPACE Forum, Orlando, FL, 2017.

Owens, A., and O. DeWeck. "Systems Analysis of In-Space Manufacturing Applications for International Space Station in Support of the Evolvable Mars Campaign." Proceedings of the American Institute of Aeronautics and Astronautics SPACE Forum, Long Beach, CA. 2016.

Paladini, S., Saha, K., Pierron, X., Sustainable space for a sustainable earth? Circular economy insights from the space sector. Journal of Environmental Management 289, 2021, 112511.

Patankar, Sunil. "Development of Fiber-Reinforced Composite Feedstock for In-Space Manufacturing of High Strength Parts." Proceedings 70th International Astronautical Congress (IAC), Washington, D.C., 21-25 October 2019 of the National Space and Missile Materials Symposium, Henderson, NV. June 2018.

Prater, T., N. Werkheiser, F. Ledbetter, D. Timucin, K. Wheeler, M. Snyder. "3D Printing in Zero G Technology Demonstration Mission: complete experimental results and summary of related materials modeling efforts." The

International Journal of Advanced Manufacturing Technology. Volume 101 (2019): pp. 391-417.

Prater, T., N. Werkheiser, F. Ledbetter, and K. Morgan. "In-Space Manufacturing at NASA Marshall Space Flight Center: A Portfolio of Fabrication and Recycling Technology Development for the International Space Station." Proceedings of the AIAA SPACE Forum, Orlando, FL, 2018.

Prater T., et al., "NASA's In-Space Manufacturing Project: Update on Manufacturing Technologies and Materials to Enable More Sustainable and Safer Exploration", Proceedings 70th International Astronautical Congress (IAC), Washington, D.C., 21-25 October 2019. IAC-19.D3.2B.5.

Riissmann, M., Lorenz, M., Gerbert, P., Waldner, M., Justus, J., Engel, P., Harnisch, M., 2015. Industry 4.0: the Future of Productivity and Growth in Manufacturing Industries. Consulting Group, Boston, pp. 1-14.

Russell, K., 2017. *Thales* Alenia Space Saves Time, Money with 3D Printing, Satellite. https://www.satellitetoday.com/innovation/2017/06/27/3d-printing-future-satellite-manufacturing/. (cited 22 July 2022).

SAP, 2020. SAP Insights. What ls Industry 4.0? Definition, Technologies, Benefits.

https://insights.sap.com/what-is-industry-4-0/. (cited 5August 2022).

Schmuland D., Carpenter C., Masse R., and Overly, J., "New Insights into Additive Manufacturing Processes: Enabling Low-Cost, High- Impulse Propulsion Systems," 27th Annual AIAA/USU Conference on Small Satellites, AIAA Paper SSC13-VII-4, 2013, American Institute of Aeronautics and Astronautics, Reston, Va.

Stewart, B.C., Doude, H.R., Mujahid, S. et al. Novel Selective Laser Printing Via Powder Bed Fusion of Ionic Liquid Harvested Iron for Martian Additive Manufacturing. J. of Materials Eng and Perform, 2022, 31, 6060–6068. https://doi.org/10.1007/s11665-022-06730-7

Su, B., Heshmati, A., Geng, Y., Yu, X., 2013. A review of the circular economy in China: moving from rhetoric to implementation. J. Clean. Prod. 42, 215–227.

SpaceX, 2022. *SpaceX Homepage*. https://www.spacex.com/. (cited 22 July 2022).

U.S. EPA. "Advancing Sustainable Materials Management: 2015 Fact Sheet". 2018.

Volz, Martin, "Materials Science in Microgravity", 3rd Annual ISS Research and Development Conference Chicago, Illinois, June 17-19, 2014.

Warner, Cheryl. "NASA Selects Three Companies to Develop 'FabLab' Prototypes." NASA Press Release. 7 December 2017. www.nasa.gov/press-release/nas-selects-three-companies-to-develop-fablab-prototypes.

PART II

SECTION 2: SPACE CHALLENGES AND OPERATIONS

5.

SPACE BASED PLATFORMS AND CRITICAL INFRASTRUCTURE VULNERABILITY (MCCREIGHT)

CHAPTER 5: SPACE BASED PLATFORMS AND CRITICAL INFRASTRUCTURE VULNERABILITY (MCCREIGHT)

Student Objectives

Students will discuss, analyze and study:

- the nature of critical infrastructure and its various subsystem elements today
- the impact of space-based platforms and technology on critical infrastructures
- the significance of selected space related technologies on

the operational integrity of critical infrastructures and their relevant cyber vulnerabilities

- Potential threat indicators related to space-based platforms after 2023
- Security and risk management issues involving the protection and safeguarding of critical infrastructures from space-based threats as well as expected future challenges

Background

For well over 20 years, we have consistently recognized the existence of critical infrastructures which undergird our nation, its security, its economy, and overall operational integrity. The variety and number of Critical Infrastructures [CI] is significant and subject to modification and expansion based on an objective assessment by national governments of those essential systems which sustain the national security, societal stability, and economic wellbeing [such as clean water and reliable energy] of the nation safeguarding its cohesion and daily operation. Simply put, most modern societies in the 21st century would collapse and fail without reliable CI.

The original list of critical infrastructures outlined in 6 USC 671 in 2002 by language contained in the 'Critical Infrastructure Protection Act' includes a vague reference to ". any component or bureau of a covered Federal agency that has been designated by the President or any agency head to receive critical infrastructure information. (CISA, 2002) Today the broad term symbolizes distinct areas of activity, enterprise and industrial operations which support and guarantee everyday life in the nation. For example, critical infrastructures [CI] encompass energy systems, water and wastewater systems, agriculture and food supply systems and telecommunications to identify just a few. Moreover, it has been clearly established an emphasized that these critical infrastructures are essential to both national and homeland security despite ample evidence that the sheer reliability, performance, operational demands, and risks for each system is distinct in many case while uniformly vulnerable in others.

What is of paramount security interest is assessing the various space-based platforms [seen as distinct potential weapons systems with disruptive capabilities] and gauging their impact on critical infrastructures as they may retain the potential to nullify and adversely affect the normal operations of CI systems especially after 2023. We must recognize that space-based systems and platforms retain their own inherent vulnerabilities apart from the supporting role these orbital systems play in sustaining ground level CI systems. Exploiting space platforms as legitimate targets themselves, when combined with their pivotal role in sustaining certain CI systems, means the layers of security must envelop both aspects. Understanding this emerging security risk and enduring challenge will tax the national and homeland security enterprise in ways unexpected. The special risks arising from cyber intrusions on space systems merits a closer look. This offers an additional vulnerability for space systems apart from ASAT [anti-satellite weapons], directed energy systems, particle beam weapons and lasers to name a few.

Space systems are usually divided into several technological and operational segments, which are responsible for different functions and components all vulnerable to cyber intrusion to some degree. Together Ground Stations, Mission Control Centers, Ground Networks, Remote Infrastructure, and Launch Facilities work together to enable management of spacecraft, payload data, and telemetry. Most often exposed to different cyber threats are the ground segment, the space segment, and the link segment. Each segment presents its own unique vestiges of cyber risk and vulnerability. (Weigel, n.d.)

The ground segment consists of all the ground elements of space systems and allows command, control and management of the satellite itself and the data arriving from the payload and delivered to the users. Due to their role in collecting data, the ground stations and terminals are exposed to the threat of cyber espionage from states and non-state actors. Moreover, the military aspect of satellites and their importance to national security render them prime targets for hostile takeover, disruption, and shutdown. Most cyberattacks on the ground segment exploit web vulnerabilities and allow the attacker to lure ground station personnel to download malwares and Trojans to ground stations' computers. Infiltrating the ground station's network can allow the attackers to access the satellite itself. Hostile access could enable the attacker to execute a Denial of Service (DoS) attack and may involve taking over Industrial Control Systems (ICS) in order to control the satellite and damage it.

The space segment consists of the satellites themselves. Major security gaps within satellites' architecture exist in both old and new satellites. Old satellites with life spans of decades were built with no awareness for cyber security; today, small satellites manufacturers tend to prioritize fast and cheap production, in which the investment in cyber security is perceived as a hurdle. Cyber threats to space segments usually derive from vulnerabilities in ground stations, in network components, and in the receivers which receive the data from the satellite, thus allowing the attacker to infiltrate to the network and remain undetected. Another threat may involve the introduction of a malware into the satellite's hardware in the supply chain, in order to compromise ground units at a later stage. Consequences of cyberattacks on satellites could also be aggravated due to the rising connection and use of Internet of Things (IoT) devices. An attack on a communication satellite could cause wide disruptions to communication channels across countries, cause panic, and endanger national security.

The link segment consists of the signal transmission between the satellite and the ground station, as well as between satellites. The most common threat is GPS jamming. As GPS systems rely on radio signals sent from the satellite in order to determine the location of the users, GPS jammers send signals over the same frequency as the GPS device, in order to override or distort the GPS satellite signals. GPS jammers are widely accessible and cheap to purchase, rendering them available also to poorer state-actors. In November 2018, Russia was suspected of disrupting GPS signals in northern Norway and Finland as the two nations participated in NATO's Trident Juncture exercise. Another type of attack is 'spoofing' – faking signals by broadcasting incorrect GPS signals, structured to resemble genuine ones. Spoofing is harder to carry out than jamming, but if executed effectively, can be much more dangerous, mainly because the victims do not necessarily know that they are being spoofed. According to a 2017 US Maritime Administration report, the GPS systems of at least 20 ships were spoofed, leading the ships 32 kilometers inland to the Gelendzhik Airport in the Black Sea, away from the original destination. The incident raised assumptions among experts that Russia had been experimenting new GPS spoofing techniques as part of its electronic warfare capabilities. While some experts define jamming and spoofing as physical threats as they involve disrupting or tampering with frequency signaling, an attacker could also intercept unencrypted satellite traffic. (Wechsler, 2020)

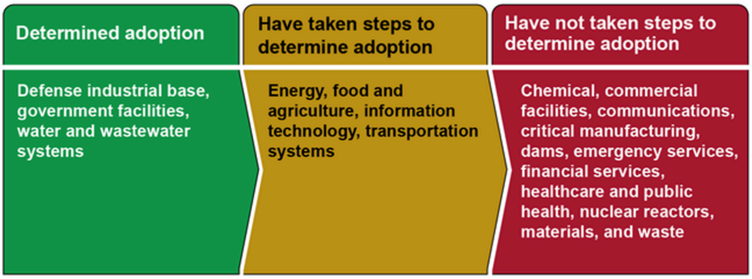
Critical Infrastructure, [Ci] A Foundational Achilles Heel, Today and Tomorrow

The Department of Homeland Security has defined, categorized, and described what critical infrastructure [CI] means and includes a list of essential systems as of 2022 in various official documents including the National Infrastructure Protection Plan [NIPP]. What is just as important is the list of current, as well as potentially relevant other critical infrastructures, which provide the secure operational backbone of our nation's economy, societal wellbeing, and security. For the last two decades each of the enumerated CI systems have been studied and evaluated to discern their fundamental operational requirements, system strengths, vulnerabilities, maintenance issues and security aspects. Each distinct CI system is reviewed and administered via the Department of Homeland Security [DHS] and there have been some interesting studies since 2002 which drew attention to significant operational and security issues. For example, via the National Critical Infrastructure Prioritization Program, the DHS oversight agency known as the Cybersecurity and Infrastructure Security Agency (CISA) is required to identify a list of CI systems and assets that, if destroyed or disrupted, would cause national or regional catastrophic effects.

Back in 2007, for example, GAO found that certain CI control systems faced increasing risks due to cyber threats, system vulnerabilities, and the serious potential impact of attacks as demonstrated by reported incidents. Threats can be intentional or unintentional, targeted or nontargeted, and can come from a variety of sources. Control systems are more vulnerable to cyber-attacks than in the past for several reasons, including their increased connectivity to other systems and the Internet. Further, as demonstrated by past attacks and incidents involving control systems, the impact on a critical infrastructure could be substantial. Control systems—computer-based systems [such as SCADA-Supervisory Control and Data Acquisition]] that monitor and control sensitive processes—perform vital safety and operational reliability functions can be found in many of our nation's critical infrastructures such as electric power generation, transmission, and distribution; oil and gas refining; and water treatment and distribution. The disruption of control systems could have a significant impact on public health and safety, which makes securing them a national priority. Subsequent studies and objective evaluations have identified other similar issues. (GAO, 2007)

CI systems have been known to be sensitive to solar storms, targeted terror attacks, and EMP explosions in addition to their cyber weaknesses. In a recent 2022 GAO report CI stakeholders identified cyberattacks as among the most prevalent threats they faced but said that the program's list was not reflective of this threat. Further, according to CISA data, since fiscal year 2017, no more than 14 states (of 56 states and territories) provided updates to the program in any given fiscal year. Ensuring that its process for determining priorities reflects current threats, such as cyberattacks, and incorporates input from additional states would give CISA greater assurance that it and stakeholders are focused on the highest priorities. Here, with high emphasis on protecting various CI systems against cyberattack, EMP or terrorist intrusion GAO found three major sectors had adopted cyber defense strategies while others were mired in various stages of adoption or implementation. The chart below illustrates one dimension of the cyber risk issue as GAO depicted it. [GAO Report-105102, Adopting Cybersecurity Frameworks in Critical Infrastructure, Feb 2022] (Sharon, 2022)

Figure 5-1 Status of Cyber Security Framework Adoption by Critical Infrastructure Sector



Determined adoption	Have taken steps to determine adoption	Have not taken steps to determine adoption
Defense industrial base, government facilities, water and wastewater systems	Energy, food and agriculture, information technology, transportation systems	Chemical, commercial facilities, communications, critical manufacturing, dams, emergency services, financial services, healthcare and public health, nuclear reactors, materials, and waste

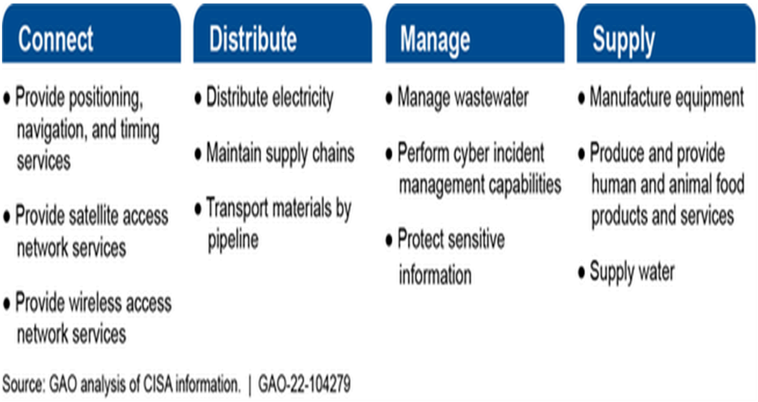
Source: GAO analysis based on agency data. | GAO-22-105103

Source: (GAO-22-105103, 2022)

According to CISA officials, a National Critical Functions framework established in 2020 was intended to better assess how failures in key systems, assets, components, and technologies may cascade across the 16 critical infrastructure sectors. Examples of critical functions are shown below in

CISA's four broad categories of "connect" (nine of the 55 functions), "distribute" (nine), "manage" (24), and "supply" (13). Cascading systems failures and disruptions are especially significant from the standpoint of ensuring continued reliable and secure operations and the inherent risks that system collapse in one area triggers failure to other CI systems. Cascading collapse or failure in one CI system can adversely affect others. Traditionally, this cascading risk has most often been assigned to the energy grid. This chart illustrates the CISA scheme for arraying National Critical Functions (GAO-22-104279, 2022)

Figure 5-2 CISA Should Improve Priority Setting, Stakeholder Involvement, and Threat Information Sharing



Connect	Distribute	Manage	Supply
• Provide positioning, navigation, and timing services • Provide satellite access network services • Provide wireless access network services	• Distribute electricity • Maintain supply chains • Transport materials by pipeline	• Manage wastewater • Perform cyber incident management capabilities • Protect sensitive information	• Manufacture equipment • Produce and provide human and animal food products and services • Supply water

Source: GAO analysis of CISA information. | GAO-22-104279

Source: (GAO-22-104279, 2022)

CISA is currently carrying out a process to break down each of the 55 national critical functions (such as "supply water") into systems (such as "public water systems") and assets (including infrastructure such as "water treatment plants". In addition, the cascading shutdown dynamic which refers to energy loss triggering other dependent CI systems failing cannot be overlooked. This is a long, complex analytical process but includes consideration of selected factors deemed to place earth-based CI systems at greatest risk. These include

- Solar storms and geomagnetic waves [errant asteroids]
- Electromagnetic Pulse [EMP] weapons
- Terrorist attacks [physical or cyber]
- Insider threats/sabotage [criminal activity]

Today we must consider other potential threats to normal CI operations beyond that short list. That would include the emergence of sophisticated space-based weapons platforms which, depending on their inherent capabilities, could cripple or destroy selected CI systems. This would include space platform failures to protect friendly CI systems as well as hostile space-based attacks on CI. Before outlining these space-based threats, a routine inventory of CI systems is needed first. Here are the identified 16 CI systems which, as of 2021, CISA and DHS regard as bedrock value to homeland security.

In 2022, the specific array of diversified CI systems which

DHS officially recognizes, and which are central and pivotal to our national and homeland security include the following major areas:

-Chemical/Petrochemical and Natural Gas Processing Facilities

-Energy systems and Energy producing organizations

-Nuclear Reactors/Nuclear Waste management

-Commercial/Business organizations and corporate enterprises

-Public Telecommunications/Internet Management/Voice-Phone-Data

-Defense Industrial Base [equipment/finished weapons systems, research & development, etc.]

-Critical Manufacturing organizations

-Dams, levees, flood control and seawall barriers

-Emergency Services Sector

-Public Health systems

-Food Supply/Agriculture

-Transportation/Trade/Shipping/Maritime and Port Security

-Financial and Economic Transfer services

-Key Government agencies and facilities

-Information Technology/Cyber Systems

Each distinct system has its own functional characteristics, operational norms, requisite technological and resource requirements, and aspects which raise issues of security and assured stability of continued performance in normal situations. Too often we reckon with calculated irony that every conceivable crisis scenario and set of demands affecting each CI system cannot be effectively deterred or nullified in all scenarios or circumstances. Clearly, those systems which are reliant on dependable energy sources and uninterrupted cyber and information/telecommunications technologies are most likely to require more robust and redundant security safeguards than other CI elements because they undergird and support the others. For example, the safety, security, and operational control systems which support and manage the daily activities of chemical plants rely heavily on reliable electric power and related energy sources to maintain the integrity of their various programs and functions. The photo below demonstrates just one small aspect of this CI system where safe and secure storage of finished and unblended chemicals enables the chemical industry to perform its ordinary work. (Nichols & Mumm, 2020)

Figure 5-3 Chemical Facility Storage Tanks [DHS-2018]

Source: Department of Homeland Security.

Source: (Primary) (GAO-20-453, 2020)

So, one paramount security issue to ensure the smooth and reliable functioning of CI systems is their ultimate reliance on energy regardless of threat, disruption, or extended crisis. External threats to that energy source where sporadic or reduced energy loads, or indefinitely cancelled energy supplies, jeopardize continued operations indicates a prime area where special protective measures, security system safeguards and threat nullification measures are needed. In many cases these adaptive security safeguards must be devised, engineered, and developed to fit the unique operational requirements of the specific CI system needing an upgrade.

CI systems reliant on consistently reliable cyber connectivity must also be considered. Earlier in 2022 Congress passed the Cyber Incident Reporting for Critical Infrastructures Act [CIRCIA] which marks an important milestone in improving America's cybersecurity. While law does not eliminate all cyber risks and concerns it recognizes in our modern complex society is the ever-present risk of cyber warfare designed to disable and weaken an adversary prior to an all-out attack. The primary worry in a surprise cyber-attack is that there will be collateral damage to the critical infrastructure of allied and friendly countries not directly involved in the current conflict.

Today, services such as healthcare systems, power grids, transportation and other critical industries are increasingly integrating their operational technology with traditional IT systems in order to modernize their infrastructure. As such, these CI systems are open to a new wave of covert cyberattacks many of which are largely undetectable or preventable . The continuing conundrum of designing effective cyber deterrent measures and technologies against future cyber threats further complicates this risk terrain and makes estimations of evolving jeopardy to our own vulnerable cyber systems where AI and quantum may be involved is very serious.

While many businesses have ramped up their security initiatives and investments to defend and protect their own commercial interests, their efforts involving security upgrades and protective measures have been piecemeal, reactive, limited and lack uniform business context across all enterprises large and small. Further the digitalization of critical infrastructure, coupled with increased dependence on third parties, has made it vulnerable to ongoing cyberattacks across multiple vectors in a global network of shared communications. Supply chain attacks are becoming increasingly commonplace with several critical infrastructure businesses being compromised as collateral damage is inflicted or they become crippled by targeted ransomware attacks. These companies in various sizes now must monitor and manage employee workforce risk, third, fourth, criminal dark web intruders and other parties (not just their vendors, but their partners and suppliers' networks, too), where the native technology stack, compliance, and regulatory frameworks, including internal policies and processes may be flawed or porous.

Vulnerabilities to cyber intrusion are several and experts agree those CI systems most at risk include energy, water, food supply, transportation, finance, and healthcare systems that are needed every day for national survival. Safeguarding these interconnected systems is crucial to assure national and homeland security against a daily onslaught of cyber probes and threats. The ability to disable and deny access to any of these resources is a massive threat to any country's economy and its continued security and stability. Worse, cyber intrusions open the door to an attacker gaining control over space systems and networks, which could have devastating consequences. That attack could come from foreign enemies as well as determined terror groups.

Again, the energy grid in particular has often exhibited a frailty owing to risks of external cyber intrusion and influence. Fundamentally the energy grid, and all the other related CI systems which it supports, is the prime CI concern to achieve the highest reliability assurance possible against disruption, breakdown, and system loss. The energy grid is complex and diversified reflecting variety of designated zones for daily service. Extra high voltage (EHV) transformers are critical components of our nation's backbone transmission grid. Approximately 90 percent of consumed power flows through the transmission grid and through such a transformer. These EHV transformers are very large, challenging to transport, and often have lengthy procurement times of one year or greater. There integral subcomponents include circuit breakers; isolators;– instrument transformers; surge arresters; neutral-earthing reactors; current-limiting reactors;

shunt reactors and capacitor banks all of them vital to secure continuous operations involving many EHV substations which may have several configurations (topologies), depending on continuity requirements, as well as the reliability and the quality of power supply. (electricaltechnology, 2018)

In addition to federally sponsored efforts many State and local entities have taken the initiative towards proactively assessing, prioritizing, and managing threats. Resources and options for investing incremental budget increases among all CI sectors is always constrained by shifting priorities. Both public and private sector organizations can share information and cyber defense best practices in critical infrastructure communities of interest, such as CISA's Information Sharing and Analysis Centers. There are also many popular commercially backed exchanges where information can be shared specific to critical infrastructure threats. Cyber risk quantification, backed by sound data science principles, has a unique opportunity to help mitigate and solve this challenge. Two key steps involve information and technology management best practices, to include network segmentation, multi factor authentication, network access control, etc. Organizations also need to implement quantitative risk management, ensuring they are able to properly assess, prioritize, and manage their relative cybersecurity risks. (CISA, 2022)

(CISA) conducts specialized but voluntary security and resilience assessments on the CI systems to assist CISA and its federal, state, local partners—and private industry—to better understand and manage disruptive CI risks. The assessments examine infrastructure vulnerabilities, interdependencies, capability gaps, and the consequences of their disruption. Vulnerability assessments, combined with infrastructure planning resources developed through the CISA sponsored Infrastructure Development and Recovery program forms an integrated planning and assessment capability. This suite of capabilities, methods, and tools support the efficient and effective use of resources to enhance critical infrastructure resilience to all hazards

Because most U.S. critical infrastructure is privately owned, the effectiveness of CISA assessments depends upon the voluntary collaboration of private sector owners and operators. CISA's Protective Security Advisors (PSAs) work collaboratively to foster and facilitate technical assistance to buttress of the security and resilience of the Nation's critical infrastructure. Assessments are offered through the PSAs at the request of critical infrastructure owners and operators and other state, local, tribal, and territorial officials. The question is—what else about CI systems interacting with space-based platforms signals a security concern?

A Brief Excursion into Cyber/Satellite Attacks on CI

Several CI systems exhibit a degree of vulnerability to cyber/space systems intrusion and disruption. For example, nuclear plants are composed of an impressive number of components such as SCADA/ICS, sensors and legacy systems that could be hit by a hacker. The most popular case of a cyber-attack was against a nuclear plant launched in 2010 . Known as Stuxnet the attack involved malware developed by experts from the US and Israel with the intent of destroying or disabling the Iranian nuclear program. Hackers hit the plant of Natanz in Iran in 2010 interfering with the nuclear program of the Government of Teheran. The Stuxnet targeted a grid of 984 converters, the same industrial equipment that international inspectors found out of order when visited the Natanz enrichment facility in late 2009. IAEA inspectors noted, "The cyber-attack against the Cascade Protection System infects Siemens S7-417 controllers with a matching configuration. The S7-417 is a top-of-the-line industrial controller for big automation tasks. In Natanz, it is used to control the valves and pressure sensors of up to six cascades (or 984 centrifuges) that share common feed, product, and tails stations'. Stuxnet was designed with a number of features that allowed to evade detection; its source code was digitally signed, and the malware uses a man-in-the-middle attack to fool the operators into thinking everything is normal. Stuxnet proves it is possible to use a malicious code to destroy operations at a nuclear plant. Experts and authorities confirm a continued risk of future cyber-attacks exists, also involving satellite systems which can enable such attacks, against Nuclear plants. (Langner, 2013)

In 2021, two Russian COSMOS satellites in orbit were stalking a US spy satellite high above the earth. It wasn't clear if they could attack U.S.-245, an American surveillance spacecraft, already in orbit. The incident passed, but it marked a new stage in the mounting arms race in space, where potentially bomb-armed satellites, laser-shooting spacecraft and other 'satellite kamikaze' technologies have moved from science fiction to reality. The stakes were made clear recently when Russia launched a missile from Earth and blasted to pieces one of its satellites in a show of force. (phys.org, 2021)

China has tested a maneuverable satellite that has demonstrated potential anti-satellite (ASAT) capabilities joining similar Russian efforts aimed at attacking US satellites, says a new study by CSIS. Recently the US used its X-37B spaceplane to covertly launch several CubeSats that could demonstrate its ASAT capabilities and practiced extensive GPS jamming during several naval exercises. And India joined the ASAT club as the fourth country to test a kinetic-kill ASAT, while France and Japan intensified exploration of new ASAT capabilities, according to the Center for Strategic and International Studies (CSIS). The three CSIS studies [2019,2020,2021] offer an analytical series which finds a major overall increase in the ability of nation-state space antagonists to threaten each other's satellites, as well as an expanded number of countries pursuing ground- and space-based capabilities to damage or destroy satellite systems. For example, the 2021 CSIS report says the U.S. Space Force notes that, "military space forces should make every effort to promote responsible norms of behavior that perpetuate space as a safe and open environment in accordance with the Laws of Armed Conflict, the Outer Space Treaty, and international law, as well as U.S. government and DoD policy." Counterspace weapons, particularly those that produce orbital debris, pose a serious risk to the space environment and the ability of all nations to use the space domain for prosperity and security. (Harrison, 2021)

These reports note that China, Russia, Iran, North Korea, India, France, Israel, UK, Japan, South Korea, all display diverse investments and enthusiasm for increased space platform launches and activity while major differences exist between them about adopting, let alone enforcing, norms applicable to satellite systems. Other CI systems are also clearly at risk as long as cyber avenues to their disruption are real and ever present. In contrast to nuclear plants, the idea that reliable access to water, especially the clean, drinkable kind, has become yet another CI battlefield. Security experts have noted that many national and local water and wastewater systems are extremely vulnerable to attacks by cyber criminals. In 2020, an unknown hacker or group of hackers was able to gain access to the operations technology (OT) system of a water treatment plant in Oldsmar, Florida attempting to poison the water supply by increasing the amount of sodium hydroxide, also known as lye, in the water from 100 parts per million to 11,100 parts per million. The attempt was thwarted by an operator who was able to reverse the change to the settings before the toxic levels of the chemical reached the water. In June 2021 NBC News claimed that a hacker attempted to poison a water treatment plant that served parts of the San Francisco Bay Area a few months earlier. (MaGill, 2021)

Finally, another example arising in Germany dealt with wind turbine operators reporting a fault in the satellite connection of their systems saying the remote monitoring and control of thousands of wind turbines had failed. The failure coincided with the Russian invasion of Ukraine making German officials suspect a Moscow-led cyber-attack. Instead, a spokesperson for the German Wind Energy Association said the disruption was due to the failure of the KA-Sat communication satellite belonging to ViaSat where turbine shutdowns appeared to be based. German wind turbine operators first reported the remote monitoring and control of thousands of wind turbines had failed due to suspected collateral damage from a Russian cyber-attack on a primarily military target. The KA-Sat network is also used by satellite communication service provider Euroskypark. Wind turbines in areas without mobile network coverage use satellite-supported communication for control and remote monitoring. Euroskypark could not be reached for comment. (Willuhn, 2022)

Grasping Space Systems and Platforms as New Critical Infrastructure

Today we must also confront another relevant CI system not officially listed with those which CISA/DHS have recognized as of 2022 but which reflect the shifting security environment of tomorrow—is space platforms and systems. During the recent 2022 Satellite conference, guest speaker Peter Hoene president and CEO of SES Government Solutions, a telecommunications services provider from Luxembourg said '…we are facing incredible threats from space-based systems,". We must also recognize the Russia-Ukraine conflict illustrates how crucial the commercial space sector, multinational satellite communications companies, and those businesses that sell remote sensing data and images are part of tomorrow's armed battles. . This would also include small businesses that supply space subsystems, launch companies, ground-station servicers, and cybersecurity support providers. With the successful launch of Space X many others followed suit.

The National Geo-Spatial Intelligence Agency declared years ago that it would buy space imagery from private sector companies. This changed the game board significantly. Remote sensing was once the purview of the military and spy agencies and less secretive NASA and NOAA for Earth observation causing the commercial space-data-as-a-service industry to explode in significance. With it, however, is an awareness of new threats. There is even the threat of "killer satellites," maneuverable spacecraft that could potentially cripple spacecraft using robotic arms or destroy them with kinetic force. One challenge remains inside the private sector is the dicey question of protecting intellectual property and patented technologies which often prevents commercial space companies from sharing data on their respective vulnerabilities.

War and interstate conflict must include a cyber and space offensive dimension after 2020 knowing that states with the ability to execute attacks in both spheres will likely do so with impunity. The ViaSat company suffered an attack at the outset of the Ukraine war, which according to press reports, knocked out users' modems throughout Europe. With the Ukraine war its government leaders warned of possible cyberattacks on domestic and international satellite systems with increased geopolitical uncertainty. Satellite systems are prone to a variety of threats and Russia amply demonstrated that in late 2021 by launching an anti-satellite test destroying a defunct spacecraft using an anti-ballistic interceptor missile. Space systems are also vulnerable to signal jamming, laser dazzling — which blinds remote sensing satellites — and cyberattacks, both in space and directed toward ground systems. (Magnuson, 2022)

Speaker Sam Costak, the national counterintelligence officer for space at the Office of the Director of National Intelligence said at the conference "While space is not designated technically as critical infrastructure, I think we can all agree that all of the critical infrastructure sectors rely on space...and the commercial space industry is just continuing to grow beyond what anybody ever thought would happen," Commercial space system providers must be factored into the conversations because despite military systems used for surveillance, reconnaissance and communication the Pentagon uses less than 15% of the space assets orbiting our planet. Private sector space companies are looking to invest in more space systems if the Pentagon can provide leasing and security assurances. Costak also said, ".the government is currently taking steps to add space to its critical infrastructure list." Back in May 2021, CISA formed the space systems critical infrastructure working group, designed to function as "a mix of government and industry members that will identify and develop strategies to minimize risks to space systems that support the nation's critical infrastructure. (Magnuson, 2022)

In addition, a white paper released in 2021 by the Intelligence and National Security Alliance (INSA) calls for the formal designation of U.S. space systems as a new sector of U.S. critical infrastructure. Developed by INSA's Cyber Council, the paper, Designating the U.S. Space Sector as Critical Infrastructure, notes that space systems have become vital to U.S. national and economic security even though space-related assets were not considered as one of 16 critical infrastructure sectors designated by the 2013 Presidential Policy Directive on Critical Infrastructure Security and Resilience (PPD-21). Space assets are now integrated into almost all essential sectors and functions, including defense, agriculture, transportation, energy, and telecommunications. Designating the space sector as critical infrastructure, the paper asserts, would enhance the resiliency of space-related assets and thereby make these other critical infrastructure sectors more secure. "Space-related capabilities have become essential to both national security and economic security, yet countries like Russia and China – which have advanced offensive cyber capabilities and anti-satellite weapons – have the potential to take them offline," said Larry Hanauer, INSA's Vice President for Policy. "Designating the space sector as part of the nation's critical infrastructure would make it easier for government organizations, the military, and commercial space companies to share information on threats and vulnerabilities and thereby enhance the space sector's resilience." (INSA, 2021)

The space sector includes mission control, launch facilities, more than 6,500 satellites currently in orbit, [some active and some not] deployed by a wide range of companies and universities engaged in advanced research & development and technology deployment. Some experts predict the space industry will reach almost $1.5 trillion in value by end of 2030. Designating the space sector as the United States' newest critical infrastructure sector would clarify government agencies' roles and responsibilities in protecting it and make clear to U.S. adversaries that the United States is committed to defending its space infrastructure, contribute to the establishment of global norms regarding the safety and security of space systems, and accelerate development of best practices and technologies for ensuring cybersecurity and resilience of space. (INSA, 2021)

When CISA established the Space Systems Critical Infrastructure Working Group [SSCIWG] in 2021 CISA's acting director Brandon Wales remarked, "The critical infrastructure on which the United States depends relies heavily on space systems. Increasing the security and resilience of space systems is essential to supporting the American people, economy, and homeland security. Secure and resilient space-based assets are critical to our economy, prosperity, and our national security," He also said, "This cross sector working group will lay the foundation for our collective defense against the threats we face today and in the future." noting, "this working group will serve as an important mechanism to improve the security and resilience of commercial space systems. It will identify and offer solutions to areas that need improvement in both the government and private sectors and will develop recommendations to effectively manage risk to space based assets and critical functions." (CISA, 2021)

Further at a conference in October 2021, an experts panel discussed the need to consider space systems as part of our nation's critical infrastructure due to its unique technologies and capabilities combined with its interdependence with other critical infrastructure sectors. Dawn Beyer, senior fellow at Lockheed Martin, was quoted saying "We're still debating whether space is critical infrastructure, meanwhile of all the domains, space is the furthest behind when it comes to cybersecurity." Samuel Visner, technical fellow at MITRE and member of the ISAC board of directors, noted that "Our adversaries see space as critical to their national interest, they see space as critical to our national interest, and frankly I think they see it as a vulnerability to our national interest that they can exploit." (Bahr, 2021)

Recognizing the value of supporting and reinforcing space-based systems which undergird CI systems is important however, beyond that fact is the issue of increasing dependency of CI systems on space platforms and the extent to which those platforms can be arrayed to target and disable CI systems as a prelude to war or other armed conflict This is much less well known and examined and will be the subject of discussion later in this chapter.

Greater Dependency of CI on Space Systems Creates New Security Concerns

Space assets require protection from extremely hostile environments where ground-based attacks, attacks from other space platforms, and cyber enabled attacks originating anywhere can happen frequently and without warning. . Attacks from cyber-space can be shown to be as harmful to spacecraft, and to their ground-based data and support systems, as radiation belts and temperature extremes have always been. To the extent that certain space systems and platforms are the targets of disruptive cyber-attacks reinforces the notion that CI systems are also in some indirect jeopardy from those cyber probes. Some examples years ago of adversarial cyber activity against space assets found in the open literature include:

–"On July 23, 2008, Landsat-7 experienced 12 or more minutes of interference. The responsible party did not fulfill all steps required to command the satellite."

— "On October 22, 2008, Terra EOS AM-1 experienced nine minutes of interference. The responsible party fulfilled all steps required to command the satellite but did not do so."

–"On June 2012, a Romanian national known as 'Tinkode' pleaded guilty in Romanian court to charges of illegally accessing numerous NASA systems as it seems the Pentagon, the Romanian government, and U.S. commercial entities were also involved in the case

In 2014 the Director of National Intelligence wrote in particular about space: "Threats to US space services will increase during 2014 and the decade beyond as potential adversaries pursue disruptive and destructive counterspace capabilities' Chinese and Russian military leaders understand the unique information advantages afforded by space systems and are developing capabilities to disrupt US use of space in a conflict. For example, Chinese military writings highlight the need to interfere with, damage, and destroy reconnaissance, navigation, and communication satellites. China has satellite jamming capabilities and is pursuing antisatellite systems. In 2007, China conducted a destructive antisatellite test against its own satellite. Russia's 2010 military doctrine emphasizes space defense as a vital component of its national defense. Russian leaders openly maintain that the Russian armed forces have antisatellite weapons and conduct antisatellite research. Russia has satellite jammers and is also pursuing antisatellite systems." (Byrne, 2014)

The key issue of satellite controls raises three risks that must be mitigated: (1) the potential for an adversary to remotely introduce a false satellite command; and (2) the potential for an adversary to prevent the satellite operator from transmitting daily commands or receive telemetry from the satellite; and (3) an adversary could wrest hostile extended control of satellite systems from their owner/operators using cyber or related interventions. " Unfortunately, specific, detailed, information about particular incidents are hard to find in the open literature including- details describing the exact commands issued by the adversary, or the various avenues of cyber access to the space system environment at the time of the attack. Worse, limited post incident forensics often make it extremely difficult for defenders to construct a viable defense for their own space systems. Regrettably, asserting that existing controls will protect against current and future risks, or that all vulnerabilities have been remedied is sometimes accepted without reasonable supporting data. Worse, it is accepted where the lack of data is used as proof. It is important to note that as the cyber-threat environment changes, cyber defenses need to be implemented or adapted to keep pace. This can only get more complicated with the onset of quantum computers and their unhackable attributes. Cyber-attackers of today and tomorrow are malicious, persistent, and evolve their attacks over time. By contrast, radiation doesn't change the way it attacks materials after you've chosen your shielding. Continual study of changing adversarial actions with respect to the operational needs of a mission is an important process that must supplement the more static failure model approaches currently prevalent in mission design. (Byrne, 2014)

Cyber Defense architectures, designs, and mitigation strategies must be evaluated against a range of conditions that reflect the existing and expected threat environment and cannot be static or adopt the 'one size fits all' philosophy. Whatever verification activity is adopted it must cover at least these attributes: [1] Range of conditions (not just single or "best case" points); [2] Observable behaviors; [3] Comparable observations; [4] Repeatable tests; and [5] worst case scenarios. Test demonstrations must raise awareness that existing fault containment zones were inadequate in providing protections, contained gaps, or did not operate as originally intended, to provide. Considering a normal systems assurance lifecycle featuring development, integration & test, and conventional operations. Tests must be robust enough to reveal a potential security breach or an exploitable weakness in a given system. Hopefully, these tests will help identify where in the systems testing and demonstration phases that existing security controls had gaps in their coverage. This is technically tough but not impossible and consideration of using red team penetration exercises to identify and root out weaknesses ought to be considered.

There is also the ever-present threat to space platforms and systems from EW [electronic warfare] technologies. This would include identification, interception, and characterization [friend or foe analysis] of deliberate or unintended electronic warfare signals and pulses. These EW considerations would also include aspects of false targeting, uplink or downlink interference, phantom or duplicate target generation, faux surveillance, degrading radiation and signal jamming. EW spoofing attacks launched via cyber mechanisms can cause GPS receivers to provide the wrong information about satellite position, time, and signal coordinates. Mitigation and defense measures can include masking, hardening and engineered deterrence subsystems.

Space and Satellite Systems and Platforms can Monitor CI

Satellite technology plays an important role in the monitoring of and response to infrastructure problems. For example, heavy machinery at ground level that's in the wrong place where disasters or hazards occur can be identified before major damage is done. Some examples which illustrate the infrastructure monitoring value of satellites include:

Communications. Satellites are integral to support global communications systems especially in a remote area or if the client needs a redundant communications plan to avoid loss of connection and its wide coverage radius allows connectivity with otherwise inaccessible locations.

Optical images. Optical sensors perform like a camera sensor capturing high resolution images for photography–or low-resolution options–where the distance between pixels equals more than 100 feet, while others can capture a distance of less than three feet between pixels. However optical sensors can't penetrate cloud cover or capture images in darkness since they rely on reflected light. This makes them unreliable during changing weather conditions and at night.

SAR images Synthetic aperture radar sensors operate on a higher frequency in the electromagnetic spectrum versus optical sensors. They transmit microwaves and measure backscattered radiation that is received analyzed and pictured as a two-dimensional image. The main advantages of SAR are its abilities to see through cloud cover and capture images in the dark.

Thermal images. Thermal image sensors capture infrared radiation from the Earth using a spectrum of colors based on temperature differences. Thermals have proven value in monitoring power lines, but often space based spatial resolution is much less precise than small aircraft (plane, helicopter, or UAV), which deliver much higher resolutions. They are also useful also in tracking changes in the composition of the land or pinpointing sudden changes observed around the infrastructure's general location to predict threats or risks which can be natural or man-made. Some specific applications of these space systems include

Pipeline monitoring. When oil and gas pipelines are buried 5 feet underground often, they are. vulnerable to construction accidents which can trigger a majority of gas pipeline failures. With well over 2 million miles of pipeline in the world, using ground-based solutions or small-craft aerial images is without real value and infeasible. Imaging satellites provide wide coverage and high-resolution alerts to companies tracking macro changes in physical pipelines – i.e., explosions, damaged segments, or ground movements – so that fixes can be made quickly.

Power line monitoring Utility companies which routinely monitor the health of power lines in their service area or to offset risks of major downtime can use aerial images used by companies to make decisions regarding maintenance of power line conductors with a reported rate of 90% accuracy. When paired with new, powerful AI image analysis software, future decisions could become more efficient and incorporate a high degree of automation, lowering response times.

Railway monitoring. Finding significant weaknesses or deformation along railway tracks is crucial to reduce the potential for disastrous consequences. SAR satellites can track extremely precise changes over enormous distances enabling random scanning of construction accidents quickly. SAR satellites can identify rail gaps and deformations which merit immediate attention. (Morgan, 2020)

Reckoning with the vulnerability of satellite communications to cyber manipulation is critical to grasping their contributing role in assuring CI stability of everyday operations. GPS and related geo-location services rooted in satellites illustrate one prime security concern. Increased deployment of satellites have left space-based assets a target for hackers looking to compromise sensitive information, for terrorist, criminal or hostile nation aims with potentially devastating consequences. With the stakes so high when it comes to protecting the data that satellites carry, security cannot be an afterthought and it must play an integral part of the design process itself.

Satellite ground technology is also advancing with more innovation and scalability, as it looks to leverage virtualization, orchestration, and network splicing to support 5G connectivity. Software-defined satellites that can be reprogrammed to move capacity based on market demands create additional problems. With many new 5G and IoT applications these connections open up potential doors for hackers making satellites the new gateway. This jacks up the requirement for smarter satellite security and protection from hackers. There was a time when satellites seemed almost untouchable, but today's hackers can purchase and operate the right equipment such as an antenna at a satellite and send communication to it and influence its normal operations.

Security is the most significant area of technical concern for most organizations deploying IoT systems and now 5G networks, with multiple devices connected across networks, platforms, and devices. This is also true for satellite, given the size and scope, as well as the number of earth station access points. The rise in IoT means if one single device isn't encrypted or the communication isn't protected, a bad actor can manipulate it and potentially a whole network of connected devices. It isn't just the devices themselves that need to be protected, but it is also every stage of data transmission too.

A key first step is for organizations to understand the vulnerabilities they have and how they can be exploited such as legacy satellite communications that are not easily updated. Significant testing must be completed to ensure upgrades for communication with next-generation platforms will not interfere or impact other key system functions. Weak encryption and old IT equipment are key vulnerabilities for satellite networks, which are a prime target for hackers to exploit. So, for over 1,500 satellites in orbit today encryption and other network security measures are essential and enable communications to be authenticated at every stage of data transmission between earth-bound devices and satellites. For authentication to work as designed enabling devices must meet compliance requirements at the networking level to safeguard data when traveling across the satellite ecosystem.

Real-time security solutions are essential because any that do not operate in real-time offer hackers an infiltration route allowing them to be in and out in seconds. Satellites play foundational roles in GPS, time validation , geolocation, weather, traffic, ATMs, video conferencing, TV and radio, inventory control, pay at pump gas stations, phone and broadband, air traffic control systems, sea navigation systems, and the vehicle navigation features used in our cars. Many countries routinely use satellites in these primary areas:

Intelligence, Surveillance, Reconnaissance and Remote Sensing; Communications; Navigation and Science and Technology. As of 2020 the array of nearly 900 US owned and operated satellites include: 353 for Intelligence, Surveillance, Reconnaissance and Remote Sensing; 391 for communications; 7 for Navigation and 94 for Science and Technology.

Figure 5-4 Competing in Space, National Air and Space Intelligence Center. Jan 2019

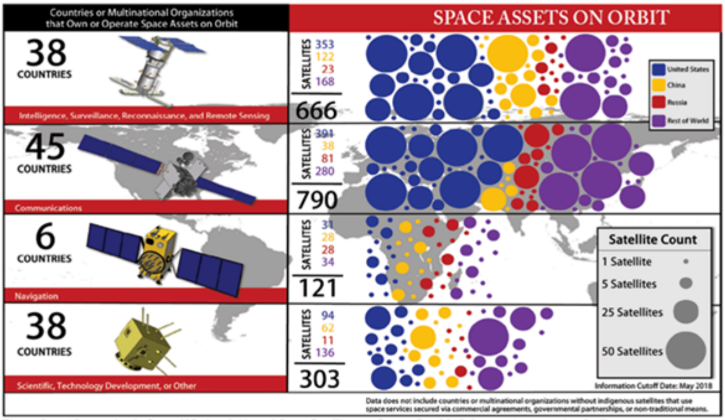


Figure from 'Competing in Space,' National Air and Space Intelligence Center. Jan 2019 (https://www.nasic.af.mil)

Source: (NASIC, 2022)

Taking a Look at UUV/Underwater Threats to CI

It is important to recognize the additional unseen threat which UUV [Unmanned Underwater Vehicles] systems pose to CI whether or not their eventual connectivity to space systems can be verified and tested. Overall capabilities linking UUVs with other UAV, satellite and related space-based platforms is not beyond the scope or pursuit of finding engineering technologies which permit operational linkages. Here are just two examples where subtle threats to port CI and related CI systems is within the realm of realistic risk.

[1]-China's once-secret unmanned underwater vehicle (UUV) may have been tested already in the strategically vital Taiwan Strait, back in 2010. These revelations come from a military-funded research program that was partly declassified recently, according to the South China Morning Post. The UUVs in question have the ability to recognize, follow, and attack enemy submarines without human instruction and conduct harbor surveillance. It was developed by the Harbin Engineering University, Beijing's top submarine research institute. The same article also raises the possibility of a variant of the sub that could be planted on sea floors and activated in the event of a clash or war. The concept seems to be based on using artificial intelligence (AI) technologies to identify and track submerged targets, promising results better than human sonar operators. Sonar operators still need to use their eyes and ears to make judgments on important issues such as identifying friendly vessels, with final decisions taken by the captain, the article asserts. (Kongsberg Gruppen Maritime, 2021)

[2]Threats to our critical infrastructure and vessels are on the increase. Combat divers and now a new generation of underwater drones, are known risk factors. These threats are evolving and in parallel the technology required to detect, track, and identify the threats is also evolving technology uses active sonar elements to insanity an area and then analyses the return signals. Typically deployed in shallow waters and with a requirement to detect threats as far as possible, the design of the instrument must consider carefully the challenges imposed by confined areas, such as complex sound velocity profiles, multipath effects, and shadow zones. The most successful sonars use a circular transducer configuration to ensure even coverage. The sonars track and analyze targets' behavior to discard false alarms. They are widely deployed today to protect harbors, critical infrastructure, and private property. Navies are equipping corvettes and patrol vessels to help protect their ships, for instance while docked overseas, or to provide a deployable detection capability. (Tena, 2019)

Spaced Based Systems as Actual Space Weapons Threats to CI

Space is a recognized domain of future warfare and conflict. Back in 2007, China demonstrated how space can become a combat zone by conducting an anti-satellite mission test. The country shot down its own weather satellite with a kinetic kill vehicle. It was just a weather satellite – their own satellite.

Here was the unmistakable and clear message to the rest of the world: –satellites can be destroyed from Earth, and at least one nation can do it. Space technology and services represent a major component of advanced societies and their inherent infrastructure. At the same time, space technologies and services lay in the vastly unsettled area of legislative and institutional measures, leading to a growing ambiguity among professional community, reunited under the concept of "space traffic management" (STM). STM seeks to address the tension between governmental and private initiatives related to the management and the coordination for space traffic, in short, reconciling the problem of space weather phenomena, space debris and near-Earth objects along with projected future launches. At the same time, STM analysis also considers the development of anti-satellite weapons and other forms of space warfare. (Janosek, 2020) (Botezatu, 2020)

The Joint Chiefs of Staff, according to the NIPP [National Infrastructure Protection Plan] report, has warned that space conflict "will be intense, highlighted by satellites maneuvering to hinder the operation of other satellites, co-orbital jamming, and the use of ground-based lasers to dazzle or destroy imaging sensors." Space attacks will include the use of anti-satellite (ASAT) weapons launched from the ground and orbiting weaponized satellites that could create large debris fields and possibly produce a chain reaction that would destroy other orbiting systems. Electronic jammers and dazzlers will be used to disrupt or impede the functioning of key satellites, such as GPS navigation and communications systems. Electronic jamming, uplink and downlink attacks, spoofing, directed energy, and lasers. (Lambakis, 2018)

Consideration of various space systems and platforms includes reckoning with orbiting systems which have been in their respective paths for some years as well as likely newcomers to the crowded zones and operational areas where emerging space weapons threats must be evaluated comparatively as many system capabilities are covert and classified. Space based platforms and systems which pose a security dilemma for most CI subsystems include a variety of well-known and sometimes vague orbiting mechanisms which merit a closer look. We must consider a variety of space-based systems which symbolize a range of potential threats to CI

Particle Beam systems accelerate particles without an electric charge—particularly neutrons—to speeds nearly at the speed of light directing them against a target. The neutrons knock protons out of the nuclei of other particles they encounter, generating heat on the target object. This technology offers a "heat ray" or "death ray" option unlike lasers, which burn the surface of a target. Instead, particle beams penetrate hover in orbit against satellites or enemy missile attack burning beyond the satellite's surface to disrupt, melt and adversely affect its interior. Such beams are immune to measures that can deflect lasers generating enough heat to burn a target, ignite its fuel supply, render it aerodynamically unstable, or fry an oncoming missile's onboard electronics.

Particle beam weapons include both charged particle beam (CPB) weapons and neutral particle beam (NPB) weapons. Charged particle beams do not propagate in straight lines in outer space because of the Earth's magnetic field. Because of this, their utility in the ASAT role appears limited. However, neutral particles can propagate long, linear distances in outer space. In late 2019 however U.S. Undersecretary of Defense for Research and Engineering Mike Griffin recently told a gathering of defense reporters, "We are deferring work on neutral particle beams, indefinitely. It's just not near-term enough." Griffin emphasized however that the Pentagon was still forging ahead with research into lasers and microwave weapons, for use by ground forces, air forces, and in space. With regard to that development there are no guarantees that despite what the US does, or declines to do, many hostile military forces have rejected the idea of jettisoning this technology or delaying its development. (Tucker, 2019) (Nichols & Carter, 2022)

High Energy Lasers high-energy laser systems use photons, or particles of light, to carry out military missions and civil defense. Directed energy [DE] technology enables detection of threats, tracking during maneuvers, and positive visual identification to defeat a wide range of threats, including unmanned aerial systems, rockets, artillery, and mortars. High energy laser weapon systems work on land, in the air and at sea, providing 360-degree coverage that protects bases, airports, stadiums and other high-value military or civilian targets against missiles, and even drone swarms. Laser systems, including coherent radiation, aligned waveform, and other devices operating at or near the optical wavelengths, operate by delivering energy onto the surface of the target. The gradual or rapid absorption of this energy leads to several forms of thermal damage. Its ruggedized packaging means it can be used as a standalone system or rapidly installed on a variety of military platforms. Full installation and testing on select combat vehicles as well as helicopters has shown its operational value.

Kinetic-Energy Weapons Kinetic-impact weapons include a wide variety of systems which can cause structural damage by impacting a target with one or more high-speed densely packed masses. Small pieces of kinetic debris can inflict substantial damage or destroy a satellite. In January 2007, China successfully tested a direct-ascent, kinetic-kill ASAT vehicle, destroying an inactive Chinese Feng Yun 1C (FY-1C) weather satellite (launched in 1999). The satellite was in a polar orbit at an altitude of 865 km (537 miles) and was attacked when it passed over the Xichang Space Centre in Sichuan Province. The satellite broke into more than 900 pieces, generating more debris. The launch vehicle was probably a mobile, solid-fuel KT-1 missile, a version of the DF-21 medium-range ballistic missile (MRBM), with a range of 1,700 km to 2,500 km, although according to some accounts it was a KT-2, also mobile and solid fuel, based on DF-31 intermediate-range ballistic missile (IRBM)/intercontinental ballistic missile (ICBM) technology, with a range of more than 6,000 km. The launch vehicle and warhead were guided to the target by ground-based radars. (SPACE, 2016) (Nichols & Carter, 2022)

EMP weapons Recently Chinese engineers brought down a large, unmanned aircraft using a new electromagnetic pulse-type weapon in what could be China's first test of its nascent venture into advanced EMP weaponry. New reports say the test reportedly concentrated a powerful beam of electromagnetic energy on the unmanned aircraft during its flight at 1,500 meters, or nearly 5,000 feet in altitude. The aircraft "did not drop immediately but veered abruptly from one side to another for a period. Flight data and analysis of debris recovered from the crash site suggested that sensitive electronic devices, including its satellite navigation system, cryoscope, accelerometer, barometric altimeter, and communication device, had not been damaged. The battery and motors also functioned properly until collision." In all likelihood, the aircraft's "flight control system malfunctioned, issuing an error control command," an engineer involved with the live-fire event explained. Unlike kinetic or explosive weapons, electromagnetic pulse-type weapons rely on 'frying' electrical systems, rendering them useless. Thus, airplanes, drones, trucks—anything that relies on onboard electronics are vulnerable unless specifically hardened against EMP threats. (Chen, 2021)

KA Band Weapons Chinese researchers have developed a microwave machine named Relativistic Klystron Amplifier (RKA) which can jam and destroy satellites in space. A Taiwan News agency recently reported. The RKA can generate a wave burst measuring 5-megawatts in the Ka-band. The Ka-band is a portion of the electromagnetic spectrum which is used for civilian as well as military purposes. It may not be able to shoot targets out of the sky from the ground, but it can be mounted onto satellites and used to attack enemy positions in space by frying their electrical components. Experts at US based think tank Centre for Strategic and International Studies (CSIS) told the Taiwan Times that these developments should force the United States to deploy space-based sensors to counter the Chinese military's new missiles. China denies that the RKA is a directed energy weapons (DEW) system. A DEW system used concentrated electromagnetic energy rather than kinetic energy to destroy enemy equipment and personnel, news agency ANI explained. The Taiwan News report expressed concern that if RKA turns out to be a DEW it can rip apart metallic materials moving at speed. (TAIWAN News, 2022)

Microsatellites and Nanosatellites We already know that microsatellites (microsats) can target US commercial space systems because they offer the opportunity for a broad range of newer countries to enter space using off-the-shelf hardware to build inexpensive satellites and very affordable launch options to place them into orbit. Currently at least 40 countries have demonstrated some ability to design, build, launch, and operate microsats. Used offensively, maneuvering microsats can inspect and interfere with operations of orbiting assets. India, Russia, China, and Japan all have the ability to launch microsats as secondary payloads to low Earth orbit (LEO) and geosynchronous Earth orbit (GEO). "Parasitic" microsats/ nanosatellites could also be launched inside the structure of primary payloads without the knowledge of the launch provider and deployed without detection. There is a significant risk that criminals, terrorists, or nation-state hackers can covertly enter a company's network to disable satellites or steal intellectual property such as satellite designs or software. For decades, government agencies or multinational corporations controlled the vast majority of satellites, and many of those satellites were as large as school buses. Data was received and commands were sent through private networks backed by sophisticated security apparatuses. Now, small, and obscure startup companies can hook up simple microsatellites (weighing 10 to 100 kilograms) to the internet for affordability and the convenience of customers. Today some imagery, weather data and communications bandwidth are delivered this way. "Microsatellites are completely driven by software and completely networked. That's where the vulnerability comes in," For example, as some experts have warned a private firm's vulnerabilities are embedded on its internet reliance. They warned that an employee on an overseas trip could unwittingly create a conduit to the company's satellite constellation and blueprints by firing up a laptop on public Wi-Fi. So, employees are no longer allowed to bring their work laptops on many such trips. Instead, they travel with blank laptops containing no information about the company or its satellite.

Likewise demand for microsatellites and nanosatellites is increasing significantly in the recent years. According to nanosats.eu, as of January 2021, more than 2,900 nanosatellites were launched in the earth's orbit. Companies across the globe are launching constellations of nanosatellites or microsatellites in the earth's orbit for earth observation and telecommunication applications such as high-speed space-based internet services. For instance, in January 2020, Sateliot, a Spain-based nanosatellite and telecommunications operator, signed a Memorandum of Understanding (MoU) with the European Space Agency (ESA) to analyze, develop, and implement innovative technologies, products, and services with space capability using 5G. The company is planning to invest around 100 million Euros to launch constellation of 20 nanosatellites for hybrid terrestrial space networks, 5G network architecture, spectrum management, and spectrum exchange. constellation. Microsatellites and nanosatellites are more cost-effective than traditional satellites and usually developed for communication, commercial, and space research purposes. The demand for these satellites has increased significantly since 2015 owing to their lightweight attribute, shorter development cycle, high capability of performing complex computational tasks, and lower cost for development and launch. Major and upcoming companies, such as Planet Labs, GomSpace, Sierra Nevada Corporation, among others, are launching constellations of micro and nanosatellites to offer near real-time remote sensing data for government and commercial clients. (Werner, 2019)

Directed-Energy Weapons Include laser, RF, and particle-beam weapons often seen collectively as "standoff" weapons because they are primarily either ground- or air-based systems many miles from their target. Most of these concepts are technically sophisticated and attack the target from longer ranges than most kinetic interceptors. In addition, these technologies are capable of engaging multiple targets, whereas interceptors tend to be single-shot systems. Additionally, if the geometric conditions are right, directed-energy weapons can acquire and attack their targets in seconds, whereas kinetic-interceptor engagement times tend to be much longer. Finally, standoff directed-energy weapons provide the enemy with a degree of deniability. This is because the attack is relatively quick—probably no intelligence indicators associated with it—and because the degradation of the target spacecraft may not be immediately apparent, making it difficult to figure out when and where the attack actually occurred. (Nichols & Carter, 2022)

Radio Frequency Weapons. RF weapons concepts include ground- and space-based RF emitters that fire an intense burst of radio energy at a satellite, disabling electronic components. RF weapons are usually divided into two categories: high-power microwave (HPM) weapons and ultrawideband (UWB), or video pulse, weapons.16 UWB weapons generate RF radiation covering a wide frequency spectrum—nominally from about 100 MHz to more than 1 GHz—with limited directivity. Because of the UWB weapon's low-energy spectral density and directivity, permanent damage to electronic components would be very difficult to achieve, except at very short ranges. The UWB enters through the satellite's antenna at its receive frequency, as well as through openings in the system's shielding. If enough power is applied, the received radiation may cause major damage to the satellite's internal communications hardware. However, in many cases, UWB weapons will simply cause system upset, which may persist only while the target is being irradiated or may require operator intervention to return the satellite to its normal state.

Most frequently an RF weapon uses radio waves at power levels high enough to cause electrical disruption. Microwaves (high-frequency radio waves) are usually preferred, so this type of device is sometimes called a High-Powered Microwave, or HPM weapon. RF weapons also overlap generally with Electromagnetic Pulse, or EMP weapons, which emit a powerful burst of radio waves in all directions. Unlike jammers, which just interfere with the signal received by radios or radar, radio frequency weapons do actual damage. They do this by two methods: 'front door coupling', where radio waves are picked by the antennas and aerials normally used for receiving, and in 'back door coupling', where wires inside the electronics act as receivers resulting in an extremely powerful pulse is to put far more current through a component than it can handle. (Nichols & Carter, 2022) (Hambling, 2019)

Orbital interceptors. These weapons are typically ground- or air-launched into intercept trajectories or orbits that are nearly the same as the intended target satellite. Radar or optical systems on board the satellite guide it to close proximity of the target satellite The variety available include : [1] Low-Altitude, Direct-Ascent Interceptors launched on a booster from the ground or from an aircraft into a suborbital trajectory that is designed to intersect that of an LEO satellite. Because these interceptor systems are on a direct suborbital trajectory, the on-orbit lifespan of these systems is measured in minutes, making them the simplest type of interceptor weapons to design, build, and test; [2] high-altitude, short-duration weapon is an interceptor that is launched from the ground into a temporary parking orbit from which it maneuvers to attack a high-altitude satellite. Because these interceptor systems enter a temporary parking orbit, the on-orbit lifespan of these systems is measured in hours, which makes them slightly more complex than direct-ascent; and [3] Long-Duration Orbital Interceptors are launched into a storage orbit for an extended period of time, possibly months to years, before it maneuvers to engage and attack the target satellite. The weapon may be stand-alone or covertly placed on or in a "mothership" satellite. Orbital choices include farsat, nearsat, space mine, fragmentation or pellet ring, and space-to-space missile. Farsats are parked in a storage orbit away from their targets and maneuver to engage them on command. Nearsats are deployed and stay near their targets to inspect and attack on command. Space mines are parked in orbits that intersect the target's orbit and are detonated during a periodic close encounter. Fragmentation or pellet rings are vast quantities of small, non-maneuvering objects that are dispersed from one or more satellites in such a way that an artificial Earth-orbiting ring is created. Satellites flying through the ring are damaged or destroyed. Space-to-space missiles are rocket-propelled interceptors launched from an orbiting carrier platform into an orbit that intercepts the intended target. Presently, there is no existing treaties or other specific international law that bans states from deploying conventional weapons in space, including the use of interceptor missiles. (Harper, 2017)

ASATs [Anti Satellite Weapons] Diverse nations are aware of and intend to deploy sophisticated ASAT systems in anticipation of the space frontier as explicit future battlefield. Many nations plan to use microsatellite technology to develop and deploy long-duration orbital ASAT interceptors. Beijing's decision to develop and deploy the ASAT system has both long-term and short-term strategic objectives. The long-term objectives are to establish a strategic balance among the larger nations, and to break up the monopoly on utilization of space that large space systems of the superpowers are holding; thus, weakening their capabilities in information warfare. In the short-term China would strengthen its capabilities in controlling the usage of space globally and change drastically the Chinese-American military balance so that the U.S. would not intervene easily in the event of a conflict in the Taiwan Strait and at the Chinese perimeter. One can expect a continual growth and development of ever increasingly sophisticated ASAT systems. On Nov. 15, 2021, Russia tested and demonstrated an anti-satellite weapon (ASAT) system by destroying one of its inactive satellites at an altitude of about 300 miles above the earth's surface. At this altitude, the satellite's debris will orbit the Earth for a long time. The United States has identified more than 1,500 pieces. Russia may have calculated that in the context of rising great-power rivalry, especially between the United States and China, the growing trend of space weaponization is the future of warfare. At the same time, this trend of weaponization opens the door to stringent space regulations that will limit the development and use of these capabilities. Displaying technological capability before new international regulations are created can be valuable for both national security and political reasons. By destroying its satellite in space, Russia achieved two objectives. It enhanced its defense and deterrence capabilities, and also projected its power before testing, demonstrating, and using ASAT capabilities could be prohibited or significantly restricted by international mechanisms. Additionally, Russia has ensured that it will be a significant party in any major international regulatory process by publicly possessing such a capability. (Paikowsky, 2021)

The overall threat these various space-based weapons systems and platforms pose to the energy grid, reliable and potable water, farm to market food supplies, public health, transportation, emergency services and the industrial/ commercial base of a nation's daily operations cannot be underestimated. It will require serious and sustained research efforts after 2022 to devise defensive, protective, and deterrent countermeasures and security practices to safeguard what major CI systems are deemed essential to normal and routine daily life in those advanced nations which demand their reliable and uninterrupted operation.

Counter Space Operations, Countermeasures and Protection of Space Systems

Because commercial and military satellites, and related space systems, are equally crucial for national defense, reliable industrial and commercial operations, as well as being part of a nation's critical infrastructure their secure and stable operations must be protected against a variety of threats. Threatening or attacking a nation's space capabilities would have domestic, economic, and political consequences and could provoke international disputes about the origin and intent of an attack and likely bring nations to the brink of open warfare. Such ambiguity and uncertainty among nations experiencing degraded satellite performance and security would trigger a crisis of national safety and survival. Risks of misinterpretation arising from lengthy lapses in secure satellite operations could accelerate national security crises rapidly and permit victimized nations to consider the advent of a surprise attack if absolute confidence in control of friendly platforms was deemed ambiguous, unreliable, or unconfirmed.

There are a number of possible crises or conflicts in which the potential vulnerability of national security space systems would be especially worrisome. During these situations, national leadership and its senior military commanders and civilian advisors would be dependent on information from satellite systems to help manage the crisis, conduct military operations, or bring about a resolution to the conflict. A real time damage assessment which depicted the status of friendly platforms and satellites would be essential along with a discerning capability to determine which systems were inoperable or compromised. If the performance of any of these. systems were reduced, the geostrategic influence and leverage of the jeopardized nations could decline rapidly. In addition, the geostrategic position of an opportunistic and determined adversary could be vastly improved, and the risks of strategic blindness or dissolving confidence in friendly space systems would be enormous tilting in favor of the attacker or party exerting operational influence over home nation satellites and systems.

Strategic miscalculation and error would be part of the ongoing crisis climate until or unless nations could restore positive control over their own orbiting space systems. The sheer opacity and technical uncertainty of verified satellite systems control in such a crisis could create conditions which would diverge among some leaders who would require further confirmation of trouble and await an update versus those presuming the worst case and launching their own pre-emptive attack on suspected enemies based on a feeling of diminished security.

Countermeasures such as hardening, mobile ground control stations, autonomous operations better threat analysis, targeting hostile space systems, creating orbital redundant nodes, randomized platform maneuverability, deploying decoys which simulate the radar and optical signatures of the satellite are all effective to some degree. In the age of quantum and deceptive cyber controls no guarantee of foolproof self-defense systems exist. Shrewd enemies with technical skills can covertly capture or control satellites unless measures are devised to nullify or neutralize satellite operations based on periodic security code transmission updates. Nevertheless, demands for upgraded defensive measures, including methods for neutralizing platforms at will, or detecting immediate operational threats are more engineering issues than reality. Here the priority and national security burden is placed equally on military and commercial satellite owners and operators.

It is important to reckon with some of the things that could go wrong and understand the security implications attached to each. For example, the potential impact of deception, disruption, denial, degradation, or destruction of specific space systems by foreign offensive counterspace operations designed to erode, weaken, or nullify friendly platforms include:

- Impairment or elimination of reconnaissance satellites that would reduce situational awareness and could lead to military surprise, underestimation of enemy strength and capabilities, less effective planning, and less accurate targeting and battle damage assessments.
- Impairment or elimination of missile launch detection satellites that would degrade the US's ability to perform missile launch warning, GPS targeting, missile defense, and would increase the psychological impact of the adversary's ballistic missiles.
- Impairment or elimination of satellite communications systems that would disrupt troop command and control problems at all force levels.
- Impairment or elimination of navigation satellites that would make troop movements more difficult, aircraft and ship piloting problematic, and could render many precision-guided weapon systems ineffective or useless.

- Impairment or elimination of Earth resource and weather satellites that would make it more difficult to plan effective military operations.

IT Vulnerability in Space Systems and the Importance Of Penetration Testing for CI

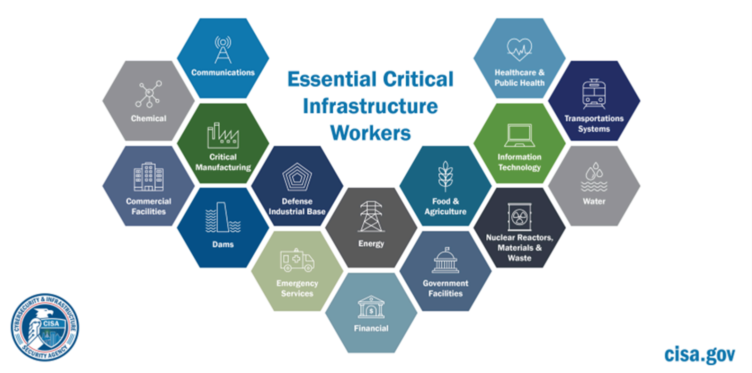
Penetration testing plays a key role in preemptive cybersecurity. Leadership at water districts, power plants and other critical infrastructure can no longer think "it will happen to others, but not us." They're seeing the impacts of successful attacks in the news and a correlated rise in their cyber insurance premiums. Penetration testing will continue its growth because the people in charge are humbler about their current safeguards and the scope of attacks. They've accepted that if they do a good job at running a plant or other facility, then someone out there is interested in compromising their hard work, whether it's for ransom, intelligence gathering or simply promoting chaos. Penetration testing is a vital part of a critical infrastructure assessment that allows all parties to assess risks and implement cybersecurity mitigations and standards. Looking for a broad range of problems, such as software vulnerabilities, network issues and even things like phishing schemes and other human-based attacks are part of it. Penetration testing is not a new practice, but it's heightened now due to the increase in nation-state attacks and people seeing successful attacks like Colonial Pipeline.

Today critical infrastructure managers are searching for someone they can trust to conduct penetration testing. It's an important part of mitigation strategies to expose what they might have missed (for potentially years) and need to address before it's too late. Overall penetration testing has become a necessity. It's a marker of the cyber hygiene of an organization, under the overall vulnerability management umbrella. While penetration testing brings forth anxiety, it also prompts change. When an experienced firm conducts the testing, they'll not only simulate attacks but also train the security team on best practices to react and survive an attack from a threat. Just two examples illustrate the value of this approach—[1] validating existing security controls to ensure they work as designed; and [2] reducing the risk of zero-day threats where attackers routinely probing IT systems find gaps and vulnerabilities before the owner can close or fix them allowing zero days to repair what's important. (Morris, 2022)

Humans and Their Essential Role in CI Systems and Space Systems

If after all the concerns about space systems, IT, cyber security, and daily IC operations rooted in technology weren't enough it is always the overlooked and discounted resource which skilled and trained people behind these various systems are which make them work as intended. The damaging lapse in human performance and productivity arising from nearly three years reeling from the global COVID crisis with staffing shortfalls and periodic skills gaps drives home the point. The workforce which underwrites, supports, and sustains CI and space systems can be easily forgotten unless attention is drawn to their vital role in making the connections between CI and space systems obvious and apparent. This DHS chart underscores the basic message. One source claims more than 104 million U.S. workers, or 71 % of the total U.S. workforce, are employed in the "Essential Critical Infrastructure Workforce". (NCSL, 2020)

Figure 5-5 Essential Critical Infrastructure Workers



Source: (NCSL, 2020)

By contrast about 170,000 workers can be identified as part of the US space systems workforce according to the US Department of Labor in 2017. (BLS, 2017) By comparison a more recent data point which includes all workers in the commercial and government space sector combined reckons the total closer to 2 million workers. This aggregate number of US based space workers when combined with CI workforce data suggests that nearly 106 million workers can be found in both camps. (Aerospace Industries Association, 2020)

Consider the Extra Achilles Heel: Devising Resilience Standards for Space and CI

Here, the engineered and periodically tested measures of resilience applicable for each distinct CI system must be weighed against space system resilience criteria which are not equivalent or similarly ranked. Most often because so much of CI and about 50% of space systems are in private commercial hands, we can find no uniform resilience criteria except to consider how these complex systems tolerate or resist natural disasters, terrorism, cyber hacking, sabotage or natural stress and age-related decline. However, it begs the question of when, how and under what rigorous standards verifiable criteria to gauge resilience in each CI and space system could be derived or developed. It also raises the perplexing dilemma of what organization or objectively skilled enterprise has the requisite talent and expertise to do so.

Inside DHS (CISA) conducts specialized but voluntary security and resilience assessments on the Nation's CI and its partners—federal, state, tribal, territorial governments, and private industry—in better understanding and managing CI risks. The assessments examine infrastructure vulnerabilities, interdependencies, capability gaps, and the consequences of their disruption. Vulnerability assessments, combined with infrastructure planning resources developed through the DHS sponsored Infrastructure Development and Recovery program. This approach forms an integrated planning and assessment capability featuring an integrated suite of capabilities, methods, and tools support the efficient and effective use of resources to enhance critical infrastructure resilience to all hazards. These voluntary, nonregulatory assessments are a foundational element of the National Infrastructure Protection Plan's risk-based implementation of protective programs designed to prevent, deter, and mitigate the risk of a terrorist attack while enabling timely, efficient response and restoration in an all-hazards, post-event situation.

Because most U.S. critical infrastructure is privately owned, the effectiveness of CISA assessments depends upon the voluntary collaboration of private sector owners and operators. CISA's Protective Security Advisors (PSAs) work locally to foster this collaboration and facilitate technical assistance to support enhancement of the security and resilience of the Nation's critical infrastructure. Assessments are offered through the PSAs at the request of critical infrastructure owners and operators and other state, local, tribal, and territorial officials.

However, the voluntary nature of uniform resilience testing and verification does raise questions about best ways to validate, confirm and test the resilience claims by CI owners and operators. (Hardcastle, 2022)

Fifty-six vulnerabilities – some deemed critical – have been found in industrial operational technology (OT) systems from ten global manufacturers including Honeywell, Ericsson, Motorola, and Siemens, putting more than 30,000 devices worldwide at risk, according to private security researchers. Some of these vulnerabilities received resilience severity scores as high as 9.8 out of 10. That is particularly bad, considering these devices are used in critical infrastructure across the oil and gas, chemical, nuclear, power generation and distribution, manufacturing, water treatment and distribution, mining and building and automation industries. The most serious security flaws include remote code execution (RCE) and firmware vulnerabilities. If exploited, these holes could potentially allow miscreants to shut down electrical and water systems, disrupt the food supply, change the ratio of ingredients to result in toxic mixtures, and do all manner of cyber based havoc including – denial-of-service condition, change control logic, or disable communication links and found frequent flaws in such as programmable logic controllers (PLCs) and remote terminal units (RTUs) – control physical processes, while level 2 devices include supervisory control and data acquisition (SCADA) and human-machine interface systems. (Hardcastle, 2022)

Outlining Threat Dynamics and Vulnerabilities for CI from Cyber and Space

It appears that cyber probes hunting for key hubs or nodes, or classes of items could they impact to deliver a shutdown many CI systems or render these systems hostage Our adversaries have been conducting infrastructure reconnaissance using cyber for many years, they likely already understand our infrastructure choke points. What is missing is a standard inventory of CI weaknesses and vulnerabilities shielded from public view and shared in classified or proprietary confidence between DHS/CISA and the managers of national CI systems. A far more serious question that has NATO ramifications is whether any CI probes and attacks which undermine or neutralize CI systems within the alliance would be seen as 'acts of war' sufficient to trigger an Article V military response? One key challenge is devising foolproof forensics to identify what party is engaged in the probe or attack with enough solid confidence to hold a hostile regime accountable. It appears that devising a standby strategy to anticipate and respond to such a scenario would be essential as part of US and NATO combined arms security.

A catalogue of verified CI system vulnerabilities is a starting point but with so much of CI in the operational control of the private sector, and with DHS urging voluntary resilience actions, it is hard to ascertain how CI is protected and sustained against threats in a global comparative manner. Another crude way of putting the issue is to consider whether some advanced societies reliant on CI and space systems have explored all the obvious [and less obvious] pathways to undermine, destroy or disrupt CI as a prelude to armed conflict or as a strategic 'checkmate' maneuver to obviate the need for a kinetic attack. In that sense the EU, US, and other advanced nations with CI at risk must tackle the sobering question of preparedness and resilience against the widest possible spectrum of threats and contingencies. If all nations, including Russia, China, Iran, and all others were equally vulnerable in CI terms one could argue the playing field is mostly level. However, what degree of confidence do we have in that perspective?

So, we are left to contemplate the spectrum of immediate and downstream threats against CI considering the ever-present risks arising from a variety of space systems. While the nexus between space systems adding increased jeopardy to CI systems is fundamental, we cannot lose sight of all the other avenues of potential CI mayhem and destruction. More specifically, the array of threat dynamics which entail robust CI protection, and which consider the reciprocal effect of space system influence on CI systems, is large and complex. It certainly includes at least the following threat factors:

- Space based weapons systems
- Catastrophic natural disasters
- Covert cyber hacking and external manipulation [quantum probes]

- Targeted terrorism
- Solar storms
- EMP attacks
- Natural age/stress related system failures
- Insider threats/sabotage
- Interstate war and armed conflict

FBI—NGB Role//Homeland Defense and Estimating CI Protection Priorities

Under existing regulations and normal interagency practices DHS has arranged for the FBI and the National Guard [NGB] to play a major role in restoring damaged or impaired CI systems in conjunction with the private sector enterprises which own and operate them. While not every CI system is rigorously tested and exercised against all possible hazard and threat scenarios the FBI role is integral most often in cases where CI damage or disruption is claimed to be linked to a terrorist act. The overall Homeland Defense posture of Pentagon resources versus defined roles in DHS contingency plans for selected natural disasters which are part of the National Planning Frameworks which depict federal interagency roles in differential disasters and hazard situations. This is also reinforced in the Comprehensive Preparedness Guide 101 which provides guidelines on developing emergency operations plans and promotes a common understanding of the fundamentals of community-based, risk-informed planning and decision making to help planners examine threats or hazards and produce integrated, coordinated, and synchronized plans.

It is fair to ask whether the NGB has developed and tested its operational plans for handling a range of CI system scenarios involving disruption or loss of functionality caused by space system interventions of attacks. In this case a comprehensive exploration of scenarios and readiness plans which are geared to a variety of scenarios for exercise purposes would make sense. In the case of other developed nations with substantial CI assets to protect and safeguard from a presumptive range of space-based threats the same challenge exists to determine if and in what ways the various agencies and organizations charged with protection and restoration of damaged CI are ready to do so. This also reinforces the point that the time and energy required to restore a damaged or impaired CI system from its victimized state to a point of interim versus full restoration presumes that in many cases the difference between interim and full CI restoration will be measured in days or weeks versus minutes or hours. This also assumes that in cases of complex cascading CI failures that resurrecting the one pivotal and keystone CI element which supports many others can be done in a manner that ensures the restoration of other dependent CI systems in an effective and timely manner, From the standpoint of realistic exercise design and conceptual testing this will be a complex and difficult undertaking. This also implies that designated teams involving both government and private sector leaders should be marshaled to assess the current standby capabilities of CI subsystems to withstand space-based damage scenarios and devise strategies for building in greater resilience for these systems.

It begs the question in advanced societies with substantial CI interests and systems to protect and support whether plans and strategies exist to be exercised and thereby affirm the concept.

Reinforcing CI Systems Against Space Based Threats

One clear signal from this brief review of CI systems and their connection to space-based systems is that advanced technologies to harden CI systems to ensure a level of resilience against presumptive space-based threats entails consideration of

- Cyber hardening
- Protective shielding
- Redundant CI systems
- Counter-space deterrent technologies

Conclusions

Once it becomes clear that CI systems are largely vulnerable to space platforms and systems those nations seeking to buttress their CI systems and dependent networks will need to devise strategies and technologies appropriate to the estimated threat. Failure to calibrate and analyze the threat, or do nothing to mitigate its worst effects, seems to leave open the issue of catastrophic CI systems breakdown and loss. How many advanced nations will accept that risk?

References

Aerospace Industries Association. (2020, Mar 11). *Workforce Statistics Aerospace Industries Association.* Retrieved from www.aia-aerospace.org: https://www.aia-aerospace.org/research-center/statistics

Bahr, L. (2021, Oct 20). *space-as-critical-infrastructure-to-enhance-cybersecurity.* Retrieved from https://spacesecurity.wse.jhu.edu: https://spacesecurity.wse.jhu.edu/2021/10/20/space-as-critical-infrastructure-to-enhance-cybersecurity/

BLS. (2017). *Space careers: A universe of options – Bureau of Labor .* Retrieved from www.bls.gov: https://www.bls.gov/careeroutlook/2017/article/careers

Botezatu, A. G. (2020, April 11). *CRITICAL_INFRASTRUCTURE_DEPENDENCY_ON_SPACE_SYSTEMS.* Retrieved from www.researchgate.net: https://www.researchgate.net/publication/304454658_CRITICAL_INFRASTRUCTURE_DEPENDENCY_ON_SPACE_SYSTEMS

Byrne, D. (2014). 2014 Conference on Systems Engineering Research. *procedia-computer-science/vol/28*, https://www.sciencedirect.com/journal/procedia-computer-science/vol/28. Retrieved from https://www.sciencedirect.com/journal/procedia-computer-science/vol/28

Chen, S. (2021, Aug 26). *did-chinese-scientists-just-bring-down-an-unmanned-plane-with-an-electromagnetic-pulse-weapon.* Retrieved from www.thestar.com.my/tech/: https://www.thestar.com.my/tech/tech-news/2021/08/26/did-chinese-scientists-just-bring-down-an-unmanned-plane-with-an-electromagnetic-pulse-weapon

CISA. (2002). *CRITICAL INFRASTRUCTURE INFORMATION ACT OF 2002.* Retrieved from www.cisa.gov: https://www.cisa.gov/publication/cii-act-2002

CISA. (2021, May 13). *cisa-launches-space-systems-critical-infrastructure-working-group.* Retrieved from www.cisa.gov/: https://www.cisa.gov/news/2021/05/13/cisa-launches-space-systems-critical-infrastructure-working-group

CISA. (2022). *Cyber Incident Reporting for Critical Infrastructure Act of 2022.* Retrieved from www.cisa.gov/circia: https://www.cisa.gov/circia

electricaltechnology. (2018, March 18). *ehv-hv-substations-design-installation-types-configuration.* Retrieved from www.electricaltechnology.org: https://www.electricaltechnology.org/2018/03/ehv-hv-substations-design-installation-types-configuration.html

GAO. (2007, Oct 17). *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain.* Retrieved from https://www.gao.gov/products/gao-08-119t: https://www.gao.gov/products/gao-08-119t

GAO-20-453. (2020, March 14). *Critical Infrastructure Protection: Actions Needed to Enhance DHS Oversight of Cybersecurity at High-Risk Chemical Facilities.* Retrieved from https://www.gao.gov/products/gao-20-453: https://www.gao.gov/products/gao-20-453

GAO-22-104279. (2022, Mar 1). *Critical Infrastructure Protection: CISA Should Improve Priority Setting, Stakeholder Involvement, and Threat Information Sharing.* Retrieved from www.gao.gov/: https://www.gao.gov/products/gao-22-104279

GAO-22-105103. (2022). *Critical Infrastructure Protection: Agencies Need to Assess Adoption of Cybersecurity Guidance.* Retrieved from www.gao.gov/: https://www.gao.gov/products/gao-22-105103

Hambling, D. (2019, Aug 27). *frontline-tech-how-are-radio-frequency-weapons-shaping-future-battlefields.* Retrieved from www.forces.net: https://www.forces.net/news/technology/frontline-tech-how-are-radio-frequency-weapons-shaping-future-battlefields

Hardcastle, e. L. (2022, June 21). *cisa-and-friends-raise-alarm-on-critical-flaws-in-industrial-equipment-infrastructure.* Retrieved from www.msn.com:

https://www.msn.com/en-us/news/technology/cisa-and-friends-raise-alarm-on-critical-flaws-in-industrial-equipment-infrastructure/ar-AAYGbOn

Harper, J. (2017, July). *Pentagon Examining Options for Space-Based Missile Interceptors.* Retrieved from www.jstor.org/: https://www.jstor.org/stable/pdf/27021837.pdf

Harrison, J. M. (2021). *space-threat-assessment-2021.* Retrieved from www.csis.org: https://www.csis.org/analysis/space-threat-assessment-2021

INSA. (2021, Nov 2). *designating-space-systems-as-new-u-s-critical-infrastructure-sector.* Retrieved from www.insaonline.org: https://www.insaonline.org/designating-space-systems-as-new-u-s-critical-infrastructure-sector/

Janosek, D. M. (2020, May 8). *part-1-critical-infrastructure-space-security-and-cybersecurity-intersect.* Retrieved from www.captechu.edu/: https://www.captechu.edu/blog/part-1-critical-infrastructure-space-security-and-cybersecurity-intersect

Kongsberg Gruppen Maritime. (2021, March 2). UUV -unmanned-persistent-surveillance-longendurance. *www.militaryaerospace.com*, pp. https://www.militaryaerospace.com/unmanned/article/14198451/unmanned-persistent-surveillance-longendurance.

Lambakis, S. (2018). *Foreign space capabilities: Implications for U.S. national security.* Retrieved from cogentoa.tandfonline.com: https://cogentoa.tandfonline.com/doi/abs/10.1080/01495933.2018.1459144?journalCode=ucst20

Langner, R. (2013, Nov). *to-kill-a-centrifuge.* Retrieved from www.langner.com: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

MaGill, J. (2021, July 25). *us-water-supply-system-being-targeted-by-cybercriminals.* Retrieved from www.forbes.com: https://www.forbes.com/sites/jimmagill/2021/07/25/us-water-supply-system-being-targeted-by-cybercriminals/?sh=77421de428e7

Magnuson, S. (2022, May 10). *acknowledging-space-systems-as-critical-infrastructure.* Retrieved from www.nationaldefensemagazine.org: https://www.nationaldefensemagazine.org/articles/2022/5/10/acknowledging-space-systems-as-critical-infrastructure

Morgan, C. (2020, April 2). satellites-role-in-monitoring-critical-infrastructure. *x2n.com/*, pp. https://x2n.com/blog/satellites-role-in-monitoring-critical-infrastructure/.

Morris, M. (2022, Jul 21). *the-rising-importance-of-penetration-testing-in-critical-infrastructure-environments.* Retrieved from www.forbes.com: https://www.forbes.com/sites/forbestechcouncil/2022/07/21/the-rising-importance-of-penetration-testing-in-critical-infrastructure-environments/?sh=31aa7fd85220

NASIC. (2022). *About-Us/Fact-Sheets/Article/1738710/competing-in-space/.* Retrieved from www.nasic.af.mil/:

https://www.nasic.af.mil/About-Us/Fact-Sheets/Article/1738710/competing-in-space/

NCSL. (2020, Mar 29). *covid-19-essential-workers-in-the-states.* Retrieved from www.ncsl.org: https://www.ncsl.org/research/labor-and-employment/covid-19-essential-workers-in-the-states.aspx

Nichols, & Carter, H. J. (2022). *Drone Delivery of CBNRECy – DEW Weapons: Emerging Threats of Mini-Weapons of Mass Destruction and Disruption (WMDD).* Manhattan, KS: New Prarie Press #46.

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

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, #38.

Paikowsky, D. (2021, Dec 28). *why-russia-tested-its-anti-satellite-weapon-349678.* Retrieved from publisher.tbsnews.net: https://publisher.tbsnews.net/features/panorama/why-russia-tested-its-anti-satellite-weapon-349678

Sharon, R. (2022, Oct 10). *GAO -105102 GAO assesses progress in adopting cybersecurity framework.* Retrieved from www.ronsharon.com: https://www.ronsharon.com/2022/02/10/gao-assesses-progress-in-adopting-cybersecurity-framework/

SPACE. (2016, Dec 21). *The Most Dangerous Space Weapons Ever.* Retrieved from www.space.com: https://www.space.com/19-top-10-space-weapons.html

TAIWAN News. (2022, Mar 19). *china-develops-laser-weapon-that-can-shoot-down-satellites.* Retrieved from taiwannew.net: https://taiwannew.net/china-develops-laser-weapon-that-can-shoot-down-satellites

Tena, I. (2019). *Standing up to new underwater threats – counter UUV intruder.* Retrieved from cdn.asp.events: https://cdn.asp.events/CLIENT_Clarion__96F66098_5056_B733_492B7F3A0E159DC7/sites/UDT-2020/media/libraries/draft-abstracts–slides/33-Ioseba-Tena.pdf

Tucker, P. (2019, Sept 5). *pentagon-shelves-neutral-particle-beam-research/159660/.* Retrieved from www.govexec.com: https://www.govexec.com/technology/2019/09/pentagon-shelves-neutral-particle-beam-research/159660/

Wechsler, G. B. (2020). *Cyber Threats to Space Systems Current Risks and the Role of NATO Gil Baram and Omree Wechsler —NATO 2020.* Retrieved from www.researchgate.net: https://www.researchgate.net/publication/342666394_Cyber_Threats_to_Space_Systems_-_Current_Risks_and_the_Role_of_NATO

Weigel, A. (n.d.). *Space System Architecture Lecture 1: Space Systems and Definitions Framing Document.* Retrieved from s3vi.ndc.nasa.gov/: https://s3vi.ndc.nasa.gov/ssri-kb/static/resources/01010wk1_framing.pdf

Werner, D. (2019, Sept). *small-satellites-big-weakness.* Retrieved from aerospaceamerica.aiaa.org: https://aerospaceamerica.aiaa.org/features/small-satellites-big-weakness/

Willuhn, M. (2022, March 1). *Satellite_cyber_attack_paralyzes_11GW_of_German_wind_turbine.* Retrieved from article.wn.com/: https://article.wn.com/view/2022/03/01/Satellite_cyber_attack_paralyzes_11GW_of_German_wind_turbine/

6.

TRASH COLLECTION AND TRACKING IN SPACE (HOOD & LONSTEIN)

Student Learning Objectives

This chapter examines the problem of trash in space, including its history, exploring how space junk is located and tracked. Potential mitigation strategies are presented and discussed. Though rarely discussed, the safety considerations of those traveling in space and those on Earth are enormous, not to mention the environmental impact trash in space has both outside and within the Earth's atmosphere. Through understanding historical considerations of waste management and the challenges presented on Earth, we hope to provide students with a foundational understanding of the issues they will confront when applying them to extraterrestrial environments.

The History of Trash

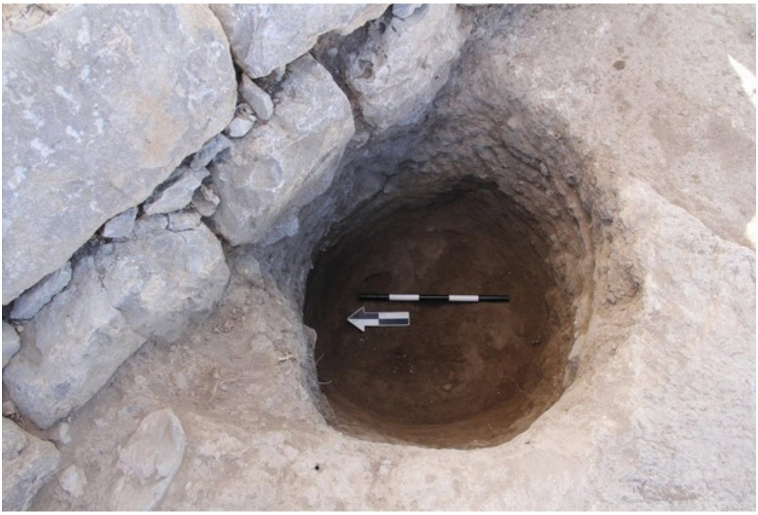
Famed MIT inventor, futurist, and engineer Carlo Ratti once said, "Some trash is recycled, some are thrown away, and some ends up where it should not end up." (Ratti, 2022)

In the 1960s and 70s, space travel and exploration were what many of our dreams were made of. Beginning with Sputnik, then the moon, mars, and beyond. While many of us dreamed of what could and may be possible, other visionaries foresaw that no matter where humans travel, they inevitably will need to address the issue of hygiene and waste management. According to many scholars, the ancient Greeks and Romans began to address the issue of trash as early as 3000 BC, when the first known landfill was created on the island of Crete, followed by the Chinese, who began to compost and recycle around 2000 BC. (Agnoletti & Serneri, 2016)

Most early forms of waste management involved the collection of trash and removing it to waste pits located outside cities. This initial waste management method helped address space and transportation concerns in densely populated cities. Plagues during the fourteenth through eighteenth centuries devastated large portions of the world's population, and waste management's objectives were refocused upon health. (Nathanson, 2020)

As the industrial revolution hit its stride in the 19th and 20th centuries, waste production increased exponentially, requiring more sanitation methods and technologies. Incineration, community collection, and sanitary forms of landfill disposal played a vital role in supporting the faster, bigger, more affluent new world. (Hoornweg & Gianelli, 2007)

Figure 6-1: Ancient Greece Trash Pit (Eastern Boeotia Archaeological Project)



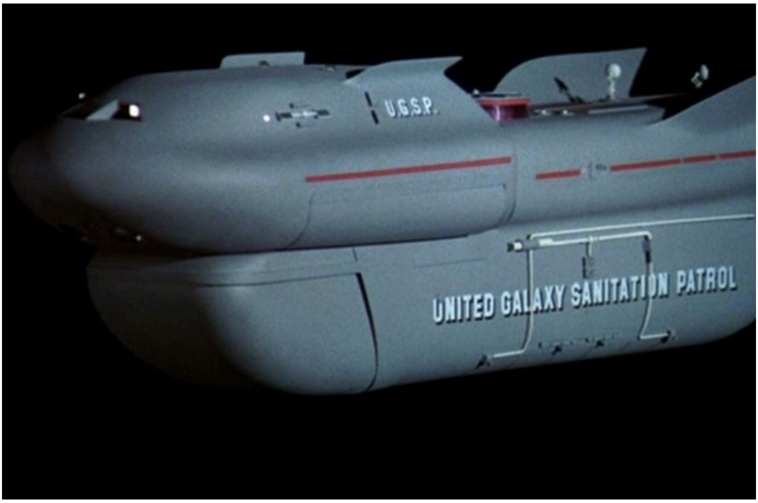
Source: (Hall, 2015)

While simple in its operation, the trash pit in Figure 6-1 was largely effective due to the force of gravity. Most trash placed in the pit was of sufficient weight that it would be difficult for the wind or other elements to overcome the gravitational force holding within the pit. Additionally, when a cover of wood or stone capped the pit, gravity again assisted in keeping the trash in place. (Harvey, 2021) As we turn to this issue of debris and other refuse outside of the Earth's atmosphere, the benefits provided by gravity are far less significant.

The Challenge of Orbital Debris in Space

Famed poet and playwright Oscar Wilde once wrote, “Life imitates Art far more than Art imitates Life” (Wilde, 2022). Many of us who grew up in the 1970’s recall a relatively obscure television comedy called “Quark.”

Figure 6-2: Quark TV Show Space Sanitation Vehicle (Courtesy Columbia)



Source: (Weiner, 2019)

The short-lived comedy bore the name of the lead character Adam Quark. The idea of quirky writers foresaw an issue many years later, which would require outer space sanitation technology. Fast forward fifty years to 2022, and Buck Henry, the writer who created Quark, has gone from comic to visionary.

How significant is the problem of space debris? Dr. Joseph Minow put it this way in 2015:

> "Micrometeoroids and orbital debris (MMOD) is the number one risk for NASA's human space flight programs. Many orbital debris objects —approximately 20,000—are large enough to be tracked and cataloged by the U.S. Space Surveillance Network and can be avoided by spacecraft maneuvering. But the unseen population of MMOD poses the biggest risk to spacecraft: the orbital debris large enough to cause damage, but too small to track, and the micrometeoroids, which can't be tracked regardless of their size." (Minow, 2016)

Dr. Minow also points to the reality that one of the greatest challenges for space vehicles again relates to the force of gravity. "Getting to space requires speed. A lot of speed. So, for NASA to send an object, like a satellite, into orbit, that object must reach velocities of several kilometers per second. And if it hits anything while in orbit, like debris, the damage can be substantial if not catastrophic." (Minow, 2016)

Factors including speed, congestion, and road hazards (debris) are well-established causative factors in modern society's fatalities on the roads and highways. According to the National Highway Traffic Safety Administration (NHTSA) conducted, in 2020, speed was a factor in 29% of all highway fatalities on U.S. roadways. The toll of human lives lost related to speed in just one year alone was 11,258 in 2020. (National Highway Traffic Safety Administration, 2022). Similarly, road debris plays a significant role in highway accidents and fatalities. According to the American Automobile Association, "Between 2011-2014, road debris was a factor in a total of more than 200,000 police-reported crashes resulting in a total of approximately 39,000 injuries and 500 deaths." (American Automobile Association Foundation for Traffic Safety 2016) Finally, that congestion and accidentality are highly correlated. (Sánchez González, 2021)

While the roads many of us travel daily may seem somewhat challenging, imagine a traffic jam in a zero-gravity environment. On Earth, we usually concern ourselves with oncoming traffic or obstacles in our front, rear, right, and left. In space, other traffic can approach from above and below as well. Further complicating things is velocity. According to NASA:

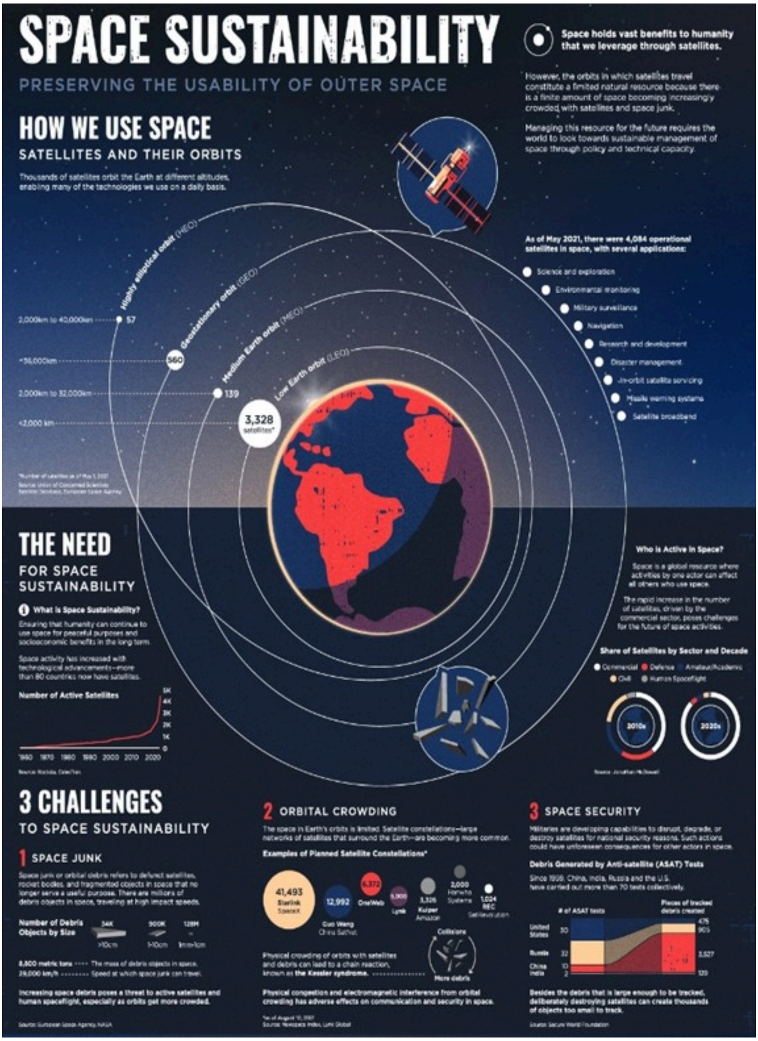
"There are approximately 23,000 pieces of debris larger than a softball orbiting the Earth. They travel at speeds up to 17,500 mph, fast enough for a relatively small piece of orbital debris to damage a satellite or a spacecraft. There are half a million pieces of debris the size of a marble or larger (up to 0.4 inches, or

1 centimeter) or larger, and approximately 100 million pieces of debris-about .04 inches (or one millimeter) larger. There is even smaller micrometer-sized (0.000039 of an inch in diameter) debris.

Even tiny paint flecks can damage a spacecraft when traveling at these velocities. Several space shuttle windows were replaced because of damage caused by material analyzed and shown to be paint flecks. Millimeter-sized orbital debris represents the highest mission-ending risk to most robotic spacecraft operating in low Earth orbit." (NASA, 2021)

According to Secure World, there are three main challenges confronting the safe and sustainable use of outer space, Space Junk. Orbital Crowding and Space Security. Separately, each of these challenges represents an existential threat to both manned and unmanned orbital operations; many believe the current situation is already unsafe and worsening with every launch of new vehicles.

Figure 6-3: Space Sustainability (Courtesy Sustainable World Foundation)



SPACE SUSTAINABILITY

PRESERVING THE USABILITY OF OUTER SPACE

Space holds vast benefits to humanity that we leverage through satellites.

However, the orbits in which satellites travel constitute a limited natural resource because there is a finite amount of space becoming increasingly crowded with satellites and space junk.

Managing this resource for the future requires the world to look towards sustainable management of space through policy and technical capacity.

HOW WE USE SPACE

SATELLITES AND THEIR ORBITS

Thousands of satellites orbit the Earth at different altitudes, enabling many of the technologies we use on a daily basis.

*Number of satellites as of May 1, 2021
Source: Union of Concerned Scientists, [illegible], European Space Agency

As of May 2021, there were 4,084 operational satellites in space, with several applications:

- Science and exploration
- Environmental monitoring
- Military surveillance
- Navigation
- Research and development
- Disaster management
- In-orbit satellite servicing
- Missile warning systems
- Satellite broadband

THE NEED

FOR SPACE SUSTAINABILITY

What is Space Sustainability?

Ensuring that humanity can continue to use space for peaceful purposes and socioeconomic benefits in the long term.

Space activity has increased with technological advancements—more than 80 countries now have satellites.

Number of Active Satellites

Source: Statista, CelesTrak

Who is Active in Space?

Space is a global resource where activities by one actor can affect all others who use space.

The rapid increase in the number of satellites, driven by the commercial sector, poses challenges for the future of space activities.

Share of Satellites by Sector and Decade

● Commercial ● Defense ● Amateur/Academic
● Civil ● Human Spaceflight
2010s
2020s

Source: Jonathan McDowell

3 CHALLENGES

TO SPACE SUSTAINABILITY

1 SPACE JUNK

Space junk or orbital debris refers to defunct satellites, rocket bodies, and fragmented objects in space that no longer serve a useful purpose. There are millions of debris objects in space, traveling at high impact speeds.

Number of Debris Objects by Size

8,800 metric tons ---- The mass of debris objects in space.
29,000 km/h -------- Speed at which space junk can travel.

Increasing space debris poses a threat to active satellites and human spaceflight, especially as orbits get more crowded.

Source: European Space Agency, NASA

2 ORBITAL CROWDING

The space in Earth's orbits is limited. Satellite constellations—large networks of satellites that surround the Earth—are becoming more common.

Examples of Planned Satellite Constellations*

Physical crowding of orbits with satellites and debris can lead to a chain reaction, known as **the Kessler syndrome.**

Physical congestion and electromagnetic interference from orbital crowding has adverse effects on communication and security in space.

*as of August 10, 2021
Source: Newspace Index, Lynk Global

3 SPACE SECURITY

Militaries are developing capabilities to disrupt, degrade, or destroy satellites for national security reasons. Such actions could have unforeseen consequences for other actors in space.

Debris Generated by Anti-satellite (ASAT) Tests

Since 1959, China, India, Russia and the U.S. have carried out more than 70 tests collectively.

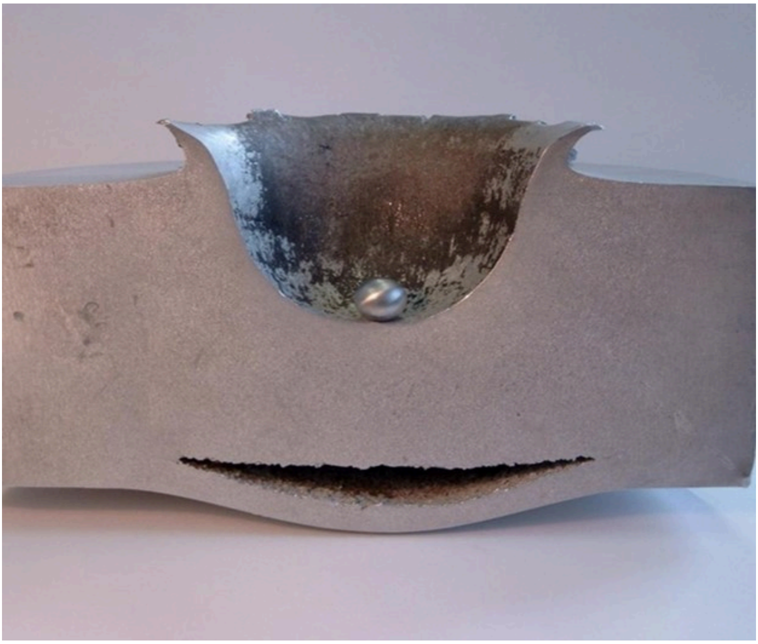
Besides the debris that is large enough to be tracked, deliberately destroying satellites can create thousands of objects too small to track.

Source: Secure World Foundation

Source: (Secure World Foundation, Bhutada, Govind Editor, 2021)

Orbital debris presents a multitude of challenges both on Earth and in space. In her recent book, "War in Space," Linda Dawson explores the use of space debris as a weapon of war. Many, including Dawson, believe we are approaching the Kessler syndrome. The Kessler syndrome is akin to a chain reaction where objects in space collide, creating more debris. The newly created debris will cause more collisions, and a nuclear reaction-like process will eventually lead to a time when "low Earth orbit is so full of debris that passage through it becomes impossible." (Dawson, 2018)

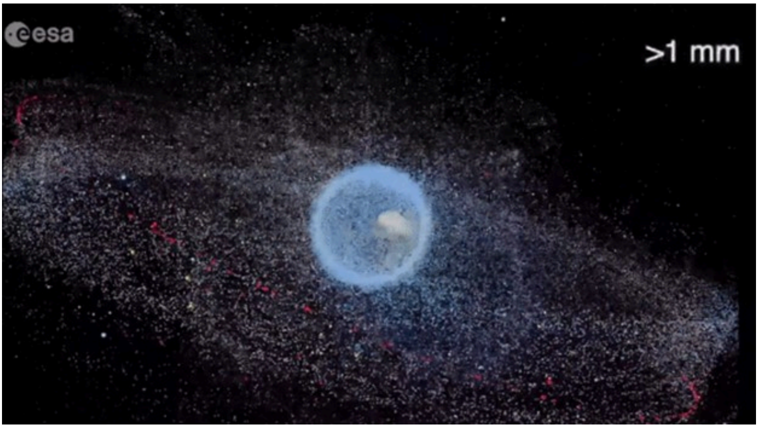
Figure 6-4: Lab Test Result Small Aluminum Ball Hitting Aluminum Block at 7 KM per second (Courtesy Scientific American and ESA)



Source:(David, 2021)

The devastation that can occur from collisions in space between vehicles and man-made and naturally-occurring debris is unfathomable. While we have documented many minor collisions so far, we have not witnessed a collision between two spacecraft, orbit vehicles, or larger debris or meteor. Given the immense force created by such collisions, it is only logical to consider the use of debris as a tool of warfare. While many private companies and governments are beginning to address the removal of space debris, the reality is that a darker side of debris exists, one where it is used as a tool for war, terror espionage, or another hostile purpose. Dawson points out that "There is a double-edged sword to the (debris removal) technology that might solve this issue, as anything that can be used to bring down unusable satellites can also bring down active ones." (Dawson, 2018) p. 60.

Figure 6-5: Visualization of space debris around Earth (Courtesy ESA)



Source: (European Space Agency, 2019)

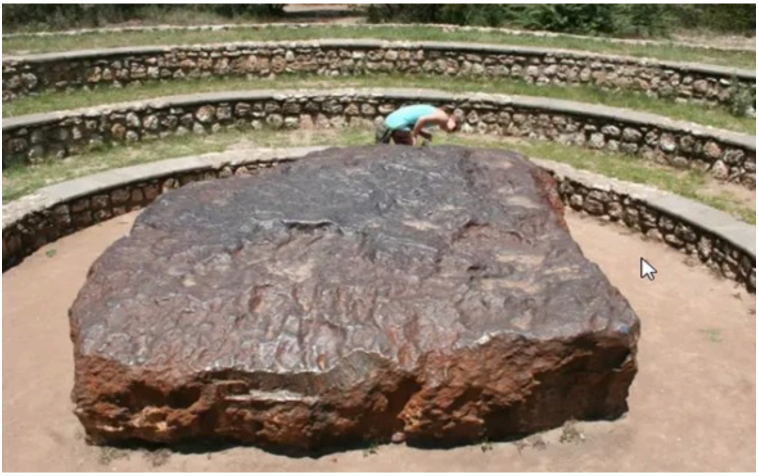
Space debris has ramifications both outside of Earth's atmosphere and at every level within it. As mankind continues to explore, understand, and use space as a resource, inevitably, we will leave our mark upon it. Sadly, part of that mark is trash. For example, in 2021, a Falcon 9 rocket pressure vessel fell onto a farm in central Washington State. Luckily no injuries occurred.

Figure 6-6: Falcon 9 Rocket Pressure Tank (Courtesy Grant County Sheriff via Twitter)

Source:(Grant County Washington Sheriff, 2022)

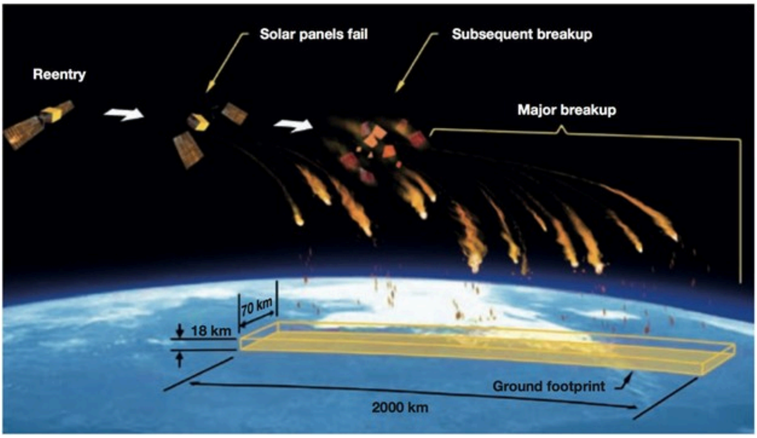
Since the launch of the former Soviet Union's Sputnik in 1957, humans have been adding to the pre-existing bounty of galactic byproducts generally referred to as Asteroids and Meteoroids. According to NASA, an asteroid is a small rocky body that orbits the Sun. When asteroids collide, debris can scatter; these collision byproducts are called meteoroids. Meteoroids can also come from comets but are not composed of rock but dust and ice. When a meteoroid comes near or in contact with Earth's atmosphere, it is called a meteor. Meteors often appear as streaks of light in a dark sky, sometimes called "falling stars." When a meteor or some portion of it makes it through Earth's atmosphere and falls to Earth, it is called a meteorite. (NASA, 2022) The largest known example of a meteorite known as *Hoba* is believed to have landed in what is known today as Namibia, weighs approximately 60 tons, and is believed to have landed some 80,000 years ago.

Figure 6-7: *Hoba* (Courtesy Compl33t / Wikimedia Commons)



Source: (Dodgson, 2017)

Figure 6-8: Space debris consists of discarded launch vehicles or parts of a spacecraft that float hundreds of miles above Earth. Image: Space Safety (World Economic Forum, 2021)



Current International Policy and Laws on Space Trash

The body of legal regulations regarding the use of space (space being defined as the area above the jurisdiction of air law) by public and private entities are referred to as space law. Currently, there are only about five such regulations of space, the most significant of those being the United Nations Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (from now on referred to as the Outer Space Treaty) of 1967. In this article, I would like to specifically describe and analyze the laws and regulations handling the increasingly prevalent issue of space debris in orbit around Earth. The National Aeronautics and Space Administration (NASA) defines space debris as "any man-made object in orbit about the Earth which no longer serves a useful function." [1] However, a major confusion discussed below is that the

Outer Space Treaty does not explicitly define what it refers to as "space objects," nor does it mention whether space debris is space objects. An excessive clustering of space debris is a problem for a few reasons. It may result in a phenomenon known as the Kessler Syndrome, in which a "cascade created when debris hits a space object, creating new debris and setting off a chain reaction of collisions that eventually close off entire orbits." [2] This endangerment of Earth's future ability to explore extraterrestrial planets and life must be avoided at all costs. Furthermore, space debris in orbit around Earth limits the amount of available space for satellites to orbit, which may result in the Tragedy of the Commons: multiple actors will aggressively vie, in an arms race, for their right to space as it is a limited resource. (Shah, 2021)

Recent accidents that continue to clutter the orbital space around Earth: ISS Swerves

MOSCOW, December 3 (Reuters) – The International Space Station (ISS) had to swerve away from a fragment of a U.S. launch vehicle on Friday, the head of Russia's space agency said, the latest in a series of incidents in which space debris have forced astronauts to respond. (Reuters, 2021)

In recent years there has been an uptick in expressed concern from recent emergency procedures carried out by the ISS. The below excerpt describes one such incident from 2021:

Since Russia conducted an anti-satellite missile test last month, calls to monitor and regulate space debris, or space junk, have grown. This generated a debris field in orbit that U.S. officials said would pose a hazard to space activities for years. (Reuters, 2021)

Figure 6-9: The International Space Station photographed from Russian spacecraft after undocking.

Source:(Reuters, 2021)

Dmitry Rogozin, head of Russian space agency Roscosmos, said that the ISS had been forced to move due to space junk from a U.S. launch vehicle sent into orbit in 1994.

Roscosmos said the station's orbit, in an unscheduled maneuver, carried out by mission control, dropped by 310 meters (339 yards) for nearly three minutes to avoid a close encounter. Rogozin added that the maneuver would not affect the planned launch of the Soyuz MS-20 rocket on December 8 from the Baikonur Cosmodrome in Kazakhstan and its docking at the ISS. (Reuters, 2021)

Looming changes that may further destabilize international space operations add more clutter to an already dirty problem: Russia leaves ISS.

MOSCOW — Russia will pull out of the International Space Station after 2024 and focus on building its orbiting outpost, the country's new space chief said Tuesday, amid high tensions between Moscow and the West over the fighting in Ukraine. Yuri Borisov, appointed this month to lead the state space agency, Roscosmos, said during a meeting with President Vladimir Putin that Russia will fulfill its obligations to its partners before it leaves. (Associated Press, 2022)

"The decision to leave the station after 2024 has been made," Borisov said, adding: "I think that by that time, we will start forming a Russian orbiting station." (Associated Press, 2022)

NASA and other international partners hope to keep the space station running until 2030, while the

Russians have been reluctant to make commitments beyond 2024. (Associated Press, 2022) NASA has been working with

U.S. companies to eventually establish private space stations to replace the International Space Station. NASA hopes these commercial space stations will be up and running by the decade's end. (Associated Press, 2022)

Clean This Mess: The Kessler Syndrome and the challenges of cleaning orbital space debris before it's too late.

Finding ways to remove at least some of all that space junk should be a top global priority, says Donald Kessler, a retired NASA senior scientist for orbital debris research. In the late 1970s, he foretold the possibility of a scenario dubbed the Kessler syndrome. As the density of space rubbish increases, a cascading, self-sustaining runaway cycle of debris-generating collisions can arise that might ultimately make low-Earth orbit too hazardous to support most space activities. (David, Leonard, 2021)

A Space Age "tragedy of the commons" is unfolding right under our nose—or right over our head—and no consensus yet exists on how to stop it. For more than a half-century, humans have been hurling objects into low-Earth orbit in ever-growing numbers. And with few meaningful limitations on further launches into that increasingly congested realm, the prevailing attitude has been persistently permissive. In orbit, it seems, there is always room for one more. (David, Leonard, 2021)

"There is now agreement within the community that the debris environment has reached a 'tipping point where debris would continue to increase even if all launches were stopped," Kessler says. "It takes an Iridium-Cosmos-type collision to get everyone's attention. That's what it boils down to…., And we're overdue for something like that to happen." (David, 2021)

Kelso says there is no "one-size-fits-all solution" to the space junk problem. He observes that removing large rocket bodies is a significantly different task than removing the equivalent mass of many smaller objects, which are in a wide range of orbits. Meanwhile, innovations by companies such as SpaceX are dramatically lowering launch costs, opening the floodgates for far more satellites to reach low-Earth orbit, where some will inevitably fail and become drifting, debris-generating hazards (unless ELSA-d-like space tugs remove them). "Many of these operators are starting to understand the difficulty and complexity of continuing to dodge the growing number of debris." (David, 2021)

For now, according to Moriba Jah, an orbital debris expert at the University of Texas at Austin, the business case for space debris removal is not monetizable and is more a "PowerPoint talk" than a real marketplace. (David, 2021)

"I think people are hoping that government comes to some common sense to help create and establish a marketplace for industries to engage in these sorts of activities," Jah says. For that to happen, he believes that spacefaring nations have to agree that near-Earth space is an ecosystem like land, air, and the ocean. "It's not infinite, so we need environmental protection," he says. (David, 2021)

Jah has in mind space sustainability metrics akin to a carbon footprint. "Let's call it a 'space traffic' footprint," he says. "We need a way to quantify when an 'orbital highway' gets saturated with traffic, so it's not usable. Then you can assign a bounty for objects and discuss nonconsensual debris removal. Maybe there is a penalty to the sovereign owner of their dead asset that's taking up the capacity of an orbit. This could create a marketplace where space-object-removal technologies can thrive." (David, 2021)

A classification scheme for objects in space is also needed. Having such a taxonomy, Jah says, would help sort out what types of technologies are required for removing different pedigrees of orbital clutter. As for the big picture, Jah says it is a simple numbers game: the rate of launches exceeds the rate of space objects reentering Earth's atmosphere. "That's not a great kind of energy balance," he adds. (David, 2021)

Alas, Jah says, policymakers are still sluggish in their reactions to the problem. After all, although events such as the 2009 Cosmos-Iridium collision generate massive amounts of debris, they are still quite rare—for now. (David, 2021)

"In my view, that 2009 collision was equivalent to passengers on the Titanic feeling that bump from an iceberg, and then there's a band playing on the deck," Jah says. "In terms of hazardous orbital debris, things are already going a detrimental way because we haven't changed our behavior." (David, 2021)

QUESTIONS:

1. As a space navigation professional, you are tasked with flight planning just as in commercial aviation within the Earth's atmosphere. What resources do you think will be needed to be able to safely navigate your entire journey as it relates to naturally occurring and man-made space debris?

2. Besides both types of space debris and direct kinetic attack, can you foresee any other type of attack vector being used in space related to waste or biological products? (Hint air, water, filtration, food, medication)

3. What could current technologies be used to create a potential low-cost solution to cleaning space debris? What resource considerations and policies would need to be considered and or created to help facilitate the removal of space debris?

References

Agnoletti, M., & Serneri, S. (2016). The Basic Environmental History. In M. Agnoletti, & S. Serneri, *The Basic Environmental History* (pp. 201-204). Florence: Springer.

American Automobile Association Foundation for Traffic Safety. (2016, August). *The Prevalence of Motor Vehicle Crashes Involving Road Debris, United States, 2011-2014.* Retrieved from AAA Foundation for Traffic Safety:

https://aaafoundation.org/prevalence-motor-vehicle-crashes-involving-road-debris-united-states-2011-2014/

Associated Press. (2022, July 26). *Russia says it will quit the International Space Station after 2024*. Retrieved from NPR: https://www.npr.org/2022/07/26/1113683450/space-station-iss-russia-leaving-2024

David, L. (2021, April 14). *Space Junk Removal Is Not Going Smoothly.* Retrieved from Scientific American: https://www.scientificamerican.com/article/space-junk-removal-is-not-going-smoothly/

David, Leonard. (2021, April 14). *Space Junk Removal Is not Going Smoothly*. Retrieved from Scientific American: https://www.scientificamerican.com/article/space-junk-removal-is-not-going-smoothly

Dawson, L. (2018). *War in Space.* New York: Springer.

Dodgson, L. (2017, February 23). *The biggest meteorites in history have plummeted to Earth and survived.* Retrieved from Business Insider: https://www.businessinsider.com/biggest-meteorites-space-junk-crashed-earth-2017-2

European Space Agency. (2019, September 19). *ESA commissions the world's first space debris removal.* Retrieved from European Space Agency: https://www.esa.int/Space_Safety/Clean_Space/ESA_commissions_world_s_first_space_debris_removal

Grant County Washington Sheriff. (2022, July 18). *What goes up must come down: The study looks at the risk of orbital* *debris casualties.* Retrieved from Space.Com: https://www.space.com/space-junk-rocket-debris-reentry-risk

Hall, A. R. (2015). “Sewers, cesspits, and middens: A survey of the evidence for 2000 years of waste disposal in York, UK,”. *Sanitation, Latrines and Intestinal Parasites in Past Populations, ed. P. D.*, 99-119. Retrieved from EBAP Excavations.

Harvey, M. (2021, May 21). *TRASH OR TREASURE? A MEDIEVAL PIT FROM ELEON.* Retrieved from EBAP EXCAVATIONS: https://ebapexcavations.org/2021/05/21/trash-or-treasure-a-medieval-pit-from-eleon/

Hoornweg, D., & Gianelli, N. (2007, October). Managing municipal solid waste in Latin America and the Caribbean:: Integrating the private sector, harnessing incentives. *Gridlines*, pp. 1-5.

Minow, D. J. (2016, July 11). *Space Debris: Understanding the risks to NASA Spacecraft.* Retrieved from NASA.

NASA. (2021, May 26). *Space Debris and Human Spacecraft*. Retrieved from NASA: https://www.nasa.gov/mission_pages/station/news/orbital_debris.html

NASA. (2022, July 28). *Asteroid or Meteor: What’s the Difference?* Retrieved from Space Place: https://spaceplace.nasa.gov/asteroid-or-meteor/en/

Nathanson, J. A. (2020, November 10). *Solid-Waste Management*. Retrieved from Encyclopedia Britannica: https://www.britannica.com/technology/solid-waste-management

National Highway Traffic Safety Administration. (2022, August 10). *Speeding*. Retrieved from NHTSA: https://www.nhtsa.gov/risky-driving/speeding#nhtsa-in-action

Ratti, C. (2022, August 5). *carloratti.com/publications/*. Retrieved from Carlo Ratti Associates: https://carloratti.com/publications/

Reuters. (2021, December 3). *Reuters*. Retrieved from Reuters Online: https://www.reuters.com/lifestyle/science/international-space-station-swerves-dodge-space-junk-2021-12-03/

Sánchez González, S. (2021). *Understanding the Effect of Traffic Congestion on Accidents.* Washington, D.C.: Transport Division, Inter-American Development Bank.

Secure World Foundation, Bhutada, Govind Editor. (2021, October 6). *Space Sustainability: Preserving the Usability of Outer Space.* Retrieved from Visual Capitalist: https://www.visualcapitalist.com/sp/space-sustainability-preserving-the-usability-of-outer-space/

Sedgwick, T. (1826). *Hints to My Countrymen.* New York: J. Seymour.

Shah, S. (2021, August 30). *August 30: The International Legal Regulation of pace Debris*. Retrieved from Cornell Undergraduate Law and Society Review: https://www.culsr.org/articles/the-international-legal-regulation-of-space-debris

Weiner, D. (2019, January 1). *An Ode To 'Quark': Richard*

Benjamin Remembers His Brief but Beloved Sci-Fi Sitcom. Retrieved from It Came From: https://itcamefromblog.com/2019/01/21/an-ode-to-quark-richard-benjamin-remembers-his-brief-but-beloved-sci-fi-sitcom/

Wilde, O. (2022, August 7). *The Decay Of Lying: An Observation*. Retrieved from The Literature Network: http://www.online-literature.com/wilde/1307/

World Economic Forum. (2021, November 24). *Should We Be Worried About Space Debris?* Retrieved from Space: https://www.weforum.org/agenda/2021/11/space-debris-satellite-international-space-station

7.

LEVERAGING SPACE FOR DISASTER RISK REDUCTION AND MANAGEMENT (CARTER)

Student Objectives

- Impact of space disaster risk reduction and management in preventing climate change
- Explore the benefits of space disaster risk reduction and management during a global pandemic.
- To further understand the advances in space can lead to greater quality of life on Earth.

Introduction

Disasters can disrupt or devastate a community, society, or country. Disaster can cause human, economic, and environmental loss. This unpredictable event can drain resources hindering all aspects of recovery. This chapter provides an overview of how satellite data can prepare and respond to global disasters and emergencies. Space disaster reduction and risk management include removing hazards, reducing vulnerabilities, and reducing exposure. Before a disaster occurs, remotely sensed data provide information for systems and models that can predict disasters and provide early warnings (UNOOSA, 2022). This form of management supports the formulation of disaster scenarios to simulate the impacts of crisis events and test emergency procedures (Le Cozannet, G., Kervyn, M., & Russo, S., 2020). The Sendai Framework is the backbone of the United Nations Office Outer Space of Affairs mission for the adoption of using space in risk reduction and management. The framework focuses on adopting measures that address the three dimensions of disaster risk (exposure to hazards, vulnerability and capacity, and hazard's characteristics) to prevent the creation of new risk, reduce existing risk and increase resilience (United Nations, 2015). The concept of space disaster reduction and risk management is not new; however, the world looked to this method to learn, monitor, and mitigate during COVID-19. There are several benefits of space technologies for disaster management and response. The ability to share satellite data, communications, and applications provide real-time monitoring of our planet. Satellite data is critical in the event of disaster response and recovery. In 60 years, the planet went from zero space technology to today; nearly half of all countries have space capabilities.

The Sendai Framework For Disaster Risk Reduction 2015 – 2030

The Sendai Framework for Disaster Risk Reduction 2015–2030 was adopted at the Third United Nations World Conference on Disaster Risk Reduction, held in March 2015 in Sendai, Miyagi, Japan (United Nations, 2015). Currently, the framework is the only international accord for disaster risk management. The Sendai Framework embodies the following:

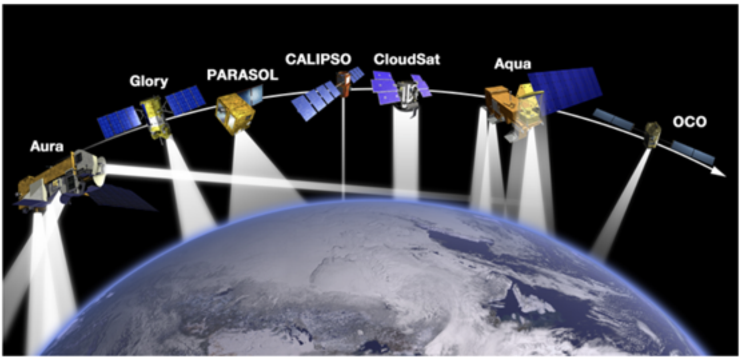
"…the need for improved understanding of disaster risk in all its dimensions of exposure, vulnerability and hazard characteristics; the strengthening of disaster risk governance, including national platforms; accountability for disaster risk management; preparedness to "Build Back Better"; recognition of stakeholders and their roles; mobilization of risk-sensitive investment to avoid the creation of new risk; resilience of health infrastructure, cultural heritage, and workplaces; strengthening of international cooperation and global partnership, and risk-informed donor policies and programs, including financial support and loans from international financial institutions. There is also a clear recognition of the Global Platform for Disaster Risk Reduction and the regional platforms for disaster risk reduction as mechanisms for coherence across agendas, monitoring, and periodic reviews in support of UN Governance bodies' (United Nations, 2015). The Sendai Framework and the Paris Agreement share a common goal of global coherence to climate change adaptation and disaster risk reduction. The agreements have a call to action for implementing policy and governance, using data and information, and monitoring/reporting standards. The Sendai Framework and the Paris Agreement encourage global partnerships to help governments develop solid risk financing strategies to respond to the impacts of climate-related disasters.

Climate Change

We can see evidence of climate change all around us, from the loss of arctic ice to the drying, wildfires increasing, and unprecedented changes in weather patterns globally. Scientists have proven the increase in human activities has caused the warming of the atmosphere resulting in devastating events. Evidence can be found in tree rings, ocean sediments, coral reefs, and layers of sedimentary rocks (NASA, 2022). Carbon dioxide from human activities is increasing about 250 times faster than from natural sources after the last Ice Age (Gaffney & Steffen, 2017). The advancement in satellites has allowed scientists to collect more data than ever before to assist in reversing damage to the planet.

NASA and international partners have the "A-Train" satellite constellation of Earth-observing satellites that follow along the same orbital track. Earth observation satellite-based remote sensing technology monitors land, marine (seas, rivers, lakes), and the atmosphere (EUSPA, 2022). The satellites have mounted payloads to gather imaging data about the Earth's characteristics. The satellite can have an Optical or thermal sensor. These payloads can report on the energy received from the Earth due to the reflection and re-emission of the Sun's energy by the Earth's surface or atmosphere (EUSPA, 2022). They operate between the visible and

Figure 7-1 "A-Train" Satellite Constellation



Source: (NASA, 2022)

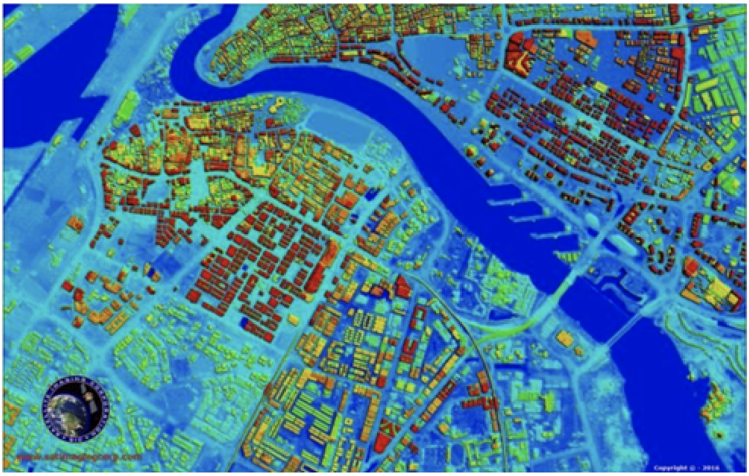
Satellites use Infrared wavelengths of the electromagnetic spectrum (EUSPA, 2022). Also, satellites can use radar sensors to capture radiation emitted from the Earth's surface. Earth observations in space deliver various data to improve space disaster risk management.

Figure 7-2 Burning in Botswana

Source: (NASA, 2022)

Cities are increasingly experiencing the impact of climate change through extreme weather events, bushfires, flooding, storm surges, and sea level rise (Hurlimann, Moosavi, & Browne, 2020). Over half of the world's 8 billion people live in cities, which is expected to increase by over 70% in the coming decades (EUSPA, 2022). Population increases directly impact the rise of temperature, bringing extreme heat events and raising the risk for dense population areas to be impacted by climate change. Being aware of the risk, urban planners use sustainable developers to provide mitigation strategies to reduce the impact of climate change on the population. Sustainable engineers use satellite-based remote sensing technologies and socio-demographic data to create heat threat maps to advise urban planners of areas that can adversely affect the population, energy production, agriculture, and transportation. Urban planners can take steps to protect citizens and infrastructure by changing traffic patterns, increasing green space, and encouraging alternative transportation.

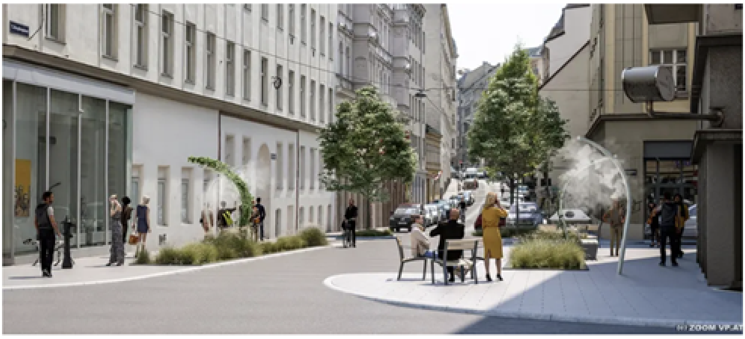
Figure 7-3 Dubai Satellite imagery and LiDAR Digital Terrain Models urban strategic information about urban planning and prevention of flooding conditions in urban areas



Source: (Satellite Imaging Corporation, 2022)

A Prague-based company, ECOTEN, uses data from various satellite programs combined with technology to assist with sustainable urban planning across Europe. EOCTEN is mapping highly vulnerable urban areas to reduce the risk of natural disasters (i.e., extreme heat events). Using this innovative method for risk reduction, Vienna is using the information to transform Zieglergasse in the 7th municipal district into a climate-adapted street. The densely populated area is modified with planted trees, several public water points, and light-colored paving. These climate-friendly changes have lowered the temperature and prevented the district's flooding.

Figure 7-4 Zieglergasse – Vienna's First Climate-Adapted Street

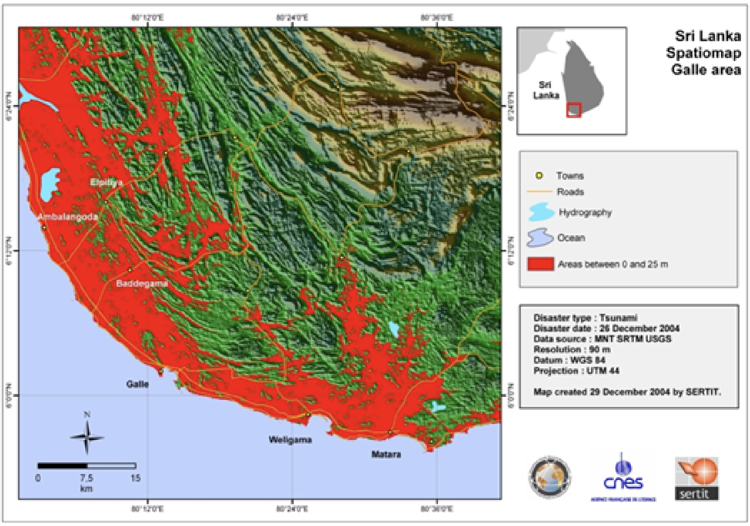


Source: (Okosvaros, 2020)

Damage Mapping After A Disaster

On December 26, 2004, the Indian Ocean tsunami was one of the deadliest disasters in modern history, with nearly 230000 people dead. In the days immediately following, the International Charter on Space and Major Disasters was activated. This initiated the gathering of satellite data over the affected region. The alliance carried out a large amount of rapid mapping in the immediate days to follow, creating over 210 individual maps from more than 19 satellites (European Space Agency, 2018). Crisis mapping continued for several days and the

Figure 7-5 Satellite map of the affected Sri Lankan coast



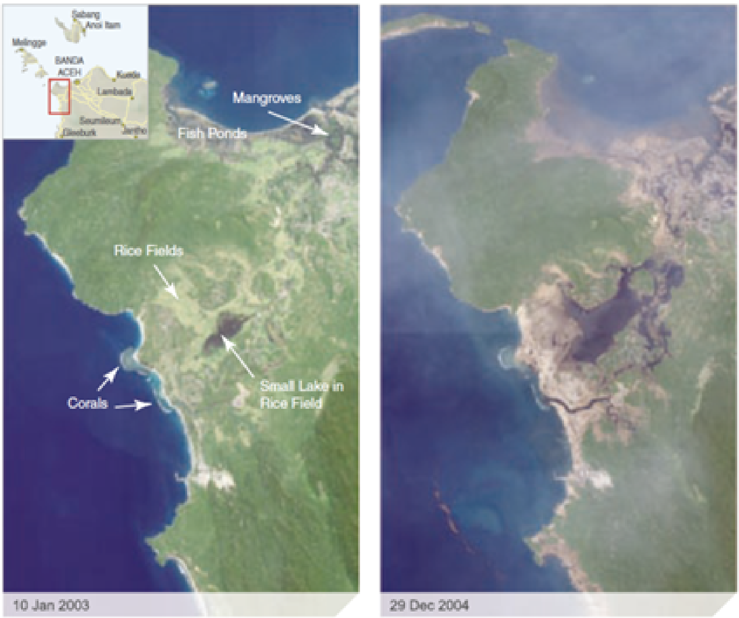
Source: (European Space Agency, 2018)

The next step would be mapping environmental damage, humanitarian aid, and rebuilding the region. The impacts of the 9.0 earthquake and tsunami were far-reaching across Indonesia, India, Malaysia, Maldives, Sri Lanka, Thailand, and Africa (DeepSea News, 2011). The satellite disaster mapping was able to identify the next environmental impacts:

- Solid Waste disaster debris and sewage
- Containment of soil and water
- Loss of infrastructure and Facilities
- Loss of natural ecosystems
- Notification of Coastal Waters
- Impact on biological communities and species

Solid waste and debris had an impact on all surrounding ecosystems. Given the mix of concrete, raw sewage, and other building waste materials, mixed were sent into the sea. The loss of life was believed to be over 100,000 souls. Once the damage assessment was complete, researchers requested a detailed vulnerability assessment of the region as part of the rebuilding effort. Poverty, structural design, and geological conditions were the top outcomes of the earthquake vulnerability assessment. Researchers considered secondary hazards such as landslides and fire. GIS mapping tsunami vulnerabilities included the ecosystem, structure, and social vulnerabilities.

Figure 7-6 Satellite Images Of Environmental Impact On Coast Post-December 26, 2004, Tsunami



Source: (DeepSea News, 2011)

Figure 7-6 gave recovery management an overview of the environmental damage to northern Sumatra in Indonesia. The tsunami wiped out the low-lying delta land, destroyed fishponds, and removed coastal vegetation. The loss of this mangrove cover is critical; this tropical timber thrives in salty seawater. These tropical trees can store large amounts of carbon, a crucial component of fighting climate change. The images also show a pocket of missing silt and soil, which stores carbon, another protection from climate change. The sandy beaches have been removed (important in some locations for turtle nesting), and the deposition of silt or mud on the reef (DeepSea News, 2011).

Global Health

The passion for science, technology, and innovation combined with space manifested during the COVID-19 pandemic. The United Nations Office for Outer Space brought together the globe to work together to use information gathered from UN Member States satellite infrastructures to understand risks, drive policy, understand the spread of COVID-19, population movement, and communication. Pandemic times highlighted part of the capacity to use space for disaster risk management; maximum potential in all corners of the world is yet to come.

COPERNICUS

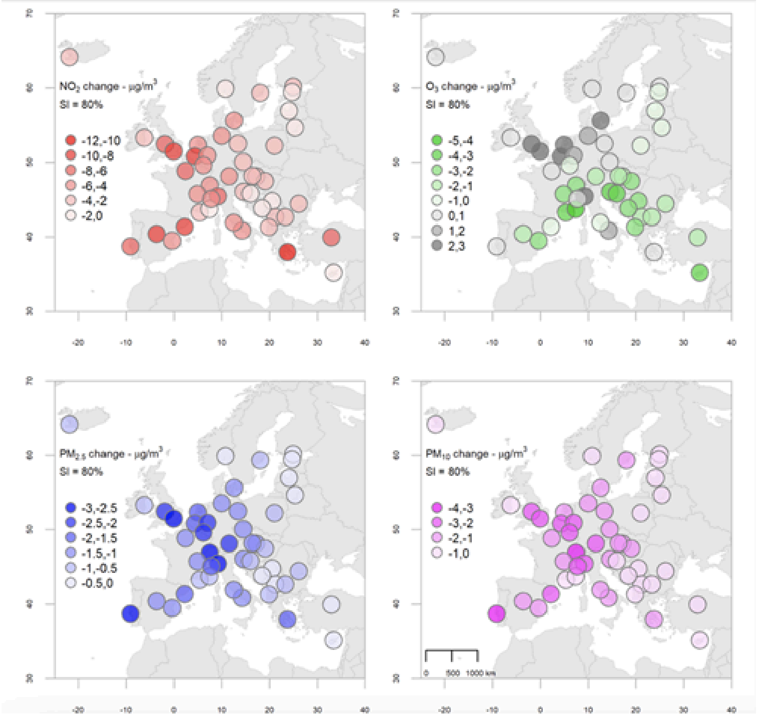
Copernicus is a component of the European Union's space program, with funding by the EU, and is its flagship Earth observation program, which operates through six thematic services: Atmosphere, Marine, Land, Climate Change, Security, and Emergency. It delivers freely accessible operational data and services providing users with reliable and up-to-date information about our planet and its environment. The program is coordinated and managed by the European Commission and implemented in partnership with the Member States, the European Space Agency (ESA), the European Organization for the Exploitation of Meteorological Satellites (EUMETSAT), the European Centre for Medium-Range Weather Forecasts (ECMWF), EU Agencies and Mercator Ocean, amongst others. (UN-SPIDER, 2020). During the pandemic, Copernicus provided EMS Rapid Mapping for COVID -19. The rapid mapping produced dynamic satellite maps, continuous census of installed infrastructure, and merging with population data to check the actual level of usage versus expected in designing, assisting with the buildout of mobile and temporary hospital infrastructure. Early in the pandemic, Copernicus was key in monitoring boardercross after lockdown directives by European countries. Optical VHR Data geospatial reporting delivered real-time images of important traffic queues at the EU border areas (i.e., traffic jams, including the details of the number of trucks versus the number of vehicles not moving) (UNOOSA, 2020).

Figure 7-7 Copernicus monitors the impact of traffic congestion at border crossings between the EU Member States during COVID- 19

Source: (UNOOSA, 2020)

Images from Copernicus were used as a decision and support tool for policy definition to determine the opening of street markets, green areas, and parks. The satellite maps with access points, land use, and usable areas were merged with population data to project the maximum number of people who can stay in an area versus limits defined by law regulation of access points. Governments using Copernicus looked at satellite maps of open areas (i.e., parks) to understand access points collated with the surrounding population to formulate policies for a maximum number of people peruse the area. (UNOOSA, 2022)

Figure 7-8 Change in concentration of NO2, ozone, and particulate matter



Source: (Atmosphere Monitoring Service, 2022)

Unique datasets originating from Copernicus Atmosphere Monitoring Service (CAMS) during the pandemic brought to light the level of air quality impacts back the length of life. By using observed changes in daily concentrations of the pollutants studied, combined with an assessment of people's exposure, scientists estimate that a total of over 800 deaths were avoided with improved air quality resulting from the governmental measures taken to limit the spread of the SARS-Cov-2 virus (Atmosphere Monitoring Service, 2022). Paris, London, Barcelona, and Milan were among the top six cities with the highest number of avoided deaths (Atmosphere Monitoring Service, 2022). There was a reduction in road transport, leading to a decrease in Nitrogen Dioxide (NO2) by over half across European cities. Vincent-Henri Peuch, Director of the Copernicus Atmosphere Monitoring Service (CAMS), commented, " ...beyond the analysis of the mortality during the first months of the pandemic, this study could help shape future policy as the public health benefits of reducing pollution in our cities and the effectiveness of certain measures are clear to see," (Atmosphere Monitoring Service, 2022).

The evolution of the COVID-19 pandemic in countries around the world using GIS and web-based dashboards, the wider reach of communication technologies, and the increasing availability of information technologies opened an opportunity for increased use of space-based solutions in these times of crises (UN-SPIDER, 2021)

Conclusions

Space applications related to telecommunications and global navigation can play a vital role in supporting disaster risk reduction, response, and recovery efforts (St-Pierre, 2016). Satellite imagery can help monitor the evolution of populations, infrastructure, and environment, offering the ability to contrast and identify vulnerabilities. Outer space can help be better prepared and reduce the volatility of the impacts of disasters. Collaborations across all nations to have the ability to access the data and develop plans for disaster preparedness are part of a piece of saving the planet from climate change.

References

Atmosphere Monitoring Service. (2022, January 26). *More than 800 deaths may have been avoided due to air quality improvement during the first lockdown phase in Europe | Copernicus.* Retrieved August 26, 2022 from Copernicus Atmosphere Monitoring Service: https://atmosphere.copernicus.eu/more-800-deaths-may-have-been-avoided-due-air-quality-improvement-during-first-lockdown-phase

DeepSea News. (2011, March 21). *From the Editor's Desk: The Environmental Impacts of Tsunamis.* Retrieved August

27, 2022 from Deep Sea News: https://www.deepseanews.com/2011/03/from-the-editors-desk-the-environmental-impacts-of-tsunamis/

European Space Agency. (2018, December 12). *A year on from the Asian tsunami, satellites are aiding regional rebuilding.* Retrieved August 26, 2022 from European Space Agency: https://www.esa.int/Applications/Observing_the_Earth/A_year_on_from_the_Asian_tsunami_satellites_are_aiding_regional_rebuilding

EUSPA. (2022, August 26). *Using Copernicus data to climate-proof cities.* Retrieved August 26, 2022 from European Union Agency for the Space Programme: https://www.euspa.europa.eu/newsroom/news/using-copernicus-data-climate-proof-cities

1. Le Cozannet, M. Kervyn, S. Russo, C. Ifejika Speranza, P. Ferrier, M. Foumelis, T. Lopez & H. Modaressi. (n.d.).

Gaffney, O., & Steffen, W. (2017, February 10). The Anthropocene equation. *The Anthropocene Review, 4*(1), 53-61. From https://journals.sagepub.com/doi/abs/10.1177/2053019616688022

Hurlimann, A., Moosavi, S., & Browne, G. (2020, August 13). *Urban planning policy must do more to integrate climate change adaptation and mitigation actions.* Retrieved August 24, 2022 from Science Direct:

https://www.sciencedirect.com/science/article/abs/pii/S0264837720325266#:~:text=Well%2Ddesigned%20urban%20planning%20policy,change%20adaptation%20and%20or%20mitigation.

Le Cozannet, G., Kervyn, M., & Russo, S. (2020, March 10). *Space-Based Earth Observations for Disaster Risk Management.* Retrieved August 17, 2022 from NASA/ADS: https://ui.adsabs.harvard.edu/abs/2020SGeo...41.1209L/abstract

Lea, R. (2022, May 11). *The History Of Satellites Explained.* Retrieved August 22, 2022 from SlashGear: https://www.slashgear.com/860409/the-history-of-satellites-explained/

NASA. (2017, October 4). *Oct. 4, 1957 – Sputnik, the Dawn of the Space Age.* Retrieved August 22, 2022 from NASA: https://www.nasa.gov/image-feature/oct-4-1957-sputnik-the-dawn-of-the-space-age

NASA. (2022). *Evidence | Facts – Climate Change: Vital Signs of the Planet.* Retrieved August 10, 2022 from NASA Climate Change: https://climate.nasa.gov/evidence/

NASA. (2022, August 15). *Recent Imagery Incorporating Aqua Data.* Retrieved August 26, 2022 from Aqua Earth-observing satellite mission | Aqua Project Science: https://aqua.nasa.gov/

Okosvaros. (2020, July 30). *Okosvaros.* Retrieved August 12, 2022 from Vienna's first climate-adapted street | Smart City: http://okosvaros.lechnerkozpont.hu/en/node/744

Satellite Imaging Corporation. (2022). *Urban Planning | Satellite Imaging Corp.* Retrieved August 26, 2022 from Satellite Imaging Corporation: https://www.satimagingcorp.com/applications/environmental-impact-studies/urban-planning/

St-Pierre, L. (2016, November 22). *Outer space is driver for disaster risk management, sustainable development – UN expert.* Retrieved August 27, 2022 from UN News: https://news.un.org/en/story/2016/11/546112-outer-space-driver-disaster-risk-management-sustainable-development-un-expert

Thiessen, M. (2022, May 19). *Oct 4, 1957 CE: USSR Launches Sputnik.* Retrieved August 22, 2022 from National Geographic Society: https://education.nationalgeographic.org/resource/ussr-launches-sputnik

U.S. Global Change Research Program. (2022). *Understand Climate Change.* Retrieved August 26, 2022 from GlobalChange.gov: https://www.globalchange.gov/climate-change

UNICEF. (2018, October 1). *Deadly earthquake and tsunami hit Indonesia.* Retrieved August 26, 2022 from UNICEF: https://www.unicef.org/stories/deadly-earthquake-and-tsunami-hit-indonesia

United Nations. (2015, March). *Sendai Framework for Disaster Risk Reduction 2015 – 2030.* Retrieved August 26, 2022 from PreventionWeb.net:

https://www.preventionweb.net/files/43291_sendaiframeworkfordrren.pdf

UNOOSA. (2020, May 18). *UNOOSA Space4Health Webinar – Afternoon Session.* Retrieved August 24, 2022 from YouTube: https://www.youtube.com/watch?v=3d_hyutqu7s

UNOOSA. (2022, January). *Benefits of space: Disasters.* Retrieved August 26, 2022 from UNOOSA: https://www.unoosa.org/oosa/en/benefits-of-space/disasters.html

UN-SPIDER. (2020, March 11). *Coronavirus disease (COVID-19) | UN-SPIDER Knowledge Portal.* Retrieved August 24, 2022 from UN-Spider: https://www.un-spider.org/advisory-support/emergency-support/12182/coronavirus-disease-covid-19

UN-SPIDER. (2021, November 16). *Space-based Solutions for Disaster Management in Africa: Networks and Information Technologies in times of crisis.* Retrieved August 26, 2022 from UN-Spider: https://un-spider.org/sites/default/files/concept-note-un_spider-bonn-conference-2021.pdf

8.

BIO-THREATS TO AGRICULTURE-SOLUTIONS FROM SPACE (SINCAVAGE, CARTER, NICHOLS)

Student Objectives

- To introduce common bioterrorism definitions, animal diseases, human diseases, and zoonoses.
- To recognize that biological attacks on agriculture can be low-tech, high-impact bioterrorism.
- What are the five potential targets of agricultural bioterrorism?
- Describe two ways remote sensing can be used to identify agricultural threats to crops.
- How can satellite observations predict vulnerable targets conducive to plants and livestock?

Definitions

Agroterrorism is a subset of bioterrorism and is defined as the deliberate introduction of an animal or plant disease to generate fear, causing economic losses and/or undermining stability. (O.S. Cupp, 2004)

Bioterrorism is the threat or use of biological agents by individuals or groups motivated by political, religious, ecological, or other ideological objectives.

Earth Observation Epidemiology or **tele-epidemiology** is defined as 'using space technology with remote sensing in epidemiology. (Wiki, 2022)

MASINT – Measurement and signature intelligence (**MASINT**) is a technical branch of intelligence gathering that detect, track, identify or describe the distinctive characteristics (signatures) of fixed or dynamic target sources. This often includes radar, acoustic, nuclear, chemical, and biological intelligence. MASINT is scientific and technical intelligence derived from the analysis of data obtained from sensing instruments to identify any distinctive features associated with the source, emitter, or sender, to facilitate the latter's measurement and identification. (Wiki, 2022)

OSI, short for OPEN-SOURCE Intelligence (also known as OSINT), is defined as any intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience to address a specific intelligence requirement. (Bazzell, 2021)

Remote Sensing (RS) uses non-ground-based imaging systems to obtain information about processes and events on Earth. It is unique among the detection and diagnostic methods discussed herein in its ability to offer passive monitoring for the disease at scale rather than active sampling. (Silva & et.al, 2021)

Introduction

Bio-threats to agricultural resources are commonly natural. However, rival governments, terrorists, and rogue actors can target critical agricultural infrastructure. The deliberate introduction of an animal or plant disease to generate fear, cause economic losses, and/or undermine stability is known as Agroterrorism, a subset of bioterrorism. (O.S. Cupp, 2004)

Terrorist groups may be motivated to attack plants, animals, or agricultural products to attract attention to a cause, incite fear, disrupt society, or demonstrate a capability to exact political concessions. Others may be prompted by motives such as economic interest, sabotage, or revenge (Ban, 2000). In the event of an agroterrorism attack, keeping the biological incursion from inflicting significant damage to human health and the economy will depend heavily on quick alerts to farmers and disease specialists.

Currently, satellite and sensor technologies are revolutionizing crop and livestock disease detection. These technologies can be used individually or in combination to support agricultural surveillance and communication to assist and mitigate threats on the ground. Satellite imaging detects the distinct environmental conditions that may serve as a refuge for the disease-carrying animals. Electromagnetic spectra also provide useful information to make decisions regarding plant physiological stress. In a captured image, plant disease is identified by observing the physiological disturbances caused by foliar reflectance in a near-infrared portion of the spectrum.

Diseases have a Significant Negative impact on Agricultural Productivity.

The burden of agriculture on endemic and naturally imported epidemic diseases is high. It confirms the capacity of animal and plant diseases to cause economic harm. The United States is free of many significant global livestock diseases because of effective surveillance of herds and imports and aggressive eradication campaigns. (Howard, 2013) In general, losses from animal disease account for 17% of the production costs of animal products in the developed world and twice that amount in the developing world.

The cost of crop diseases to the US economy has been estimated to be more than $30 billion / year. The costs include reducing quantity (bushels/acre) and quality (blemished fruit, toxins in grain) yield, short-term control costs, pesticides, and long-term management and harvesting. (Howard, 2013)

What are the Agriculture, Livestock, and Companion Animal Weapons?

The Animal and Plant Health Inspection Service (APHIS), the US Department of Agriculture (USDA) and The Center for Food Security and Public Health (CFSPH) have developed some serious wallcharts about Agriculture and Zoonotic Bioterrorism. These wallcharts portray the threats that must be considered in every risk assessment to develop detection, mitigation, and recovery countermeasures.

The Center for Food Security and Public Health (CFSPH) at Iowa State University has developed two charts titled "Animal Disease From Potential Bioterrorist Agents" that show the CDC Category, (A-C) the severity (mild, moderate, severe) of disease in potentially affected species [cattle, sheep, goats, pigs, horses, dogs, cats, birds and other], incubation period and prominent clinical signs. (CFSPH, 2022) All of the charted diseases and agents in these charts have technical fact sheets and they may be found at: (Spickler, 2022)

The Center for Food Security and Public Health (CFSPH) at Iowa State University has developed two charts titled "Human Disease From Potential Bioterrorist Agents" that show the CDC Category (A-C), route of transmission, potential body system affected (Septicemia, Respiratory, Intestinal, Cutaneous, Ocular, and Neurological), incubation period in days, person to person contact and prominent clinical signs. (CFSPH, 2022) All of the charted diseases and agents in these charts have technical fact sheets and they may be found at: (Spickler, 2022)

The Center for Food Security and Public Health (CFSPH) at Iowa State University has developed two charts titled "USDA High Consequence Foreign Animal Disease and Pests" which show the disease or agent in tiers (Tier 1- Tier 3), humans affected, species affected, incubation period, mode of transmission, and prominent clinical signs in animals. (CFSPH, 2022) All of the charted diseases and agents in these charts have technical fact sheets and they may be found at: (Spickler, 2022)

The Center for Food Security and Public Health (CFSPH) at Iowa State University has developed two charts titled "Select Zoonoses of Companion Animals" that show Animal Impact by disease category (Bacteria, Viruses, Fungi, Parasites) on species with Zoonotic Potential (Dogs, Cats, Birds, Ferrets, Rabbits, Rodents and other), incubation period, and prominent clinical signs. (CFSPH, 2022) All of the charted diseases and agents in these charts have technical fact sheets and they may be found at: (Spickler, 2022)

The Center for Food Security and Public Health (CFSPH) at Iowa State University has developed two charts titled "Select Zoonoses of Companion Animals" that show Human Impact by disease category (Bacteria, Viruses, Fungi, Parasites) , person to person vector transmission, transmission from animals, potential body system affected (Septicemia, Respiratory, Intestinal, Cutaneous, Ocular, Neurological, and Death), incubation period, and prominent clinical signs. (CFSPH, 2022) All of the charted diseases and agents in these charts have technical fact sheets and they may be found at: (Spickler, 2022)[1]

Potential Targets of Agricultural bioterrorism

There are five potential targets of agricultural bioterrorism: *field crops; farm animals; food items in the processing or distribution chain; market-ready foods at the wholesale or retail level; and agricultural facilities, including processing plants, storage facilities, wholesale and retail food outlets, elements of the transportation infrastructure, and research laboratories.* (Nichols & Carter, 2022) (Parker, 2002) (Wilson, 2000) (Bipartisan Committee on Biodefense, 2022) (Carus, 2015)

Developing a consensus for a list of the major bioterrorist threats and action items is thus the priority in protecting crops and animals. Such a list is necessary to guide the development of surveillance plans, diagnostic tests, and response plans for best containing and eradicating an introduced pathogen. Here is one from the Bipartisan Committee on Biodefense: (Bipartisan Committee on Biodefense, 2022)

■ direct losses of agriculture commodities to diseases

■ costs of diagnosis and surveillance

■ required the destruction of contaminated crops and animals to contain the disease

■ costs of disposal of mortalities and carcasses

■ damage to consumer and public confidence

■ need for long-term quarantine of infected areas

- losses due to export and trade restrictions
- disruption of commodity markets.

Containment, Eradication & Control

Introducing exotic pathogens that cause highly contagious animal or plant diseases may elicit rapid and aggressive attempts to contain and eradicate them. Still, these measures cause more economic damage in the short term than the disease itself. Cost may not be the primary factor if the infectious disease becomes endemic. (Howard, 2013)

Containment and eradication of exotic animal diseases are commonly done by culling the potentially exposed animal to break the chain of transmission. (N.M. Ferguson, 2001) Many animal diseases (potential bioterrorist threats) are caused by viruses, for which there are limited therapies once the animal is infected. Fungi cause about 75% of plant diseases. These can be controlled with varying degrees of effectiveness by applying fungicides. (Strange, 1993)

Transmission of bacterial and viral crop diseases is difficult to control with chemical pesticides unless insect vectors transmit the diseases. (Madden & et.al., 2000) Because of these difficulties, containment and eradication of bacteriological pathogens depend heavily on quarantining infected areas and removing infected and exposed plants. (Howard, 2013)

Agricultural Bioterrorist Attack Requires Relatively Little Expertise Or Technology

One of the reasons that a bioterrorist attack on human populations is difficult is that the development of an effective bioweapon is a technically daunting task. Many bioagents are poorly transmitted to humans requiring large amounts to be disseminated to cause mass casualties. The only way to cause mass damage is to use a respirable aerosol. This is also a danger to the perpetrators. (Howard, 2013) (Nichols & Carter, 2022)

The same difficulties do not exist for many of the diseases that would affect agricultural bioterrorist weapons. These diseases of animals and crops are highly contagious and spread effectively from the point source. Moreover, humans can safely handle the causative organisms without risk of infection. There is no need for vaccination, special precautions, or prophylactic antibiotic use. (Howard, 2013) (Nichols & Carter, 2022)

Material to initiate the plant or animal disease outbreak can be produced in small quantities – a few milligrams could be sufficient to initiate multiple outbreaks in widely separated locations. The raw materials can easily be smuggled into the US. They do not even need to be created in a laboratory. (Howard, 2013)

Dissemination requires little experience. Animal virus preparations can be diluted and disseminated with a simple atomizer in close proximity to the animals. Simply exposing a mass of sporulating fungi in the air immediately upward of a target field could be effective for plant diseases. Weather is the only fly in the ointment. One nightmare scenario is the introduction of a pathogen without perpetrators entering the US. Sorghum is planted on both sides of the Southern border, and wheat and barley are along the Canadian – US border. Multiplication of pathogens in the foreign acreage could lead to numbers of spores blowing across the US border and initiating the escalating outbreak. An advantage to the terrorists is that disease surveillance and control programs are less effective/rigorous OCONUS. (Howard, 2013)

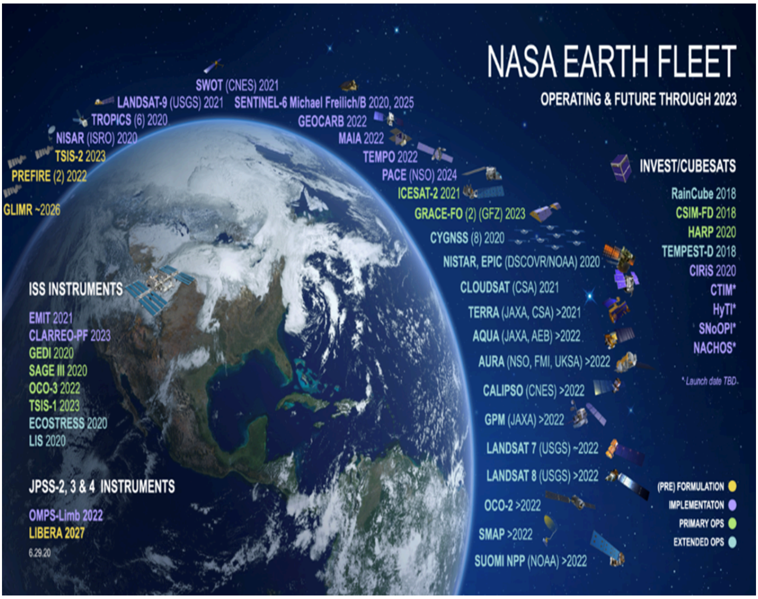
BIO-THREATS TO AGRICULTURE – SOLUTIONS FROM SPACE (AGRO-TERRORISM)

Monitoring of plant pathogens

What is needed?

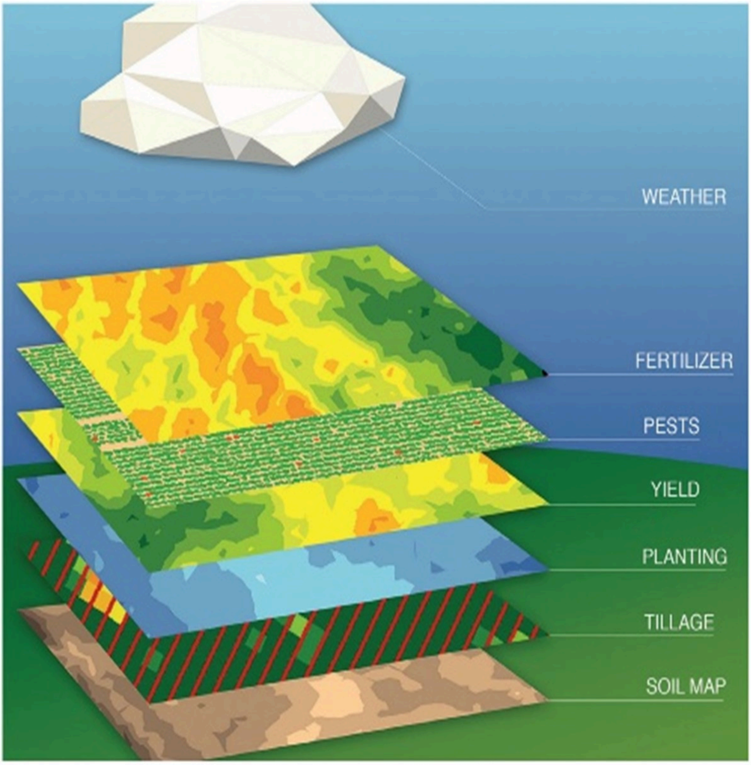
Answer: A real-time monitoring and communication of abnormalities within livestock and crops using satellite technology. Figure 8-1 shows the operating and planned NASA Earth Fleet through 2023. The Landsat series is particularly useful for agricultural bioterrorism studies. (NASA, 2021)

Figure 8-1 NASA Earth Fleet



Source: (NASA, 2021)

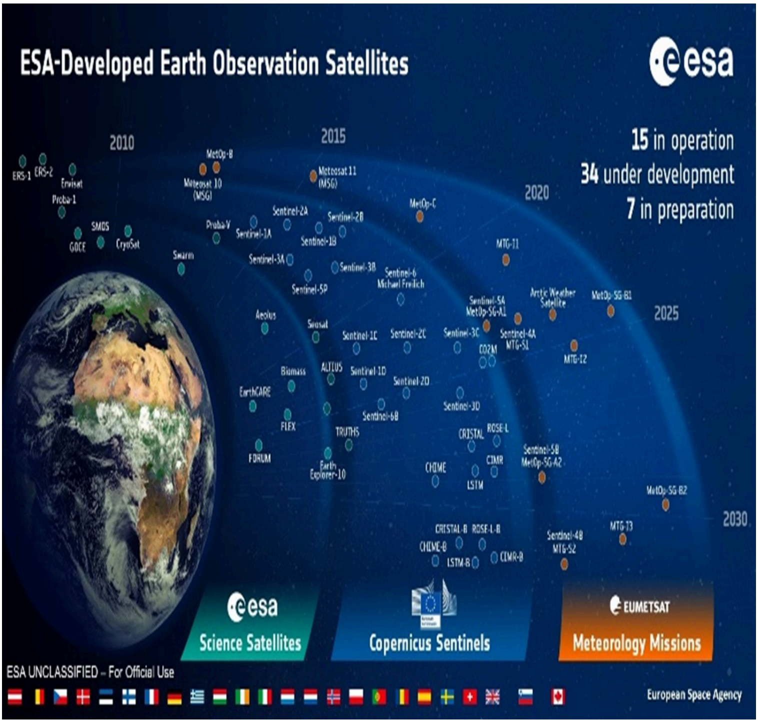
Figure 8-2 Layers of Agriculture Investigation



Source: (NASA, 2021)

Figure 8-2 shows the agriculture density map where satellites must penetrate with MASINT sensors. (NASA, 2021) Figure 8-3 shows the ESA operational plan for its satellites. (ESA, 2019) Figure 8-4 shows the satellites used to help researchers and defense analysts develop intelligence and data for various missions.

Figure 8-3 ESA Developed Earth Observation Missions Pillars



Source: (ESA, 2019)

Figure 8-4 ISR Satellites and their Missions Diversity

ENVISAT
LANDSAT
RADARSAT
SPOT
Ngari
Muztagh Ata
Everest
Nam Co
Nyingchi
Climate
Lakes
Grasslands
Glacier
Ecology

Source: (NASA, 2021)

MASINT

Broadband and multispectral methods rely primarily on visible (VIS) and near-infrared (NIR) reflectance indices, such as normalized difference vegetation index (NDVI). Ability to offer passive monitoring for the disease at scale rather than active sampling. A change in plant behavior could show indications of tampering by bad actors when geological and meteorological variables have been accounted for. (Silva & et.al, 2021)

Remote Sensing (RS) is a technique for obtaining information on an object without physical contact by measuring the electromagnetic energy reflected/backscattered or emitted by the surface of the Earth (Freek D. van der Meer, 2007).

"A significant step forward in earth observation was made with the development of imaging spectrometry. Imaging spectrometers measure reflected solar radiance from the Earth in many narrow spectral bands. Such a spectroscopical imaging system can detect subtle absorption bands in the reflectance spectra and measure the reflectance spectra of various objects with very high accuracy. As a result, imaging spectrometry enables better identification of objects at the Earth's surface and better quantification of the object properties than can be achieved by traditional earth observation sensors such as Landsat TM and SPOT. " (Freek D. van der Meer, 2007)

As a noncontact technique, we include in the definition of RS also spectral measurements acquired by portable instruments such as handheld spectroradiometers (also called proximal sensing). These measurements are processed and analyzed to retrieve information on the object observed (i.e., plant health, in this case). RS is an indirect assessment technique, able to monitor vegetation conditions from a distance and evaluate the spatial extent and patterns of vegetation characteristics and plant health in this application. Sensors can be distinguished into active or passive; whether they emit artificial radiation and measure the energy reflected or backscattered (active sensors), the reflected solar radiation, or the emitted thermal radiation (passive sensors). (Martinelli, 2015)

Monitoring of Invasive Plants

Publicly available scientific literature about Agroterrorism, biological crimes, and biological warfare targeting livestock and poultry dates back over 100 years. Copious research reports, peer reviews, books, and studies characterizing bioterrorism risks, threats, impact, and detection methods for/ to plant ecosystems and the US economy. They have been published as OSI. Similarly, research reports, papers, and special government studies have been completed detailing *effective plant-advanced bioterrorism countermeasures*. These are generally CLASSIFIED and not OSI. They will not be addressed in this chapter.[2] [3] We will briefly discuss two interesting OSI / UNCLASSIFIED studies/ examples performed to *monitor* invasive plants. We will then conclude with a feedlot concern.

The effective and regular remote monitoring of agricultural activity is not always possible in developing countries because access to cloud-based geospatial analysis platforms or expensive high-resolution satellite images is not always available. High-resolution satellite images medium-resolution satellite images were used to map the spatial distribution of sickle bush (*Dichrostachys cinerea*), an archetypal allochthonous invasive plant in Cuba that is becoming impossible to control owing to its rapid growth in areas planted with sugar cane in the

Trinidad-Valle de Los Ingenios area (Cuba), a UNESCO World Heritage Site. (E. Moreno, 2021)

"Two images were used (WorldView-2 and Landsat-8); these were subjected to supervised classification, with accuracy values of 88.7% and 93.7%, respectively. Vegetation cover was first derived from the WorldView-2 image. This information was then used as the training field to obtain spectral signatures from the Landsat-8 image so that Landsat images may be regularly used to monitor *D. cinerea* infestations. The results obtained in the spatial distribution map for sickle bush in the Landsat-8 images had overall reliability of 93.7% and a Kappa coefficient reliability of 91.9%. These values indicate high confidence in the results, which suggests that sickle bush has invaded 52.7% of the total 46,807.26-ha area of the Trinidad-Valle de Los Ingenios. This process proved extremely effective and demonstrated the benefits of using high-resolution spatial images from which information can be transferred to free satellite images with larger pixel size." (E. Moreno, 2021)

Another satellite study performed by B. Chen and colleagues**. (Chen & et.al., 2019)** California's Central Valley continually faces serious challenges of water scarcity and degraded groundwater quality due to nitrogen leaching. Orchard age is one of the key determinants of fruit and nut production and directly affects consumptive water and fertilizer demand. Chen developed a robust detection method to track crop cover dynamics and identify the planting year through time series of Landsat imagery within the Google

Earth Engine (GEE) platform. They used a full archive of Landsat data (Landsat-5 TM, Landsat-7 ETM+, and Landsat-8 OLI) from 1984 to 2017 as inputs and automated the GEE workflow for the on-fly mapping. (Chen & et.al., 2019)

Chen's method showed very high accuracy in estimating tree crop ages, with an R2 of 0.96 and a mean absolute error of less than half a year, when compared with 142 records provided by almond growers. They further evaluated the accuracy of the statewide mapping of planting years for all fruit and nut trees in California and found an overall agreement of 89.2%. (Chen & et.al., 2019)

Feedlot density detection

The highly concentrated breeding and rearing practices of our livestock industry make it a vulnerable target for terrorists because diseases could spread rapidly and be very difficult to contain. For example, 80 and 90 percent of grain-fed beef cattle production is concentrated in less than 5 percent of the nation's feedlots. Therefore, deliberately introducing a highly contagious animal disease in a single feedlot could have serious economic consequences. (epidemiology) (Agroterrorism: What Is the Threat and What Can Be Done About It?, 2004)

There is a concern about creating transgenic plant pathogens, pests, or weeds resistant to conventional control methods. This prospect has already been realized through developing a genetically mutant superweed, reportedly resistant to current herbicides. The superweed was reportedly designed to "attack corporate monoculture" and target genetically engineered crops. (Parker, 2002)

According to Plant Health Inspection Service (APHIS), Earth Observation Epidemiology, or tele-epidemiology, is one of the most promising technologies to monitor feedlot density and diseases. Satellite imaging detects the distinct environmental conditions that may serve as a refuge for the disease-carrying animals. Electromagnetic spectra also provide useful information to make decisions regarding plant physiological stress. (Martinelli, 2015) (APHIS & USDA, 2022)

Conclusions

Despite the US's best efforts, the US will continue to be vulnerable to deliberate introductions of exotic plant and animal diseases by terrorist groups. The vulnerability to agricultural biological attack is a consequence of intrinsically low security of agricultural targets, the technical ease of engagement, and the large economic repercussions of even small outbreaks.

The good news is that the US is aggressively stepping up its ISR efforts via satellite. Satellite intelligence on agricultural and cattle feeding zones reduces the risks of successful attacks.

References

Agroterrorism: What Is the Threat and What Can Be Done

About It? (2004). Retrieved from https://www.rand.org/: https://www.rand.org/pubs/research_briefs/RB7565.html

APHIS & USDA. (2022). *wallchart-animal-disease-from-potential-bioterrorist-agents.* Retrieved from https://www.cfsph.iastate.edu: https://www.cfsph.iastate.edu/pdf/wallchart-animal-disease-from-potential-bioterrorist-agents

Ban, J. (2000, June). *Agricultural Biological Warfare: An Overview.* Retrieved from https://www.ojp.gov/ncjrs: https://www.ojp.gov/ncjrs/virtual-library/abstracts/agricultural-biological-warfare-overview

Bazzell, M. (2021). *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information, 8th edition.* Bazzell.

Bipartisan Committee on Biodefense. (2022, June). *defense-of-animal-agriculture/.* Retrieved from https://biodefensecommission.org: https://biodefensecommission.org/reports/defense-of-animal-agriculture/

Carus, W. (2015, Aug 10). The History of Biological Weapons Use: What We Know and What We Don't. *Health security*, pp. 13.4 (2015): 219-255. Retrieved from https://www.liebertpub.com/: https://www.liebertpub.com/doi/10.1089/hs.2014.0092

CFSPH. (2022). *select-zoonotic-diseases-of-companion-animals-wallchart/.* Retrieved from https://www.cfsph.iastate.edu:

https://www.cfsph.iastate.edu/product/select-zoonotic-diseases-of-companion-animals-wallchart/

Chen, B., & et.al. (2019, May). *Automatic mapping of planting year for tree crops with Landsat satellite time series stacks.* Retrieved from https://www.sciencedirect.com: https://www.sciencedirect.com/science/article/abs/pii/S0924271619300802

1. Moreno, e. (2021, Sept 29). *Affordable Use of Satellite Imagery in Agriculture and Development Projects: Assessing the Spatial Distribution of Invasive Weeds in the UNESCO-Protected Areas of Cuba.* Retrieved from https://www.mdpi.com: https://www.mdpi.com/2077-0472/11/11/1057

ESA. (2019, May). *ESA-developed_Earth_observation_missions_pillars.jpg.* Retrieved from https://www.esa.int: https://www.esa.int/var/esa/storage/images/esa_multimedia/images/2019/05/esa-developed_earth_observation_missions/19415135-3-eng-GB/ESA-developed_Earth_observation_missions_pillars.jpg

Freek D. van der Meer, S. d. (2007, July 27). *Imaging Spectrometry: Basic Principles and Prospective Applications.* Retrieved from https://books.google.com/: https://books.google.com/books/about/Imaging_Spectrometry.html?id=XDBRCpQy64UC

Howard, J. J. (2013). *Weapons of Mass Destruction and Terrorism.* NYC: McGraw Hill.

Madden, L., & et.al. (2000). A theoretical assessment of the effects of vector-virus transmission mechanism on plant virus disease epidemics. *Phytopathology*, pp. 90:576-594.

Martinelli, F. e. (2015). *Advanced methods of plant disease detection. A review.* Retrieved from https://link.springer.com/article/10.1007/s13593-014-0246-1:
https://link.springer.com/article/10.1007/s13593-014-0246-1

N.M. Ferguson, D. C. (2001). Transmission Intensity and impact of control policies on the foot-and-mouth epidemic in Great Britain. *Nature*, pp. 413: 542-548.

NASA. (2021, April). *NASA_satellite_fleet.jpg.* Retrieved from https://gpm.nasa.gov/: https://gpm.nasa.gov/sites/default/files/2021-04/NASA_satellite_fleet.jpg

Nichols, & Carter, H. J. (2022). *Drone Delivery of CBNRECy – DEW Weapons: Emerging Threats of Mini-Weapons of Mass Destruction and Disruption (WMDD).* Manhattan, KS: New Prairie Press #46.

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

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, #38.

O.S. Cupp, D. W. (2004). Agroterrorism in the U.S.: key security challenge for the 21st century. *Biosecurity and Bioterrorism: Biodefense Strategy, Practice and Science 2, 97–105.*, pp. 2, 97–105. Retrieved from https://pubmed.ncbi.nlm.nih.gov/15225403/: https://pubmed.ncbi.nlm.nih.gov/15225403/

Parker, H. S. (2002). *McNair_65_agriculturalbioterrorism.pdf.* Retrieved from https://www.files.ethz.ch: https://www.files.ethz.ch/isn/10897/McNair_65_agriculturalbioterrorism.pdf

Silva, G., & et.al. (2021, May 20). Plant pest surveillance: from satellites to molecules. *Emerg Top Life Sci.*, pp. 5(2):275-287. doi:10.1042/ETLS20200300. PMID: 33720345; PMCID: PMC8166340.

Spickler, A. R. (2022, October 6). *bioterrorismdisease or agents have technical fact sheets.* Retrieved from https://www.cfsph.iastate.edu: https://www.cfsph.iastate.edu/diseaseinfo/factsheets/

Strange, R. (1993). *Plant Disease Control.* London: Chapman and Hall.

Wiki. (2022). *Measurement_and_signature_intelligence (MASINT) definition.* Retrieved from https://en.wikipedia.org: https://en.wikipedia.org/wiki/Measurement_and_signature_intelligence

Wiki. (2022, Aug 26). *Tele-epidemiology.* Retrieved from https://en.wikipedia.org: https://en.wikipedia.org/wiki/Tele-epidemiology

Wilson, T. M. (2000, Sept). Agroterrorism, Biological Crimes, and Biowarfare Targeting Animal Agriculture: The Clinical, Pathologic, Diagnostic, and Epidemiologic Features of Some Important Animal Diseases. *Emerging diseases of animals*, 23-57. Retrieved from https://www.sciencedirect.com: https://www.sciencedirect.com/science/article/abs/pii/S0272271218300222

Endnotes

[1] These wallcharts are packed with excellent information and recommended.

[2] All research and writings must be OPEN Sourced, UNCLASSIFIED, and verifiable with reliable sources. This is the managing editor's strict policy.

[3] Risk assessment for bioterrorism and other forms of terrorist attacks are discussed in (Nichols R. K., Unmanned Vehicle Systems and Operation on Air, Sea, and Land, 2020)

9.

MODELING, SIMULATIONS, AND EXTENDED REALITY (OETKEN)

This chapter provides an overview of immersive technology and surrounding use cases in emerging space systems. Recent advancements in virtual, augmented, and extended reality technologies have created new and exciting frameworks in the areas of simulation, modeling, and training. This chapter explores those frameworks and provides insight into how they fit within current and future space systems.

Student Learning Objectives

After reading this chapter, students should be able to do the following:

1. Define and differentiate virtual, augmented, and extended reality
2. Describe the framework of a virtual environment

3. Define and differentiate the degrees of freedom in immersive simulation
4. Differentiate use case protocols for augmented versus extended reality technology integration in space systems

Foundations of Immersive Systems Technology

Immersive technology and its relationship to human-centered emerging space systems have the potential to significantly enhance many facets of aerospace design and space exploration. Immersive systems are the technologies used to create an experience where system engineers and designers enhance parts of a user's physical world with computer-generated input (The Interaction Design Foundation, 2021) Emerging space systems can be enhanced through immersive technologies that use virtual reality (VR), augmented reality (AR), and extended reality (XR). System engineers and designers are on the threshold of a tremendous opportunity to enhance and improve the user experience for pilots, astronauts, and other space-related occupations by embedding immersive systems technologies in the lab and in the field.

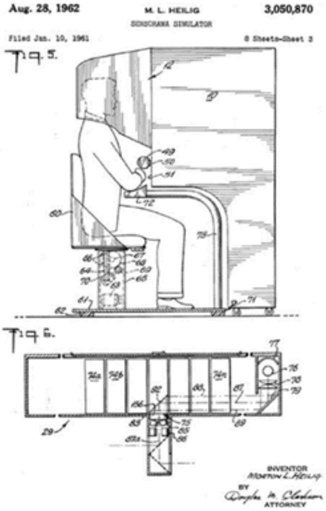
Virtual Reality

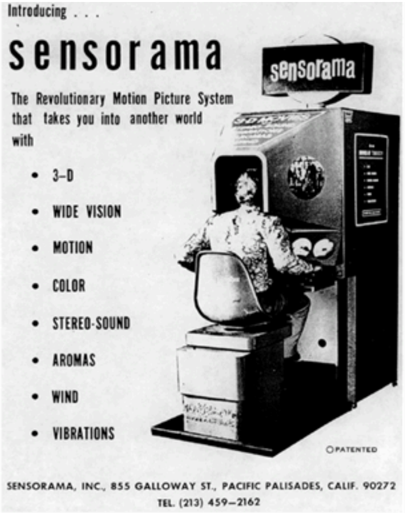
Much of the virtual reality technologies found in today's ecosystems are built on ideas that date back as early as the 1800s. The first stereoscope, using twin mirrors to project a single image, was invented in 1838, and that concept eventually morphed into the View-Master toy, which was patented in 1939 and is still in production. The next big technological leap in immersive systems came from Morton Heilig, who is often regarded as the father of VR (Gackenbach, 2017). Heilig had the vision to create a multisensory theater experience that would be more immersive than anything people had previously experienced. His Sensorama simulator (Figure 9-1) was a fully immersive, multisensory theater experience that encompassed 3-D images, stereo sound, wind, smells, and vibrations.

In order to make the Sensorama simulator more immersive, Heilig invented a

side-by-side dual film 3-D camera and projector. He made five films dedicated to the Sensorama, which included a motorcycle ride through New York City, a bicycle ride, a ride of a dune buggy, a helicopter ride over Century City, and a dance by a belly dancer (Carlson, 2017). The experience of the motorcycle ride through New York included a seat that would vibrate as a motorbike would, air that would rush through the user's hair, and smells of the road and a passing bistro (Gackenbach, 2017).

Figure 9-1 The Sensoroma





Introducing . . .

sensorama

The Revolutionary Motion Picture System that takes you into another world with

- 3-D
- WIDE VISION
- MOTION
- COLOR
- STEREO-SOUND
- AROMAS
- WIND
- VIBRATIONS

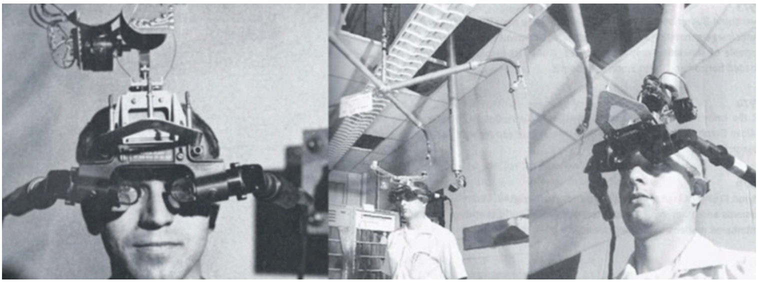
©PATENTED

SENSORAMA, INC., 855 GALLOWAY ST., PACIFIC PALISADES, CALIF. 90272
TEL. (213) 459–2162

Source: (Basso, 2017)

In 1965, another inventor named Ivan Sutherland created a head-mounted device that Sutherland marketed as a window into a virtual world. Sutherland's device was the first head-mounted display to incorporate computer technology to mediate a VR system (Gackenbach, 2017). Sutherland's system became known as the "Sword of Damocles" (Figure 9-2). The name arises from the Greek story of Damocles, in which a sword was suspended in the air by a hair, directly above the King's head—and at any moment, the hair could break, killing the King (Skurzynski, 1994). Similarly, Sutherland's contraption consisted of a height-adjustable pole attached to the ceiling. The system used this design setup due to the extreme weight of the headgear.

Figure 9-2 The Sword of Damocles



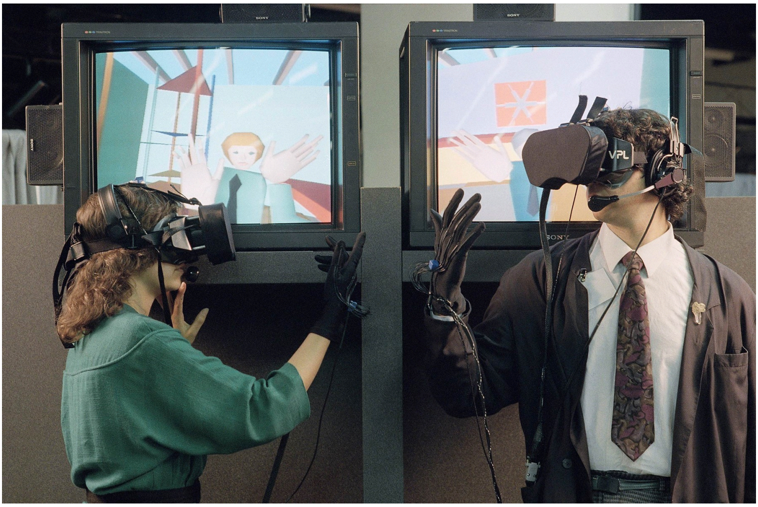
Source: (Van Krevelen, 2010)

This was the first time that computers were used to display a real-world environment whose elements were augmented by a computer (Adams, 2014). The headgear itself was made of cathode ray tube monitors, a mechanical tracking system, an ultrasonic tracking system, eyeglass display optics, and many computer programs and algorithms. Sutherland's system was able to project a transparent, 3-D wireframe cube onto the semitransparent optic lenses to create the illusion that the cube was floating in the room (Sunderland, 1968). The graphics were primitive—however, the 3-D cube would move and tilt, corresponding to the observer's head movements.

The term "virtual reality" was first used in the 1980s when Jaron Lanier started to design and develop goggles and gloves needed to experience what he called "virtual reality." Visual Programming Languages (VPL) was one of the first companies to design, develop, and sell VR products to consumers. VPL developed the DataGlove, the EyePhone, and AudioSphere

(Figure 9-3). These devices, when used together, created an immersive experience. The DataGlove used fiber optic cables attached to the back of the glove, which immitted tiny light beams as the user bent and moved their hand. Then, a computer interpreted the light beams and would generate an image on a small screen inside the EyePhone helmet. There were two drawbacks that limited the success of Lanier's systems: it was too expensive for the average consumer, and it was a one-size-fits-all glove (Burdea, 2003). Additionally, the DataGlove lacked tactile feedback, which reduced any sense of presence and was inconsistent with expectations of reality.

Figure 9-3 The VPL DataGlove and EyePhone



Source: (Sorene, 2014)

The 1970s and 1980s were an exciting time in the field of virtual reality. Advances in optical technology ran parallel to projects that worked on haptic devices and devices that would allow users to move around in virtual space. At NASA's Ames Research Center in the mid-1980s, the Virtual Interface Environment Workstation (VIEW) system (Figure 9-4) combined a head-mounted device with VPL's DataGloves to enable haptic interaction. The VIEW system used a head-mounted stereoscopic display system in which the display may be an artificial computer-generated environment, or a real environment relayed from remote video cameras (Rosson, 2022). can "step into" this environment and interact with it. For this project, NASA developed the DataSuit—a full-body garment equipped with sensors that increased the sphere of performance for virtual reality simulations by reporting to the computer the motions, bends, gestures, and spatial orientation of the user (Rosson, 2022).

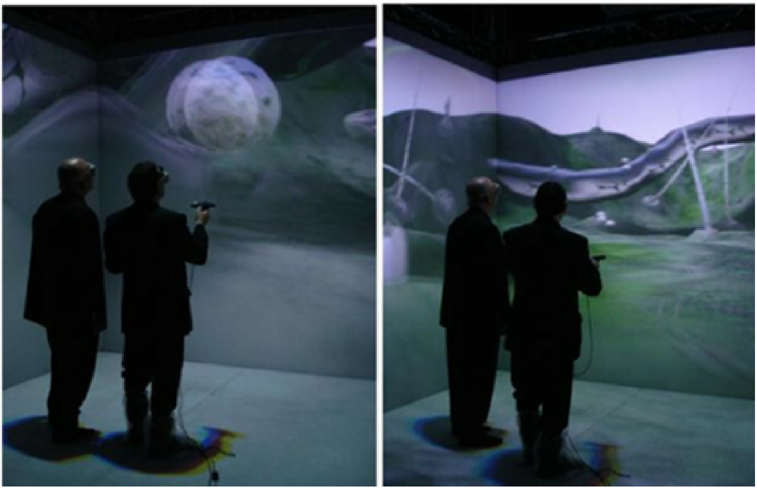
Figure 9-4 The NASA VIEW system

Source: (Rosson, 2022)

A large leap towards more interactivity in VR technology came in 2001 with the SAS cube—a computer-based cubic room (Figure 9-5). The SAS cube was nicknamed "The Cave," which was in reference to Plato's allegory of the cave, wherein he challenges human ideas of perception, reality, and illusion. The SAS cube room used projectors and sensors driven by PCs that react to people in the room. The advancements in PC graphics developed by the gaming industry meant that a cluster of relatively inexpensive PCs could be used instead of large supercomputers to yield the processing power required for effective vividity and interaction (Jacobson J. &., 2005) (Jacobson J. L.-L., 2005). The SAS cube system used rear projectors to cast stereoscopic images onto four screens, one of which was the floor. The continuous visual images synchronized across all screens produced a virtual landscape. Users wear 3-D glasses equipped with motion tracking sensors, which track

head movement (Fuchs, 2011). The stereoscopic images made the environment look 3-D, and sensors let users interact with objects and navigate the space (Robertson, 2001).

Figure 9-5 The SAS Cube System



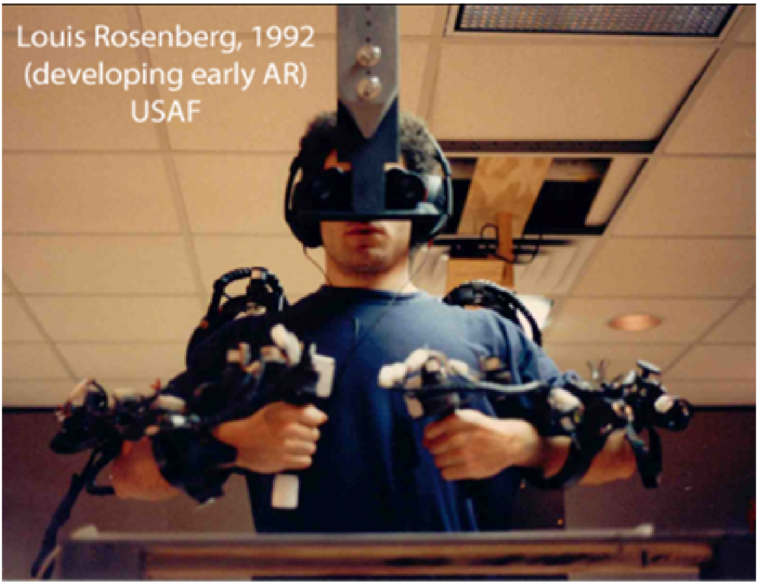
Source: (Jacobson J. &., 2005)

Augmented and Mixed Reality

Augmented reality systems differ from virtual reality in many conceptual and technical aspects. Augmented reality is accomplished through the human eye's view of the physical world in which various elements are enhanced by computer-generated input and digital artifacts. These inputs and artifacts can range from sound to video, graphics to GPS overlays, and more (The Interaction Design Foundation, 2021).

One of the first functional augmented reality systems was a robotic system designed and developed in 1992 at The United States Air Force Armstrong Research Lab by Louis Rosenberg. Rosenberg designed an AR system called Virtual Fixtures (Figure 9-6A & 9-6B), which was an incredibly complex robotic system designed to compensate for the lack of high-speed 3-D graphics processing power in the early 1990s (The Interaction Design Foundation, 2021). The system enabled the overlay of sensory information onto a workspace to improve user productivity.

Figure 9-6A The Virtual Fixtures Robotic System



Source: (Rosenberg, 2022)

Figure 9-6B The Virtual Fixtures Robotic System

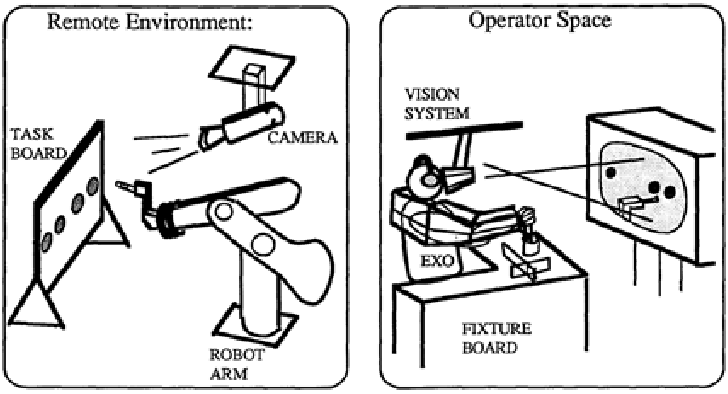


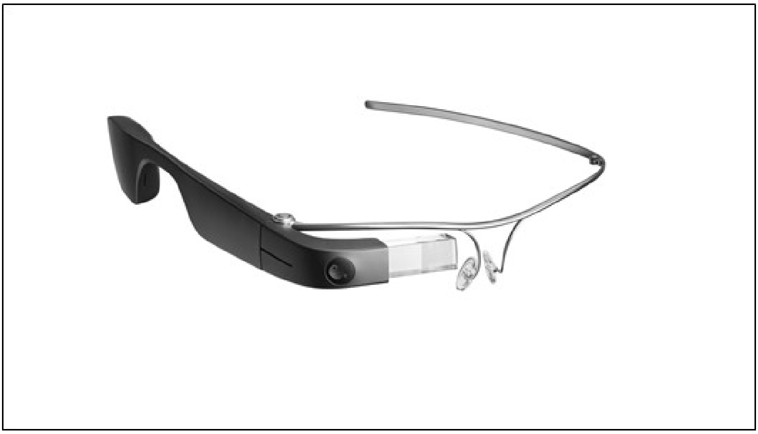
Figure 1: Experimental Setup for Telepresence Performace Assessment showing operator and workspace.

Source: (Rosenberg, 2022)

The first commercial AR application was introduced in 2008 by a German marketing agency in Munich. The agency designed a printed magazine ad for a model BMW Mini, which, when held in front of a computer's camera, also appeared on the screen. Through the connection of markers on the physical print ad and the virtual car model, users were able to control the car on the screen and move it around to view different angles simply by manipulating the piece of paper (Javornik, 2016). The application was one of the first marketing campaigns that allowed interaction with a digital model in real-time.

Google's Project Glass AR device (Figure 9-7) was presented to the public in 2012. Google Glass is an optical head-mounted display wearable device that is controlled with an integrated touch-sensitive sensor or with natural language voice commands. After Google made the public announcement for Google Glass, there was a surge of new AR research and an increase in the public perception of augmented reality technology (Arth, 2015). However, Google Glass was never quite successful in the consumer market. In January of 2015, Google announced that it would stop producing the Google Glass prototype. In July of 2017, Google announced the Google Glass Enterprise Edition and an updated version of the enterprise edition in 2019.

Figure 9-7 Google Glass AR Device

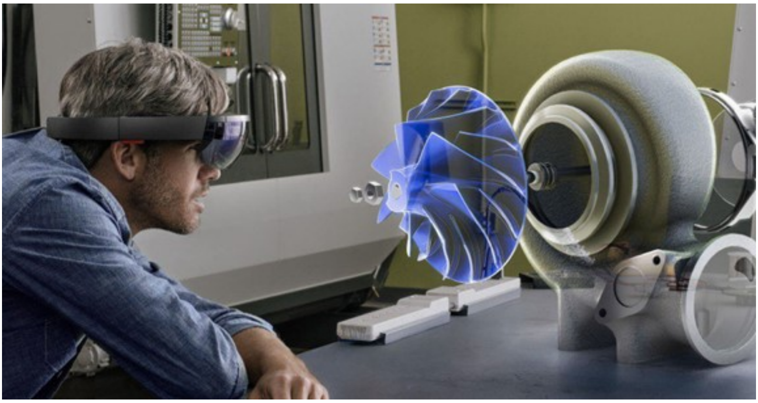


Source: (Statt, 2020)

In January of 2015, Microsoft announced the Hololens (Figure 9-8A). The Hololens is a headset that fuses AR and VR technologies. The device contains an integrated Windows computer system with a see-through display and multiple sensors. The Hololens is Microsoft's take on augmented reality, which they call mixed reality (Arth, 2015). Using multiple sensors, advanced optics, and holographic processing that melds seamlessly with its environment, the device generates holograms that can be used to display information, blend with the real world, or even simulate a virtual world. The Hololens has a plethora of optical sensors, with two on each side for peripheral environment understanding and sense, a main downward facing depth camera to pick up hand motions, and specialized speakers that simulate sound from anywhere in the room. The Hololens also has several microphones, an HD camera, an ambient light sensor, and

Microsoft's proprietary "Holographic Processing Unit" that has similar processing power as an average laptop. The device is capable of sensing the spatial orientation of the operator in relation to its position in the room, tracking walls and objects in the room, and blending holograms into the physical environment. The Microsoft Hololens 2 was released in 2019 and improved on the immersiveness, ergonomics, and connectivity of the original device.

Figure 9-8A Microsoft Hololens Device



Source: (Landyshev, 2019)

Basics of Dynamic Modeling in Virtual Environments

A virtual world is representative of an environment made up of objects, avatars, actuators, and other elements. In a general sense, we are dealing with dynamic environments where objects can move when touched. Forces and torques from various sources act on virtual objects. Simulating the dynamics of virtual environments is an

important part of an application, regardless of whether it is dynamics of rigid bodies, deformation dynamics, or dynamics of fluids (Mihelj, 2014). Inclusion of the relevant dynamic responses allows realistic behavior of the virtual environment to be achieved. A model of a body in a virtual environment must include a description of its dynamic behavior. This description also defines the body's physical interaction with other bodies in the environment. Body dynamics can be described based on various assumptions, which then determine the level of realism and the computational complexity of the simulation.

Interaction and Simulation in Complex Systems

Complex immersive systems require advanced levels of interaction within the virtual environment in order to maintain integrity. Mihelj et al. (2014) describe this level of interaction based on a computer-generated framework:

Interaction with a computer-generated environment requires the computer to respond to the user's actions. The mode of interaction with a computer is determined by the type of the user interface. Proper design of the user interface is of utmost importance since it must guarantee the most natural interaction possible. The concept of an ideal user interface uses interactions from the real environment as metaphors through which the user communicates with the virtual environment (p. 205).

The principal elements of interaction inside a virtual environment can be broken down into three main functionalities: manipulation, navigation, and communication. (Mihelj, 2014) note that "manipulation allows the user to modify the virtual environment and manipulate objects within it; navigation allows the user to move through the virtual environment; and communication occurs between different users or between users and digital intermediaries within the virtual environment" (p. 207). One of the advantages of operating in an immersive environment is the ability to interact with objects or manipulate objects in the environment (Mihelj, 2014). The ability to experiment in a new environment, real or virtual, enables the user to gain knowledge about the functioning of the environment. Some manipulation methods are shown in (Figure 9-8B).

Figure 9-8B Manipulation Methods

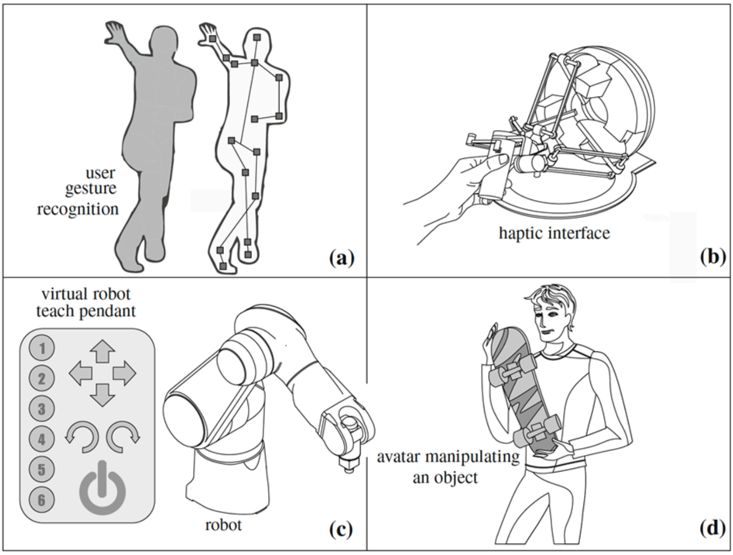


Fig. 9.1 Manipulation methods: **a** direct user control (gesture recognition), **b** physical control (buttons, switches, haptic robots), **c** virtual control (computer-simulated control devices) and **d** manipulation via intelligent virtual agents

Source: (Mihelj, 2014)

Navigation represents movement in space from one point to another. It includes two important components: (1) travel—how the user moves through space and time and (2) path planning —methods for determination and maintenance of awareness of position in space and time, as well as trajectory planning through space to the desired location (Mihelj, 2014). Moreover, simultaneous activity of multiple users in a virtual environment is a vital aspect of a VR framework. (Mihelj, 2014) offer a good description of how simultaneous activity can be achieved in a virtual environment:

Users' actions in virtual reality can be performed in different ways. If users work together in order to solve common problems, the interaction results in cooperation. However, users may also compete among themselves or interact in other ways. In an environment where many users operate at the same time, different issues need to be taken into account. It is necessary to specify how the interaction between persons will take place, who will have control over the manipulation or communication, how to maintain the integrity of the environment and how the users communicate. Communication is usually limited to visual and audio modalities. However, it can also be augmented with haptics (p. 210).

As technology advances, immersive systems become more complex, and their use requires many new skills. Engineers and designers are currently working on best-practice scenarios and frameworks to put in place, but many of the principals dealing with this complex environment are already in place. (Mihelj, 2014) explain this complexity in detail:

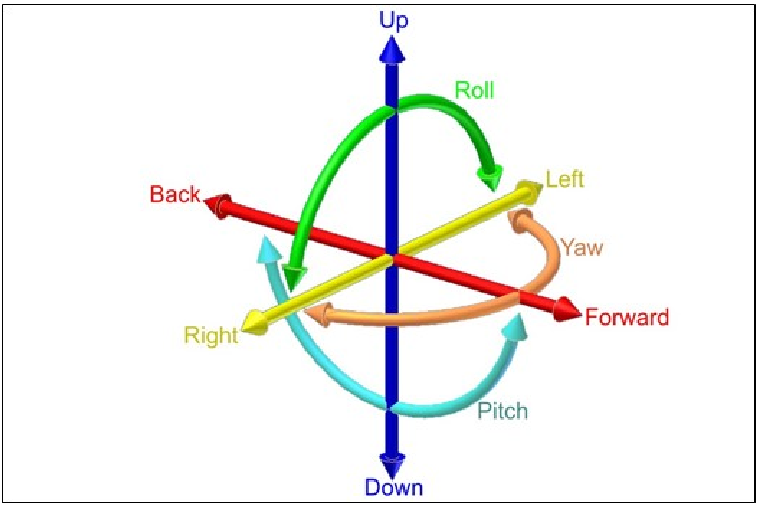
Extended reality is a medium that is suitable for training operators of such systems. Thus, it is possible to practice flying an aircraft, controlling a satellite, navigating a space vehicle, repairing an engine, and many other tasks in a virtual environment. Such environments are also important in the field of advanced robotics. Their advantage is not only that they enable simulation of a robotic cell but also behave as a real robot controller. This saves time required for programming since robot teaching is done in a simulation environment offline while the robot can still be used in a real environment in the meantime. At the same time, a virtual environment enables verification of software correctness before the program is finally transferred to the robot. Simulation-based programming may thus help avoid potential system malfunctions and consequent damage to the mechanism or robot cell (p. 217-219).

Degrees of Freedom in Immersive Simulation

Degrees of freedom (DoF) is a reference to the number of basic ways a rigid object can move through 3-D space. In total, there are six degrees of freedom. Three degrees correspond to rotational movement around the x, y, and z axes. These are commonly referenced as pitch, yaw, and roll. The other three degrees correspond to translational movement along the x, y, and z axes. These can be thought of in reference to how an object is moving forward or backward, moving left or right, and moving up or down.

Most VR and XR headsets and input devices are set up in 3DoF or 6DoF configurations. 3DoF means one can track rotational motion but not translational. In regard to the immersive environment, that means one can track whether the user has turned their head left or right, tilted it up or down, or pivoted left and right. 6DoF (Figure 9-9) means one can additionally track the translational motion in the immersive environment—whether the user has moved forward, backward, laterally, or vertically.

Figure 9-9 6Dof Illustration

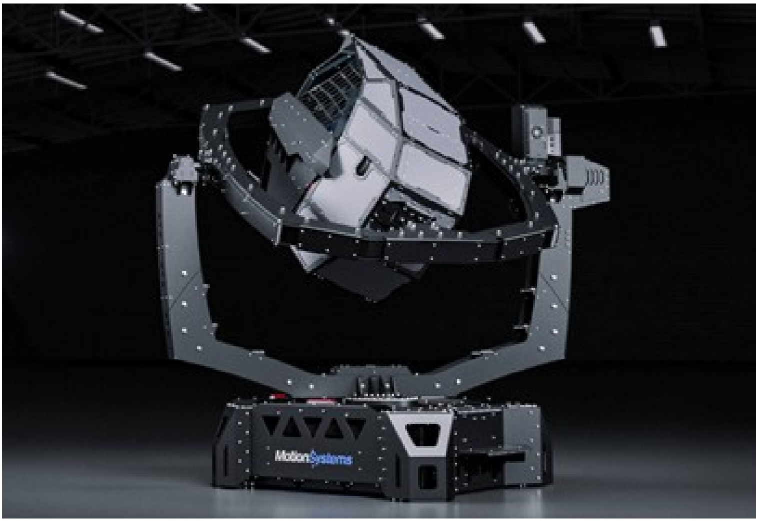


Source: ShareAlike 4.0 International (CC BY-SA 4.0))

Use of Motion Control Platforms

Cybersickness or Virtual Reality sickness are similar to Motion Sickness. The symptoms are almost identical in that users feel dizzy as if they were on a car trip or feel sick as if they were on a bumpy plane ride. The intensity of cybersickness depends on the VR technology that the headset is using. Symptoms often involve problems with presence and balance and eyes sending false perspectives as motion is displayed in the headset. Through the use of mechanical movement, motion control platform systems (Figure 9-10) provide the capability of staying immersed in longer virtual and extended reality simulation sessions without feeling nauseous. Motion control systems incorporate the principal physics of 3DoF or 6DoF to provide a minimization of mismatches between movement and graphics, which enhances disorientation for the user.

Figure 9-10 3DoF Motion Control Platform System



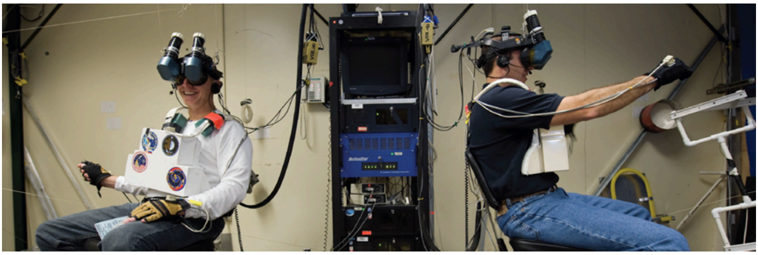
Source: (Motion Systems EU. , 2022)

AR and XR Uses Cases in Space Systems

In order for XR solutions to become a mainstream addition to the modern space systems workflow, they need to be efficient, immersive, and ergonomic. Hand and eye tracking solutions are ideal for making the XR experience feel more natural, but it is also important for the right hardware and software innovations to be implemented to ensure these features deliver the right results (Carter, 2022). For example, lightweight and untethered headsets with powerful displays will make it easier to engage in XR environments for longer periods of time. To improve the overall ergonomic experience, developers are researching eye-tracking technology to detect the visual needs of the user at any given time and adjust the rendering accordingly (Carter, 2022). Additionally, enhanced artificial intelligence solutions built into XR technology will aid in making the immersive experience feel more natural when it comes to using hand and eye tracking software. The right AI innovations will be able to track even the most minute finger movements and gestures, even when parts of a person's hand are hidden from direct view (Carter, 2022).

The current standard for human-system integration in space hardware development makes use of high-fidelity mockups to test operational scenarios and human interactions. This process is iterated at different scales and development stages, and it usually requires the use of great resources and implementation time (Netti, 2021). Immersive technologies can help mitigate this problem by minimizing the dependency on physical prototyping of assets and help condense the iterative evaluation/implementation process optimizing the transition from CAD modeling to human-in-the-loop testing. NASA is currently using XR simulation technology to test a Multi-Mission Extra Vehicular Robot (MMEVR) that is designed to be a collaborative/autonomous robot for EVA operations. The MMEVR human-system integration experiment (Figure 9-11) is to explore the robot collaboration capabilities in regular spacecraft maintenance scenarios and to understand how the hardware performance is affected by the human component and, conversely, how the human capabilities in space are affected by the hardware component (Netti, 2021).

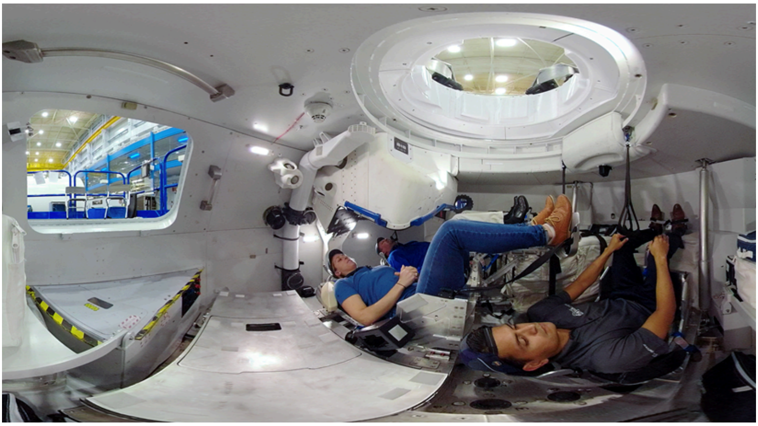
Figure 9-11 MMEVR Testing Environment



Source: (Netti, 2021))

Crewed space mission requires astronauts to practice and simulate every detailed step of the flight mission thousands of time. Although launching a spacecraft from zero to orbit takes only 12 minutes, it requires years of preparation and hundreds of hours of complex training simulations (varjo.com, 2022). For the mission to be successful, everything needs to go flawlessly. The Boeing Starliner flight-test crew in Houston has implemented a new and innovative way to train for this space system. The crew is using the Varjo XR3 extended reality system (Figure 9-12). The XR3 system allows astronauts to train remotely from anywhere in the world with the same level of realism and interactions as in a physical simulator. The system uses industry-leading visual quality to ensure virtual instruments in the spacecraft can be read and operated accurately. This type of immersive simulation experience can be used to train for any procedure. Additionally, it unlocks the ability to train in pre-launch quarantine in crew quarters, which was previously impossible.

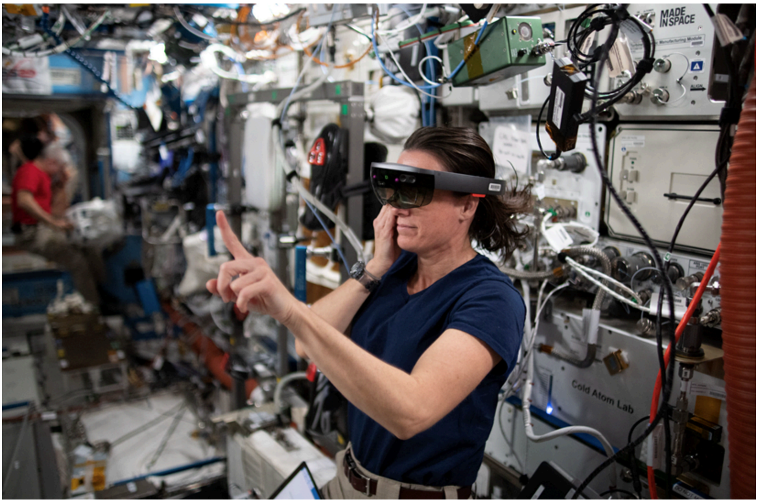
Figure 9-12 Boeing Starliner Varjo XR3 Testing



Source: (nbcnews, 2018)

NASA is also using augmented reality technology to explore various applications that can be used to assist astronauts aboard the International Space Station. (Experiment details, 2022) The T2 Augmented Reality (T2AR) project (Figure 9-13) demonstrates how station crew members can inspect and maintain scientific and exercise equipment critical to maintaining crew health and achieving research goals without assistance from ground teams (Guzman, 2021). The project demonstration used 3-D directional cues to direct the astronaut's gaze to specific work sites and displayed procedure instructions. The device followed an astronaut's verbal instructions to navigate procedures and displayed AR cues and procedure text over the hardware as appropriate for the procedure step being performed (Guzman, 2021). The system also provided supplemental information, such as instructional videos and system overlays, to assist in performing the procedure.

Figure 9-13 NASA T2AR Project Demonstration



Source: (NASA, 2021)

Future Thinking in Immersive Systems Technology

The future of immersive systems technology is exciting and yet full of unknowns. Engineers and designers are just beginning to harness the full potential of new technological advancements. Intelligent systems, machine learning, advanced micro processing, and advanced optics will provide the platforms for new immersive systems to emerge. These XR and AR technologies will eventually merge and integrate more seamlessly with the human body—which is ideal for complex space systems. One way is through AR contact lenses. While it's true that AR glasses will get better, cheaper, and more comfortable, in the future, they may also become obsolete as AR lenses take over. Such lenses are already in development.

The Mojo AR contact lens prototype (Figure 9-14) is a huge step forward for advanced immersive technology. The new Mojo Lens prototype accelerates the development of invisible computing, the next-generation computing experience where information is available and presented only when needed (Mojo, 2022). This type of AR experience allows users to access timely information quickly and discreetly without having to look down at a screen or lose focus on the people and physical world around them.

Figure 9-14 Mojo Advanced AR Contact Lens

Source: (Mojo, 2022)

The power of XR and AR technology is grounded in the ability to turn information into experiences, which can make many aspects of one's life richer and more fulfilling. For businesses, XR offers huge scope to drive business success, whether that means engaging more deeply with customers, creating immersive training solutions, streamlining business processes such as manufacturing and maintenance, or generally offering customers innovative solutions to their problems. In the end, the potential benefits of XR and AR far outweigh the challenges.

References

Adams, R. &. (2014). Augmenting virtual reality. *Military Technology*, pp. 38(12), 16–24.

Arth, C. G. (2015). The history of mobile augmented reality. *arXiv preprint*, p. arXiv:1505.01319.

Basso, A. (2017). Advantages, critics and paradoxes of virtual reality applied to digital systems of architectural prefiguration, the phenomenon of virtual migration. *Proceedings of the International and Interdisciplinary Conference IMMAGINI.* Brixen, I: Conference IMMAGINI. doi:Basso, A. (2017). Advantages, critics and paradoxes of virtual reality applied to digital systems of architectural prefiguration, the phenomenon of virtual migration. Proceedings of the International and Interdisciplinary Conference IMMAGINI, Brixen, I

Buis, A. (2021, August 3). *Earth's Magnetosphere: Protecting Our Planet from Harmful Space Energy*. Retrieved August 12, 2022, from NASA Global Climate Change: https://climate.nasa.gov/news/3105/earths-magnetosphere-protecting-our-planet-from-harmful-space-energy/

Burdea, G. C. (2003). *Virtual reality technology (Vol. 1).* Hoboken, NJ: John Wiley & Sons.

Carlson. (2017). *history/lesson17.html.* Retrieved from design.osu.edu: https://design.osu.edu/carlson/history/lesson17.html

Carter, R. (2022). The hottest trends in XR hand and eye tracking for 2022. *XR Today*. Retrieved from https://www.xrtoday.com/mixed-reality/the-hottest-trends-in-xr-hand-and-eye-tracking-for-2022

Experiment details. (2022, Aug 21). Retrieved from www.nasa.gov/: https://www.nasa.gov/mission_pages/station/research/experiments/explorer/Investi gation.html#id=7587

Fuchs, P. M. (2011). *Virtual interfaces. Virtual reality: Concepts and technologies.* CRC Press.

Gackenbach, J. B. (2017). Looking for the Ultimate Display: A Brief History of Virtual Reality. In Boundaries of self and reality online: Implications of digitally constructed realities . *Academic Press Essay*, pp. 239–259.

Group on Earth Observations. (n.d.). *About Us*. Retrieved August 8, 2022, from Group on Earth Observations: https://www.earthobservations.org/geo_community.php

Guzman, A. (2021, Aug 21). *New augmented reality applications assist astronaut repairs to space. NASA.* Retrieved from www.nasa.gov: https://www.nasa.gov/mission_pages/station/research/news/augmented-reality-applications-assist-astronauts

Holzinger, M. J., Chow, C. C., & Garretson, P. (2021, May 3). *AFRL Portal*. Retrieved August 7, 2022, from A Primer on Cislunar Space: https://www.afrl.af.mil/Portals/90/Documents/RV/A%20Primer%20on%20Cislunar%20Space_Dist%20A_PA2021-1271.pdf?ver=vs6e0sE4PuJ51QC-15DEfg%3D%3D

Howell, E. (2017, August 21). *Lagrange Points: Parking*

Places in Space. Retrieved August 7, 2022, from Space.com: https://www.space.com/30302-lagrange-points.html

Hudson, K. E. (1990). *Communications Satellites: Their Development and Impact.* New York, NY: Macmillan Inc.

Indian Space Research Organization. (n.d.). *Earth Observation Applications*. Retrieved August 8, 2022, from Indian Space Research Organization: https://www.isro.gov.in/earth-observation/applications

Jacobson, J. &. (2005). Game engine virtual reality with CaveUT. *Compute*, pp. 38(4), 79–82.

Jacobson, J. L.-L. (2005). *Proceedings of the 2005 ACM SIGCHI International Conference on Advances in Computer Entertainment Technology – ACE '05* (pp. Jacobson, J., Le Renard, M., Lugrin, J.-L., & Cavazza, M. (2005). The CaveUT system. Proceedings of the 2005 ACM SIGCHI International Conference on Advances in Computer Entertainment Technology – ACE '05. https://doi.org/10.1145/1178477.1178503). ACE. doi:https://doi.org/10.1145/1178477.1178503

Javornik, A. (2016, Oct 4). *The mainstreaming of augmented reality: A brief history. Harvard Business Review.* Retrieved from hbr.org: https://hbr.org/2016/10/the-mainstreaming-of-augmented-reality-a-brief-history

Jones, A. (2022, July 1). *China launches new Gaofen 12 Earth observation satellite*. Retrieved August 8, 2022, from Space.com: https://www.space.com/china-launches-gaofen-12-satellite

JPL. (2001, November 3). *Joint Propulsion Lab*. Retrieved August 9, 2022, from Seals, Sea Lions and Satellites: https://www.jpl.nasa.gov/news/seals-sea-lions-and-satellites

Landyshev. (2019). *mixed-reality-microsoft-hololens-headset-business/.* Retrieved from www.visartech.com/: https://www.visartech.com/blog/mixed-reality- microsoft-hololens-headset-business/

Mihelj, M. N. (2014). *Virtual Reality Technology and applications* . London: Springer.

Mojo. (2022, March 30). *we-have-reached-a-significant-milestone.* Retrieved from www.mojo.vision/: https://www.mojo.vision/news/we-have-reached-a-significant-milestone-blog

Motion Systems EU. . (2022, May 30). product/simulators/ ps-3rot-150-v2/. *Motion Systems EU.* Retrieved from https://motionsystems.eu/product/simulators/ ps-3rot-150-v2/

NASA. (2010, November 9). *Global View of Fine Aerosol Particles*. Retrieved August 12, 2022, from NASA Earth Observatory: https://earthobservatory.nasa.gov/images/ 46823/global-view-of-fine-aerosol-particles

NASA. (2010, September 22). *New Map Offers a Global View of Health-Sapping Air Pollution*. Retrieved August 12, 2022, from NASA Earth Observatory: https://www.nasa.gov/ topics/earth/features/health-sapping.html

NASA. (2010, April 1). *TIROS, the Nation's First Weather Satellite*. Retrieved August 6, 2022, from NASA History:

https://www.nasa.gov/multimedia/imagegallery/image_feature_1627.html

NASA. (2012, April 9). *NASA Views Our Perpetual Ocean*. Retrieved August 9, 2022, from NASA: https://www.nasa.gov/topics/earth/features/perpetual-ocean.html

NASA. (2016, September 16). *Sea Ice*. Retrieved August 9, 2022, from NASA Earth Observatory: https://earthobservatory.nasa.gov/features/SeaIce/page1.php

NASA. (2017, October 26). *A River of Rain Connecting Asia and North America*. Retrieved August 12, 2022, from NASA Earth Observatory: https://earthobservatory.nasa.gov/images/91175/a-river-of-rain-connecting-asia-and-north-america

NASA. (2021, June 23). *Earth Observing System Project Science Office*. Retrieved August 8, 2022, from NASA: https://eospso.nasa.gov/content/nasas-earth-observing-system-project-science-office

NASA. (2021, April 15). *NASA-Built Instrument Will Help to Spot Greenhouse Gas Super-Emitters*. Retrieved August 12, 2022, from NASA: https://www.nasa.gov/feature/jpl/nasa-built-instrument-will-help-to-spot-greenhouse-gas-super-emitters

NASA. (2021, August 25). *Protecting the Ozone Layer Also Protects Earth's Ability to Sequester Carbon*. Retrieved August 12, 2022, from NASA: https://www.nasa.gov/feature/

goddard/esnt/2021/protecting-the-ozone-layer-also-protects-earth-s-ability-to-sequester-carbon

NASA. (2021, October). *Satellites View California Oil Spill*. Retrieved August 9, 2022, from NASA Earth Observatory: https://earthobservatory.nasa.gov/images/148929/satellites-view-california-oil-spill

NASA. (2022, July 22). *50 Years of Landsat*. Retrieved August 6, 2022, from NASA History: https://www.nasa.gov/image-feature/50-years-of-landsat

NASA. (2022). *Aqua Earth-observing Satellite Mission*. Retrieved August 8, 2022, from NASA Earth Observing Systems: https://aqua.nasa.gov

NASA. (2022). *NASA Covers Wildfires Using Many Sources*. Retrieved August 12, 2022, from NASA Earth Observatory: https://www.nasa.gov/mission_pages/fires/main/missions/index.html

NASA. (2022). *Ozone Monitoring Instrument (OMI)*. Retrieved August 12, 2022, from NASA Aura: https://aura.gsfc.nasa.gov/omi.html

nbcnews. (2018, Sept 30). *360-video-inside-boeing-s-starliner-space-capsule.* Retrieved from www.nbcnews.com/: https://www.nbcnews.com/mach/science/360-video-inside-boeing-s-starliner-space-capsule-ncna914856

Netti, V. G. (2021). A Framework for use of immersive technologies for human-system integration testing of space hardware. *2021 ACM CHI Virtual Conference on Human Factors in Computing Systems* (pp. Netti, V., Guzman, L., &

Rajkumar, A. (2021). A Framework for use of immersive technologies for human-system integration testing of space hardware). Yokoha: ACM.

NOAA. (2011, August 1). *Ocean Currents*. Retrieved August 9, 2022, from National Oceanic and Atmospheric Administration (NOAA): https://www.noaa.gov/education/resource-collections/ocean-coasts/ocean-currents

Pacific Marine Mammal Center. (2019, January 2). *Satellite Tracking*. Retrieved August 12, 2022, from Pacific Marine Mammal Center: https://www.pacificmmc.org/satellite-tracking

Parker, J. S., & Anderson, R. L. (2013, July). *Transfers to Low Lunar Orbits*. Retrieved August 7, 2022, from JPL DESCANSO Book Series: https://descanso.jpl.nasa.gov/monograph/series12/LunarTraj–05Chapter4TransferstoLowLunarOrbits.pdf

Patel, K. (2019, March 1). *5 Stories from 5 Years of Precipitation Measurements from Space*. Retrieved August 9, 2022, from NASA Earth Observatory: https://earthobservatory.nasa.gov/blogs/earthmatters/2019/03/01/5-stories-from-5-years-of-precipitation-measurements-from-space/

Preston, S. (2022, April 26). *Monitoring River Flushing And Hydropower From Space*. Retrieved 2022, from Planet Pulse: https://www.planet.com/pulse/monitoring-river-flushing-and-hydropower-from-space/

Robertson, R. (2001, Nov 11). *CGW/2001/*

Volume-24-Issue-11-November-2001-/immersed-in-art.aspx. Retrieved from www.cgw.com: http://www.cgw.com/Publications/CGW/2001/Volume-24-Issue-11-November-2001-/immersed-in-art.aspx.

Rosenberg, L. (2022, May 19). *How a parachute accident helped jump-start augmented reality. IEEE Spectrum.* Retrieved from spectrum.ieee.org: https://spectrum.ieee.org/history-of-augmented-reality

Rosson, L. (2022, Aug 21). *The Virtual Interface Environment Workstation (VIEW), 1990. NASA.* Retrieved from www.nasa.gov/ames/: https://www.nasa.gov/ames/spinoff/new_continent_of_ideas

Skurzynski, G. (1994). Virtual reality. Cricket. *Cricket*, pp. 21(11), 42–46.

Sorene, P. (2014, Nov 24). *Jaron Lanier's eyephone: Head and glove virtual reality in the 1980s. Flashbak.* . Retrieved from flashbak.com: https://flashbak.com/jaron-laniers-eyephone-head-and-glove-virtual-reality-in-the-1980s-26180/

Statt. (2020, Feb 4). *Google opens its latest Google Glass AR headset for direct purchase.* Retrieved from www.theverge.com: https://www.theverge.com/2020/2/4/21121472/google-glass-2-enterprise-edition-for-sale-directly-online

Sunderland, I. (1968). *Carlson/history/PDFs.* Retrieved from design.osu.edu/: http://design.osu.edu/carlson/history/PDFs/p757-sutherland.pdf.

Temming, M. (2021, January 21). *Space Station Detectors Found the Source of Weird 'Blue Jet' Lightning*. Retrieved

August 12, 2022, from Science News: https://www.sciencenews.org/article/space-station-detectors-found-source-weird-blue-jet-lightning

The Interaction Design Foundation. (2021). *augmented-reality-the-past-the-present-and-the-future.* Retrieved from www.interaction-design.org/: https://www.interaction-design.org/literature/article/augmented-reality-the-past-the-present-and-the-future

The Space Option. (2012, October 1). *Cislunar Space*. Retrieved August 7, 2022, from The Space Option: https://thespaceoption.com/portfolio/cislunar-space/

Van Krevelen, D. W. (2010). A survey of Augmented Reality Technologies, applications and limitations. *International Journal of Virtual Reality*, pp. 9(2), 1–20. Retrieved from https://doi.org/10.20870/ijvr.2010.9.2.2767

varjo.com. (2022, Aug 21). *Varjo & Boeing: A new era in astronaut training using virtual reality.* Retrieved from varjo.com: https://varjo.com/boeing-Starliner/

World Health Organization. (2022). *Air Pollution*. Retrieved August 12, 2022, from WHO Health Topics: https://www.who.int/health-topics/air-pollution#tab=tab_1

World Meteorological Organization. (2022, February 1). *WMO certifies two megaflash lightning records*. Retrieved August 12, 2022, from World Meteorological Organization: https://public.wmo.int/en/media/press-release/wmo-certifies-two-megaflash-lightning-records

PART III

SECTION 3: HUMANITARIAN USE OF SPACE TECHNOLOGIES

10.

DRONES AND PRECISION AGRICULTURAL MAPPING (MUMM)

Student Learning Objectives

The student will gain knowledge of the concepts and framework related to the current and future uses of space assets and autonomous systems in the agriculture industry.

A Look Back at the Traditional Agriculture Monitoring Systems

Since the early days of humankind's need to grow and harvest food from the earth, the value of information on crop yields, water supplies, seed stores, weather, and other data is key to the success of output for the next growing season. Currently, satellite and remote sensing data is collected and analyzed as it is used worldwide by the "agricultural industry to make decisions, understand changes, and estimate future conditions. Like forecasting commodity price data, researchers and industry professionals use these spatial data to forecast changes to conditions under different management strategies, climate scenarios, and market pressures" (Farmtogether, 2022).

The first agricultural revolution occurred in approximately 10,000 B.C. as humans shifted from being hunter-gathers to subsistence farmers and herders. The second agricultural revolution started about 300 years ago, which ushered in new agrarian techniques, including selectively breeding livestock and crop rotation systems. The third agricultural revolution boosted crop yield and improved plant technologies throughout the 1940s, 50s, and 60s (Epplett, 2021).

The Industrial Revolution was the catalyst for farmers shifting from the small family farm yields to the industrial output of the modern farm. This shift was instrumental in allowing the sharing of all recorded data with farmers in other states and other countries. The days of small farming and handwritten journals are gone and replaced with data and trend analytics to increase farm production to meet the demands as the population shifts from rural farms to urban and city life. As a result, the world's population flourishes as "food is more accessible around the world, especially in wealthier, more developed places, due largely to effects of the Industrial Revolution and changes that have occurred in society" (Colby Community, 2018).

The importance of the agriculture industry is a hallmark of our current civilization as food security, nutrition, and availability are keys to a productive society. The "concern with ensuring social stability was evident with the creation of the League of Nations Health Organization, which was launched to combat epidemics in Eastern Europe, but eventually came to sponsor a nutrition program" (Colby Community, 2018).

The agricultural industry is undergoing rapid transformations as interconnected network sensor systems, automated equipment, data feeds, and in-depth scientific studies are taking food production into a technical revolution. However, this revolution is not without challenges as "technological innovation has resulted in substantive improvements in the availability, timeliness and overall quality of agricultural data, many technical and institutional challenges remain" (Carletto, 2021).

The agriculture industry is a linchpin to humankind on our planet and in outer space. The use of satellite data in the "agriculture sector is not new; organizations have been utilizing images from space to study land-use ever since the first satellite of NASA's Landsat program started beaming back pictures in 1972". (Measures, 2021)

The "difference between then and now is that the data we're generating can be integrated into all the additional innovations taking place on the farm" (Measures, 2021) with the combined use of space-based platforms, machine learning, and several forms of autonomous systems now offer humankind the most efficient and effective ways to make agricultural decisions since farming began.

Outer Space to the Subsoil

Satellites are commonplace today as the world consumes GPS data on thousands of different devices daily, and Starlink launches thousands of communication satellites every year. The "advantage with satellite images is it is near real-time data and can cover a large area in a short time…they also eliminate the need for costly manual data collection and the potential for human error". (Measures, 2021) Historically, crop yields were only as good as the individual family farmers' journal notated experiences and the Farmer's Almanac. Now with new technology, farmers are merging intuition and expertise with data from satellites to analyze and make decisions at the field level.

Satellite imagery is widely adopted in precision agriculture because of its cost-effectiveness and accuracy. Helping agronomists everywhere save time, resources, and money. Satellite data collects detailed information to predict crop yields, including NDVI. Earth observation (E.O.) data can measure details, such as soil moisture, to help farmers support crop health. (Increase Crop Yield With Precision Agriculture Technology, 2022)

As depicted in Figure 10-1, overhead imagery reduces the need for higher-cost ground sensors or hands-on physical testing. One advantage of using drone-collected data is that it can be easily integrated to provide multiple layers of information in just a few minutes.

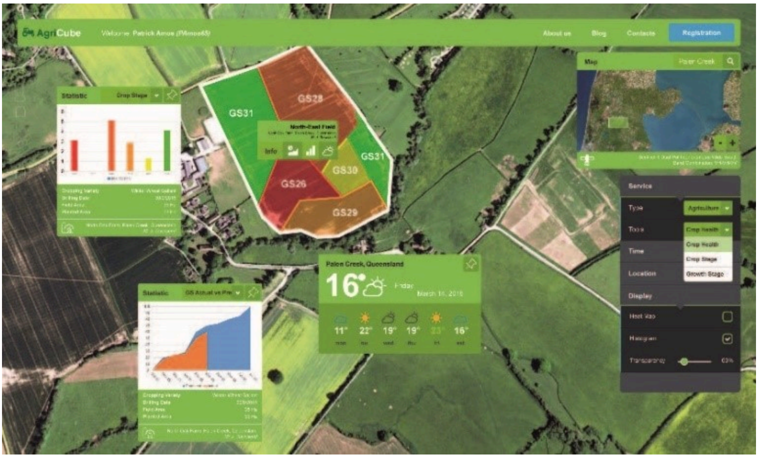
Figure 10-1 Autonomous crop data collection

www.cema-agri.org
European Agricultural Machinery
CEMA

Source: (CEMA, 2021)

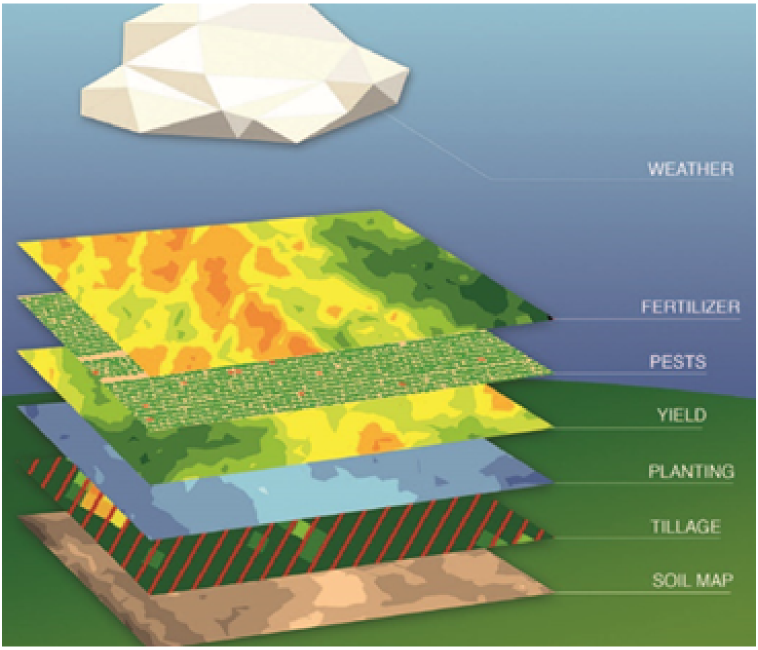
The Earth Observation Satellites (EOS) have been in orbit since the early 1970s. These satellites allow for multiple data layers to create soil maps, analyze acreage that has been tilled or planted, estimate yields, identify pests, and determine the nutrient content of fields. Farmers can now integrate all of this information with water tables, weather, and other data in a farm management software package to create precision agriculture far beyond the typical family farming in the past 100 years.

Figure 10-2 Example of integrated data layers accessible from a farm management system



Source: (Jarman, 2018)

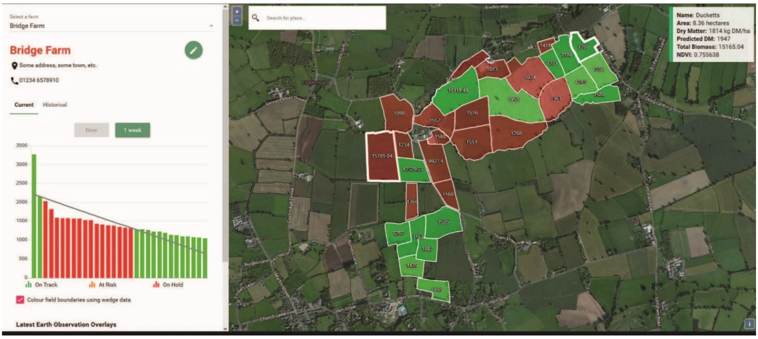
Figure 10-3 Example of the types of agrarian data layers stored and accessible from a farm management system



Source:(Jarman, 2018)

Figures 10-2 and 10-3 above are examples of "online farm management platform that exploits computer vision and crop modeling to integrate EOS, weather, and field data to automatically assess each field across the whole farm for grass biomass and grazing readiness" (Jarman, 2018). Not only can the system be used of for crops, but the data can also be used for livestock management. Using the data collected as shown in Figure 10-4, the "fields in green are shown to the farmer as being suitable for grazing, while those in red require further growth" (Jarman, 2018).

Figure 10-4 Farmers can use the drone-collected data to determine where livestock can best graze



Select a farm
Bridge Farm

Bridge Farm
Some address, some town, etc.
☎ 01234 6578910

Name: Ducketts
Area: 8.36 hectares
Dry Matter: 1814 kg DM/ha
Predicted DM: 1947
Total Biomass: 15165.04
NDVI: 0.755638

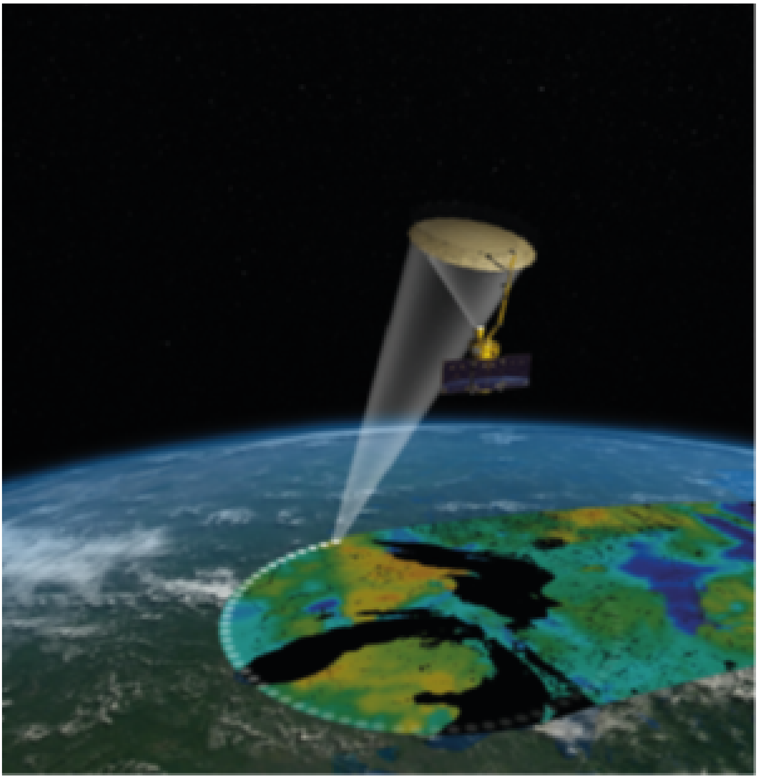
☑ Colour field boundaries using wedge data

Latest Earth Observation Overlays

Source: (Jarman, 2018)

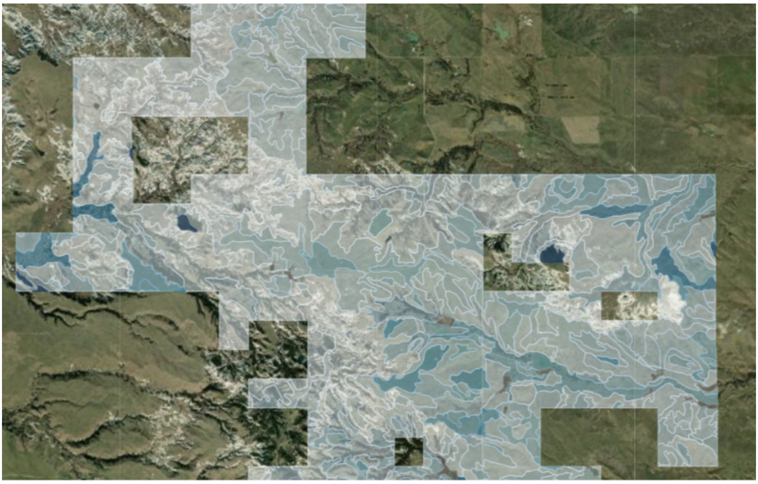
The Gridded Soil Survey Geographic Database (gSSURGO) is generally the most detailed level of soil geographic data developed by the National Cooperative Soil Survey (NCSS). See Figures 10-5 and 10-6. These databases are a compilation of "remote sensing soil data product(s) that now includes soil organic carbon estimates which can be applied to a farm or ranch to see most carbon-rich locations as shown in the map above where darker blue locations have high carbon stock estimates" (Farmtogether, 2022).

Figure 10-5 Rendering of NASA's Soil Moisture Active Passive (SMAP) satellite, collecting global soil moisture data. Image credit: NASA



Source: (Jarman, 2018)

Figure 10-6 Sample rendering of the USDA NRCS gSSURGO satellite gathering soil data

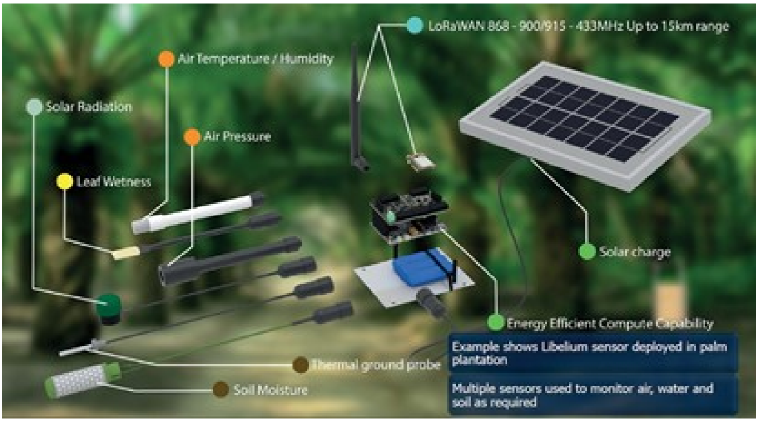


Source: (Farmtogether, 2022)

Integrated Autonomous Systems

The integrated nature of agriculture data lends itself well to the evolution of Internet of Things (IoT). An emerging topic in the IoT arena is in the "agriculture field and IoT-based precision agriculture. IoT applications can range from water spraying from drones, soil recommendation for different crops, weather prediction and recommendation for water supply, etc." (Roy, 2022) This emerging field is described as the Internet of Precision Agricultural Things (IopaT).

Figure 10-7 A diagram of a wireless sensor node. Image source: Inmarsat (2017).


LoRaWAN 868 - 900/915 - 433MHz Up to 15km range
Air Temperature / Humidity
Solar Radiation
Air Pressure
Leaf Wetness
Solar charge
Energy Efficient Compute Capability
Thermal ground probe
Soil Moisture

Example shows Libelium sensor deployed in palm plantation

Multiple sensors used to monitor air, water and soil as required

Source: (Jarman, 2018)

IoT devices linked to software and hardware tools allow for the rapid integration and digital data flow that informs agricultural machinery using the latest in-situ monitoring information and farming inputs – seedlings, irrigation water, fertilizers, and pesticides. See Figure 10-7. This information can inform autonomous equipment and be targeted with a square mile, providing accuracy to account for natural variability in growing conditions/crop production across a field.

Autonomous Ground Vehicles

Integrating space, drone, and IoT data allows for a plan to move forward with tilling, seeding, watering, weeding, and harvesting. Ideally, at this point, the farmer should introduce the next set of autonomous systems, which are autonomous ground vehicles.

An easily recognizable name in the farming equipment industry is the John Deere brand of Deere & Company, based in Moline, Illinois. John Deere revealed a fully autonomous tractor at the Consumer Electronics Show (CES) in January 2022 that would be available for sale later in the year. John Deere states, "The autonomous tractor serves a specific purpose: feeding the world. The global population is expected to grow from about 8 billion to nearly 10 billion people by 2050, increasing the global food demand by 50%" (John Deere, 2022).

John Deere's push for autonomous farm equipment comes at a critical time; "farmers must feed this growing population with less available land and skilled labor, and work through the variables inherent in farming like changing weather conditions and climate, variations in soil quality and the presence of weeds and pests" (John Deere, 2022).

Figure 10-8 John Deere autonomous tractor

Source: (John Deere, 2022)

The autonomous tractor (see Figure 10-8) can be networked and controlled via the John Deere Operations Center Mobile application, which

"provides access to live video, images, data, and metrics and allows a farmer to adjust speed, depth, and more. If any job quality anomalies or machine health issues occur, farmers will be notified remotely and can optimize the machine's performance". (John Deere, 2022) Deere & Company recognizes that IoT must also be secure. The Company has taken an active role in posturing its systems for cybersecurity, stating:

"We have made cybersecurity a critical component of our new machines. We have added protective features to our hardware and software and updated how new vehicles are engineered… every step of the development process and continuously evolving cybersecurity processes and solutions to minimize vulnerability to cyber-attack”. (John Deere, 2022)

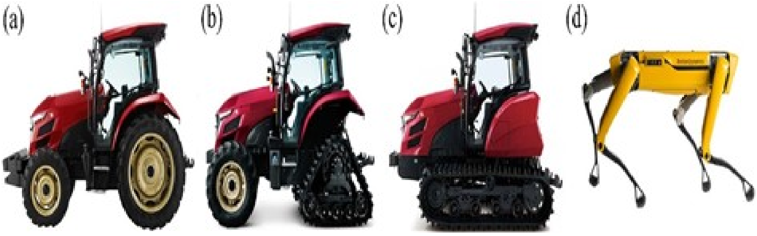
Tractors are not the only farm equipment that is being automated; several other machines are being introduced, as indicated in Table 10-1.

Different platforms used in autonomous agricultural vehicle

Table 10-1 Autonomous agricultural vehicles and capabilities (Roshanianfard, 2020)**.**

Types of Platforms	Varieties	Applications as Autonomous Vehicles
Tractor	Row crop tractors, general purpose tractors, tracklayers. Two-wheel tractors	Pulling/pushing different machines (agricultural machinery, tanks, vehicles, or trailers). The pre-planting process includes plowing, tilling, disking, harrowing, planting, weeding, watering, fertilizing, harvesting, winnowing, and threshing.
Combine harvester	Wheel type (self-propelled), trawler type, (track), tractor mounted	Harvesting, winnowing, and threshing
Utility vehicle	Utility vehicles (UTV), all-terrain vehicles (ATV)	Transporting, plowing (field, snow), raking, harrowing, mowing grass, building fences, spreading seeds, catching calves, carrying firewood
Transplanter	Rice transplanter, vegetable transplanter, flower transplanter	Transplanting seedlings
Boats	Motorboat, airboat	Fertilizing, weeding

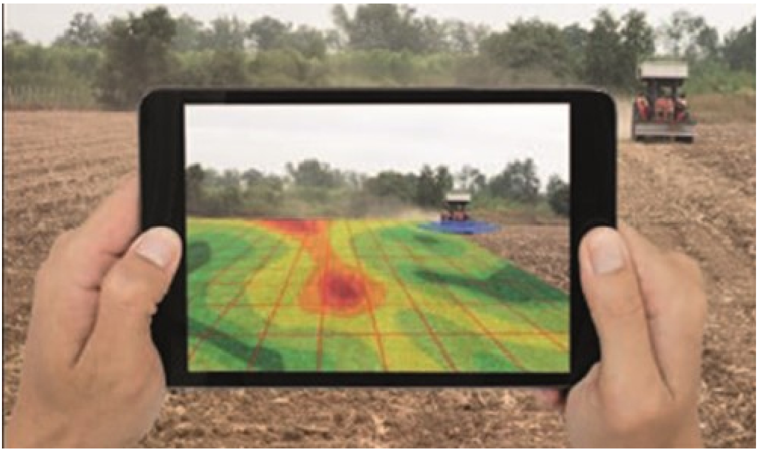
Figure 10-9 Transporter system types, (a) wheel-type, (b) half-crawler, (c) crawler-type (YANMAR, 2022), and robotic leg (YANMAR, 2022)



Source: (Roshanianfard, 2020)

The farmer can integrate these autonomous systems into an augmented reality that allows the farmer to "see" the data to gain a greater understanding, as depicted in Figure 10-10.

Figure 10-10 An example of augmented-reality farming solutions displayed on a regular handheld device



Source: (Jarman, 2018)

Automated Weeders and Crop Eradication for Food Crops

Crop eradication can take several forms and reasonings. Primarily, weeds rob crops of valuable nutrients and water, reducing crop yield. The weeds can be eliminated by sprayer drones that are "already being deployed for agricultural applications, and their load limitations are offset by their ability to make precise spot applications... Other technologies in development include precision flamers, lasers, abraders, or cultivators who can replace or augment herbicides" (Finkelnburg, 2021). See Figure 10-11 as an example.

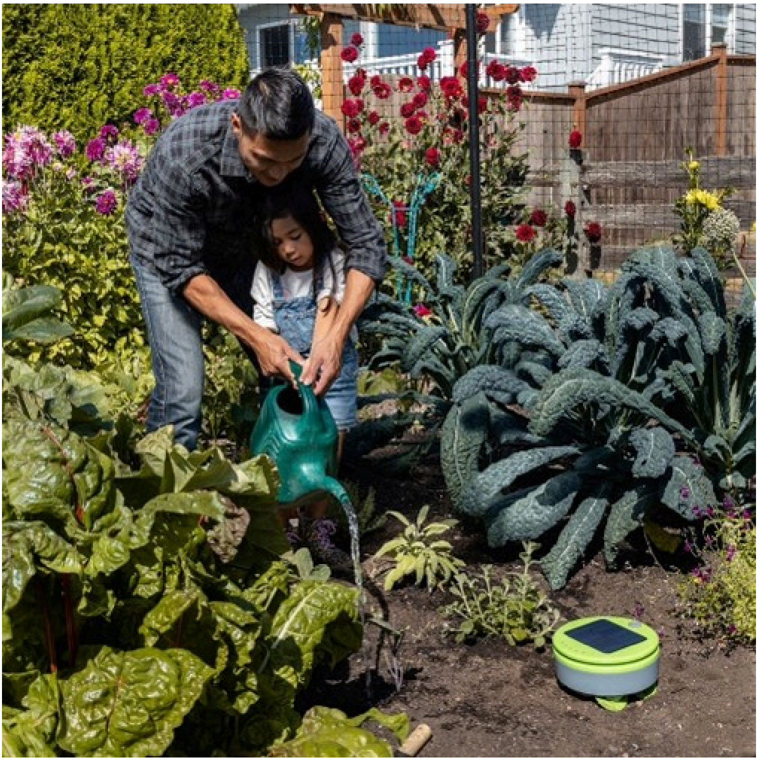
Figure 10-11 The Future of Weed Control-Drone Precision Spraying

Source: (Finkelnburg, 2021)

Weed control allows for precision application of herbicides, while crop dusters and other manual efforts are "… believed to be one of the least efficient agricultural activities. Precision A.I. estimates that more than 80% of herbicides end up wasted on bare ground, while another 15% of the harmful chemicals fall on the crops" (Singh, 2021). The Company is developing drones that use a combination of A.I. and computer vision to spray only the problem areas and avoid unimpacted crops. Precision A.I. believes that by targeting specific areas that need herbicides can reduce costs by as much as $52 U.S. dollars per acre. (Singh, 2021).

The weed control gardening assistance of autonomous systems spans from large industrial farms to small backyard gardens. Tertill is the inventor of Roomba, the long-standing and very successful automated home vacuum cleaner. Tertill can assist small farmers in helping "grow delicious organic vegetables – without all the weeding. Enjoy taking care of your plants – let Tertill take care of the weeds...Proven as effective as hand weeding by the Cornell School of Agriculture" (Tertill, 2022). See the Tertill in Figure 10-12.

Figure 10-12 Image of the Tertill automated weeder in a backyard garden



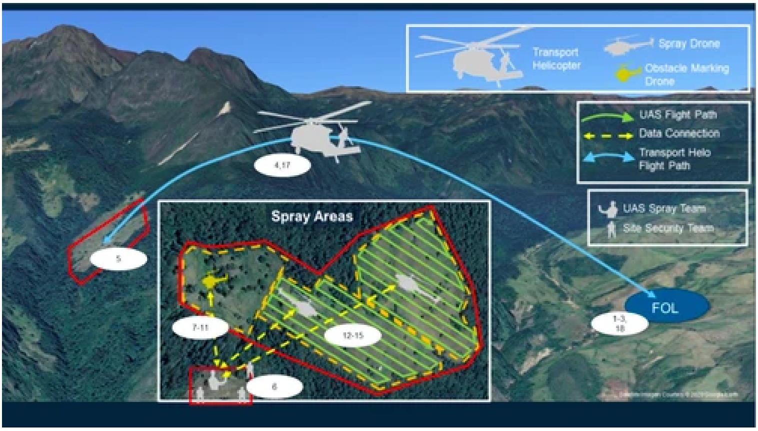
Source: (Tertill, 2022)

Crop Eradication for Illegal Crops

Illicit drug crops also need to be eradicated, yet the requirements can take on very different aspects in the data collection and the employment of autonomous systems.

In dealing with illegal crops such as illicit drugs, remote sensing using satellites and drones are effective in surveying and gathering data for law enforcement use. Reports indicate that in June 2022, the U.S. State Department initiated a drone spraying program to "use multi-functional drones to remotely identify, then kill coca crops in Colombia – which are often protected by guards, perimeters of explosives, or even wild animals – with reduced risks to humans involved" (Crumley, 2022).

Figure 10-13 Overview of how drones could identify illegal crops from the U.S. Department of State



Source: (Cox, 2022)

For many decades, the State Department operated a fleet (contractor and government-operated) manned aircraft intending to use "aircraft to spray a glyphosate-based herbicide mixture on coca and opium poppy fields, which are illegal in Colombia and are the vital ingredients of the cocaine and heroin trades... Pilots release the spray only after they have visually identified coca in the flight line" (Aerial Eradication of Illicit Crops: Frequently Asked Questions. (2003). Washington DC: US Department of State, 2003). However, these older methods of drug crop eradication do not offer the precision that autonomous systems can provide, coupled with a reduced cost and reduced risk to human lives as the "Department of State wants the drones because it says improvised explosive devices, ambushes, and hazardous wildlife are threats to personnel ."(Cox, 2022) See Figure 10-13.

As with other areas of the agriculture sector, sensors, databases, and autonomous systems show great promise in being more effective and efficient than their traditional human-operated counterparts.

Space Farming-Unlocking the Possibilities

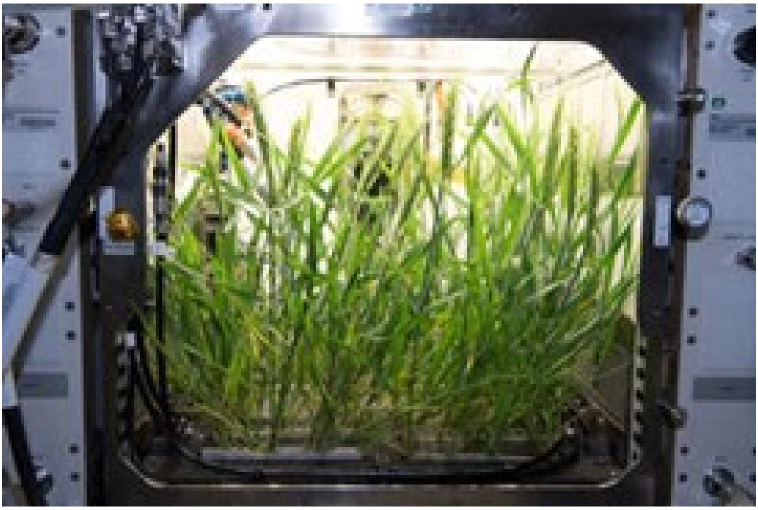
Space-based platforms are changing how we grow food and live on earth, yet they are also evolving humankind's ability to work, explore and live in space. The idea of growing food in space is one of the goals and a true necessity to make space travel viable; “almost half of the experiments being carried out on the International Space Station (ISS) revolve around biotechnology and plant growth in space” (Space Farming: How Does Farming Work in Space?, 2021) (“Space Farming: How Does Farming Work in Space?” 2021).

The ability to apply these zero-gravity experiments to current food production methods would change spaceflights as we know them today by “creating self-sufficient crews for the first manned flights to Mars, creating a garden on the ISS, or even just cultivating food in space to alleviate the adverse environmental impacts farming on Earth has on local ecosystems .”(Space Farming: How Does Farming Work in Space? 2021)

The Vegetable Production System, known as Veggie, is a space garden residing on the space station. Veggie’s purpose is to help NASA study plant growth in microgravity while adding fresh food to the astronauts’ diet and enhancing happiness and well-being on the orbiting laboratory…Veggie has successfully grown a variety of plants, including three types of lettuce, Chinese cabbage, mizuna mustard, red Russian kale, and zinnia flowers (Growing Plants in Space, 2022).

Veggie is only one of many experiments that are focused on plant production. Another experiment is the Advanced Plant Habitat (APH); like Veggie, it is a growth chamber on the space station for plant research, see Figure 10-14. “It uses LED lights and a porous clay substrate with controlled release fertilizer to deliver water, nutrients, and oxygen to the plant roots" ("Growing Plants in Space," 2022). APH is an automated system that uses "cameras and more than 180 sensors that are in constant interactive contact with a team on the ground at Kennedy (space center)" (Growing Plants in Space, 2022).

Figure 10-14 The first growth test of crops in the Advanced Plant Habitat aboard the International Space Station yielded great results. Credits: NASA

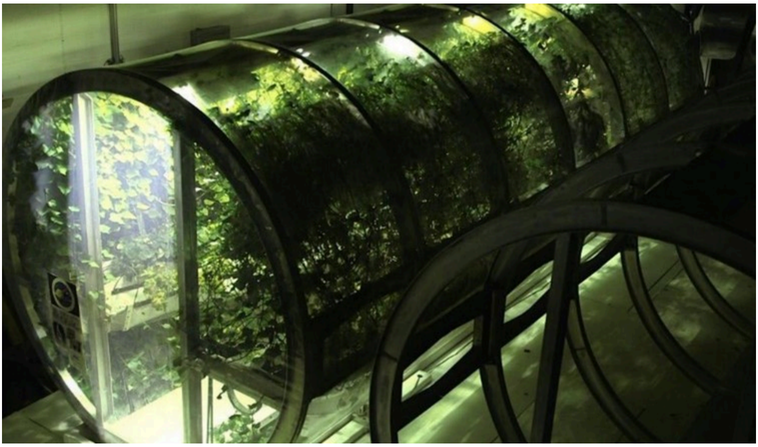


Source: (Growing Plants in Space, 2022)

The United States is not the only country working to grow food in space. Russia launched plant experiments as part of the second Sputnik ship in the 1960s (Sinelschikova, 2020). The conquest of space and the human desire to explore the vastness of space is only limited by our ability to grow sustainable crops in space.

A vitamin space greenhouse refers to 'Vitacikl-T' – a titanium tube setup that allows a conveyor-belt system to grow vegetables aboard the International Space Station. The construction consists of a spinning drum with six root modules…The operations are performed in a cycle, one taking place every 44-66 days, and, for the time being, this type of setup has been able to produce bigger and better results than any other foreign-made space gardens. (Sinelschikova, 2020) See Vitacikl-T growing plants in Figure 10-15.

Figure 10-15 A picture of 'Vitacikl-T' Institute of Biomedical Problems (IBMP) R.A.



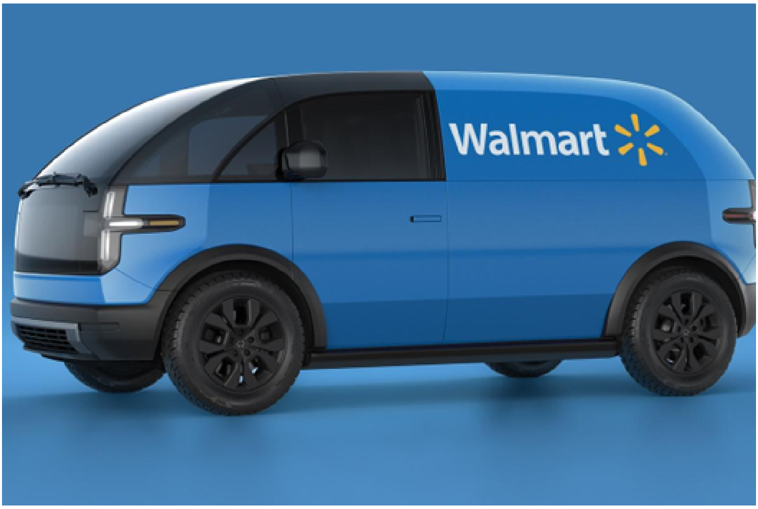
Source: (Sinelschikova, 2020)

Plants have been grown at the ISS since 1982. "Russian cosmonauts have been eating produce grown in space since 2003, and American astronauts began doing the same in 2015. Eating space-grown cultures has been allowed by law since the 1980s when scientists first determined their safety" (NASA, 2022).

The data gathered from the plant lifecycle in space can be applied to everyday farming with the databases and lessons learned just a click away. Space agriculture also has the "potential to impact farming practices here on Earth – namely with higher yields, more efficient production systems, and closed loop nutrient and water recycling systems that make the most of every drop of resource at our disposal ."(Space Farming: How Does Farming Work in Space? , 2021) The lessons in farming from traditional family farms, industrial farming, and space-based farming are paving the way for humankind to realize the dream of exploring Mars or taking a vacation on board a galactic space station.

Walmart has entered into an agreement with Canno Electric Vehicles to provide "4,500 Canoo Lifestyle Delivery Vehicles (LDVs), which will be driven by Walmart staff as they fulfill online orders, with an option to purchase up to 10,000. (Lavars, 2022). There is speculation that Walmart will evaluate the LDVs for autonomous delivery to remain competitive. See a rendering of the LDV in Figure 10-16. Kroger formed a collaboration with Nuro autonomous vehicles in 2018. Two years later, Walmart also entered a relationship with Nuro. Walmart has continued to step into the autonomous delivery space by partnering with Cruise, a self-driving vehicle company that operates in several large cities, including San Francisco, California, and Phoenix, Arizona (Cruise Self Driving Vehicles, 2022). See the rendering of Cruise vehicle in Figure 10-17.

Figure 10-16 A rendering of the Canoo Lifestyle Delivery Vehicle



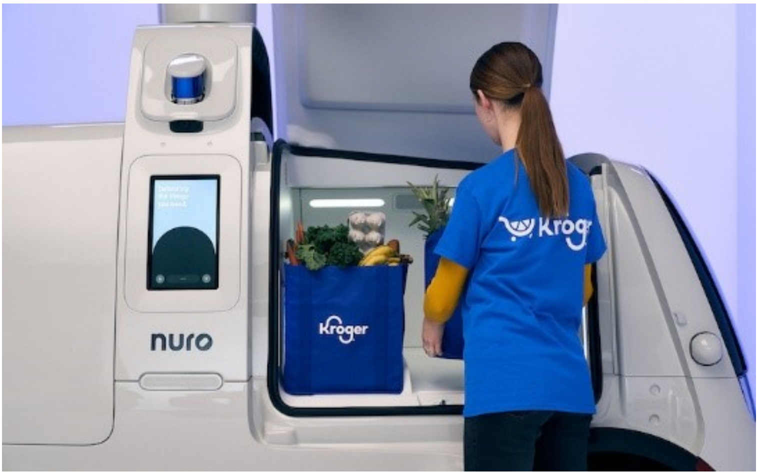
Source: (Lavars, 2022)

Figure 10-17 Walmart partners with Cruise vehicles for additional robotic delivery coverage

Source: (Cruise Self Driving Vehicles, 2022)

Several grocery stores, along with Kroger, already have autonomous delivery. Kroger said, “The role of autonomous vehicles in our seamless ecosystem continues to increase, contributing to meeting our customers in the context of their day without compromising on the quality or value while contributing to our long-term growth and sustainability goals .”(Redman, 2022)

Figure 10-18 An example of the Nuro vehicle Kroger uses



Source: (Redman, 2022)

Kroger plans to expand the Nuro autonomous delivery service's availability in Houston with the inception of the third-generation vehicles. (Redman, 2022) See an example of the Nuro in Figure 10-18.

Conclusions

The days of the family farm dairy being one of the only data sources for farming is long over. Even the days of limited information sharing from one town to another have ceased. The reality of obtaining, analyzing, and using multiple layers of agrarian data from around the world at the push of a button is now the agricultural arena reality. The lessons learned, generational experience, crop planting tips, tricks, weather, watering analysis, and numerous other data points are now available to all in the industry, from beginner farmers to institutional operations. Spaced-based platforms and various autonomous systems used today are just the start. The fifth industrial revolution is posed for humankind and machines to metaphorically dance together with few limitations.

The ability to use space data, aggregated with IoT data to inform drones on precision weed and water control, is the new reality of the agricultural industry. The world now uses autonomous systems for precision agriculture and does dull, dirty, dangerous, repetitive jobs that assist in increasing production while easing the employment issues.

The modern-day farmer spends more time with data, chemicals, and computers than dirt and seeds. The need to grow food for an increasing population continues to challenge the industry. Using technology to increase livestock worldwide or assist in humanitarian relief in underserved countries gives purpose to this technology far beyond the labor savings and scientific quest for knowledge. Humankind's desire to reach beyond our planet and colonize other planets and galaxies will continue to bring one undeniable truth to light: agriculture will be at the center of all humankind's endeavors.

Questions

1. Do you think human evolution will see the day when all agriculture, from beginning to end, is done by

autonomous systems?

2. List three disruptive technologies that have altered the family farm in the past 50 years.
3. When designing an agricultural footprint, how would you take advantage of airspace and freedom of movement with autonomous systems versus manned systems?
4. Can agriculture and a nation's food supply be weaponized? If so, can you name three ways the use/misuse of autonomous systems can neutralize this weaponization?
5. Describe data layers and how they can be applied to the agricultural arena?

References

Aerial Eradication of Illicit Crops: Frequently Asked Questions. (2003). Washington DC: US Department of State. (2003). Retrieved from https://2001-2009.state.gov/: https://2001-2009.state.gov/p/inl/rls/fs/18987.htm

Carletto, C. (2021). Better data, higher impact: improving agricultural data systems for societal change. *Carletto, C. (2021). Better data, higher impact: improving agriculturEuropean Review of Agricultural Economics* (pp. 48(4), 719-740,doi:10.1093/erae/jbab030). Carletto, C. (2021). Better data, higher impact: improving agricultural data sysERAE .

CEMA. (2021, July 19). *CEMA_smart_agriculture_solutions_support_EU_eco-schemes_FINAL.* Retrieved from https://www.cema-agri.org: https://www.cema-agri.org/images/publications/position-papers/ 2021_07_19_CEMA_smart_agriculture_solutions_support_ EU_eco-schemes_FINAL_.pdf

Colby Community. (2018). *The Long Lasting Effects of the Industrial Revolution. (2018). Global Food, Health, and Society.* Retrieved from https://web.colby.edu/: https://web.colby.edu/st297-global18/2018/10/29/the-long-lasting-effects-of-the-industrial-revolution/

Cox, J. (2022). *US Wants to Use Drones to Kill Coca Plants in Colombia.* Retrieved from https://www.vice.com/: https://www.vice.com/en/article/bvmgbz/us-wants-to-use-drones-to-kill-coca-plants-in-colombia

Cruise Self Driving Vehicles. (2022). Retrieved from https://www.getcruise.com/services: https://www.getcruise.com/services

Crumley, B. (2022). *US eyes drone deployment to eradicate Colombia's coca crops.* Retrieved from https://dronedj.com/: https://dronedj.com/2022/06/14/us-eyes-drone-deployment-to-eradicate-colombias-coca-crops/

Defense, U. S. (2020, March 11). *DOD adopts 5 principles of artificial intelligence ethics.* Retrieved from Army, mil: 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

Epplett, A. (2021). *What was the Agricultural Revolution?* Retrieved from https://study.com/: Epplett, A. (2021). What was the Agricultural Revolution? Retrieved from https://study.com/learn/lesson/agicultural-revolution.html#:~:text=The%20Agricultural%20Revolution%20of%20the,led%20to%20an%20enclosure%20movement

Farmtogether. (2022). *the-power-of-satellite-imagery-in-agriculture.* Retrieved from The Power of Satellite Imahttps://farmtogether.com: The Power of Satellite Imagery Ihttps://farmtogether.com/learn/blog/the-power-of-satellite-imagery-in-agriculture

Finkelnburg, D. (2021). *The Future of Weed Control.* Retrieved from https://www.no-tillfarmer.com: https://www.no-tillfarmer.com/articles/10627-the-future-of-weed-control

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/

Green, L. C. (1998). *The Law of War in Historical Perspective.* Providence, RI: U.S. Naval War College.

Growing Plants in Space. (2022). Retrieved from https://www.nasa.gov/content/: https://www.nasa.gov/content/growing-plants-in-space

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.

Increase Crop Yield With Precision Agriculture Technology. (2022). Retrieved from https://skywatch.com/agriculture-ndvi/: https://skywatch.com/agriculture-ndvi/#:~:text=Satellite%20imagery%20is%20being%20widely, information%20to%20predict%20crop%20yields

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

Jarman, M. &. (2018). *Satellites for agriculture-Catapult Satelite Applications.* Retrieved from https://projectblue.blob.core.windows.net/: https://projectblue.blob.core.windows.net/media/Default/Imported%20Publication%20Docs/SatellitesForAgriculture1825_181217_WEB.pdf

John Deere. (2022). *John Deere Reveals Fully Autonomous Tractor at CES 2022.* Retrieved from https://www.deere.com/: https://www.deere.com/en/news/all-news/autonomous-tractor-reveal/

John Deere. (2022). *Building Digital Security into Autonomous Tractors.* Retrieved from www.deere.com/en/: https://www.deere.com/en/stories/featured/building-digital-security-into-autonomous-tractors/

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.

Lavars, N. (2022). *Walmart eyes an electric future in Canoo's Lifestyle Delivery Vehicle.* Retrieved from https://newatlas.com/: https://newatlas.com/automotive/walmart-electric-canoo-lifestyle-delivery-vehicle/?utm_source=New+Atlas+Subscribers&utm_campaign=8c8dda7960-EMAIL_CAMP

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/

Measures, N. (2021). *How satellite imagery is helping precision agriculture grow to new heights.* Retrieved from https://www.eco-business.com: https://www.eco-business.com/news/how-satellite-imagery-is-helping-precision-agriculture-grow-to-new-heights/

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

MIT Technology Review. (2018, March 12). *When an AI 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/

NASA. (2022). *NASA Is Growing Chili Peppers In The Space Station.* Retrieved from https://www.livekindly.com: https://www.livekindly.com/nasa-growing-chili-peppers-space-station/#:~:text=Astronauts%20and%20cosmonauts%20have%20been,doing%20the%20same%20in%202015.

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

Redman, R. (2022). *Kroger to step up unmanned grocery delivery in Houston.* Retrieved from https://www.supermarketnews.com/:

https://www.supermarketnews.com/technology/kroger-step-unmanned-grocery-delivery-houston

Roshanianfard, A. N. (2020). A review of autonomous agricultural vehicles (The experience of Hokkaido University). *Journal of Terramechanics*, 91, 155-183. doi:10.1016/j.jterra.2020.06.006.

Roy, S. K. (2022). Genetic Algorithm based Internet of Precision Agricultural Things (IopaT) for Agriculture 4.0. *Internet of Things* (pp. 18, 100201). (IopaT) for Agriculture 4.0. doi:https://doi.org/10.1016/j.iot.2020.100201. Retrieved from ral Things (IopaT) for Agriculture 4.0. Internet of Things, 18, 100201. doi:https://doi.org/10.1016/j.iot.2020.100201: Roy, S. K., & De, D. (2022). Genetic Algorithm based Internet of Precision Agricultural Things (IopaT) for Agriculture 4.0. Internet of Things, 18, 100201. doi:https://doi.org/10.1016/j.iot.2020.100201

Selbst, A. D. (2020). NEGLIGENCE AND AI'S HUMAN USERS. *Boston University Law Review*, 1323.

Sinelschikova, Y. (2020). *Russia invents new way to grow vegetables in space.* Retrieved from https://www.rbth.com/: https://www.rbth.com/science-and-tech/333203-russia-grow-vegetables-space

Singh, I. (2021). *Precision farming company raises $20M to deploy herbicide-spraying AI drone swarms.* Retrieved from https://dronedj.com: https://dronedj.com/2021/05/06/precision-ai-drone-spraying/

Space Farming: How Does Farming Work in Space? (2021).

Retrieved from https://stories.pinduoduo-global.com/agritech-hub: https://stories.pinduoduo-global.com/agritech-hub/how-does-space-farming-work

Tertill. (2022). *Tertill Weeding Robot.* Retrieved from https://tertill.com/products/tertill: https://tertill.com/products/tertill

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/department-of-defense-press-briefing-on-the-adoption-of-ethical-principles-for/

United States Department of Defense, Defense Innovation Board. (2019). *AI 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

YANMAR. (2022). *Boston dynamics Transporter Systems.* Retrieved from www.bostondynamics.com/products: https://www.bostondynamics.com/products

11.

CIVILIAN USE OF SPACE FOR ENVIRONMENTAL, WILDLIFE TRACKING, & FIRE RISK ZONE IDENTIFICATION (RYAN)

This chapter provides an overview regarding how an increasing variety of civilian uses of space is transforming terrestrial activities such as monitoring endangered species, tracking environmental changes, and providing fire risk management support. The global perspective made possible from the high ground of space has transformed and enriched many civilian activities, providing more, different, and better data that contributes both to the science and to the practice of these activities.

Student Learning Objectives

After reading this chapter, students should be able to do the following:

1. Define cislunar space
2. Describe how satellites are used for a variety of civilian uses

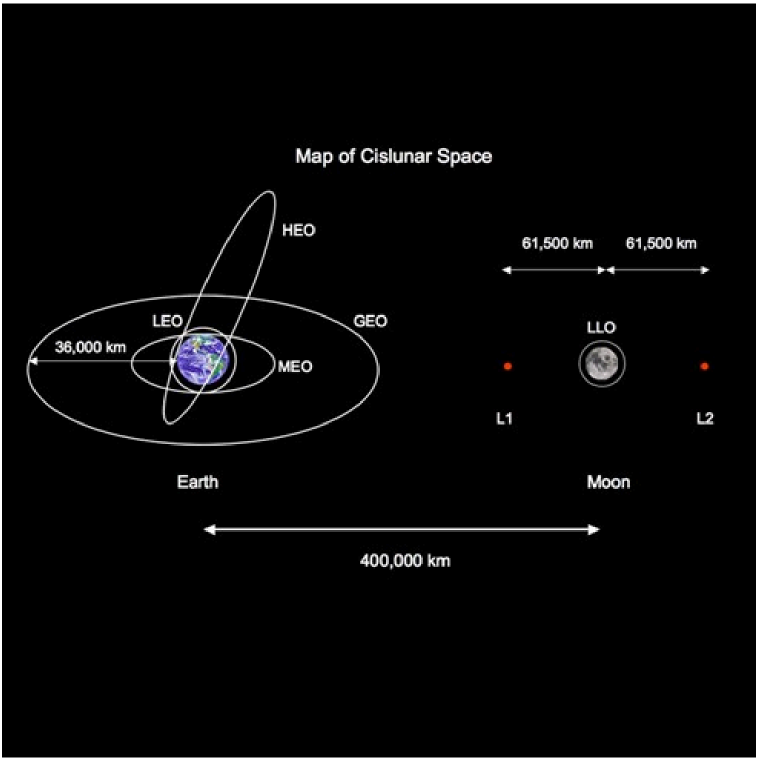
Introduction

The first venturing of humankind out of our earthly atmosphere required harnessing the capabilities and resources of nation-states to accomplish. In the United States, the intentional use of space for civilian purposes was declared in the National Aeronautics and Space Act of 1958: "it is the policy of the United States that activities in space should be devoted to peaceful purposes for the benefit of all mankind". (Hudson, 1990) Since then, the National Aeronautics and Space Agency (NASA) has systematically expanded the civil use of space, often in cooperative efforts with other nations. As a result, the impact of space technology is extensive, touching on nearly every aspect of modern life. In this chapter, three applications are specifically explored, with the caveat that these are but three of the broad uses of space-based resources to augment the terrestrial based efforts that we humans use to make life better.

In this chapter, the part of space discussed is that part called cislunar (also spelled cis-lunar), which is to say that area extending from near-Earth space to the Moon's orbital sphere (Holzinger, Chow, & Garretson, 2021). The specific definition of cislunar space is: "Cislunar space is the area around the Earth extending out to just beyond the Moon's orbit, and including all of the five Lagrangian points that are stable in position in reference to the Earth and Moon as they rotate about each other." (The Space Option, 2012) Figure 11-1 shows a graphical description of cislunar space, annotated with common orbits, L1, and L2 for reference. The acronyms are defined here:

- LEO: low earth orbit, which is between 160 and 2,000 km above the earth's surface (CSIS, 2017)
- MEO: middle earth orbit, which is between LEO and GEO(CSIS, 2017)
- GEO: geosynchronous orbit, which orbit at 35,786 km(CSIS, 2017). (Note that this use of the acronym GEO should not be confused with the Group on Earth Observations, also referred to as GEO.)
- HEO: highly elliptical orbit, which orbit along an oblong rather than a circular path for greater dwell time over a part of the earth (CSIS, 2017)
- LLO: low lunar orbit is approximately 100 km above the lunar surface(Parker & Anderson, 2013)
- L1 and L2: "Lagrange points are caused by the balance between the gravitational fields of two large bodies; equilibria between two pulling forces."(CSIS, 2017)

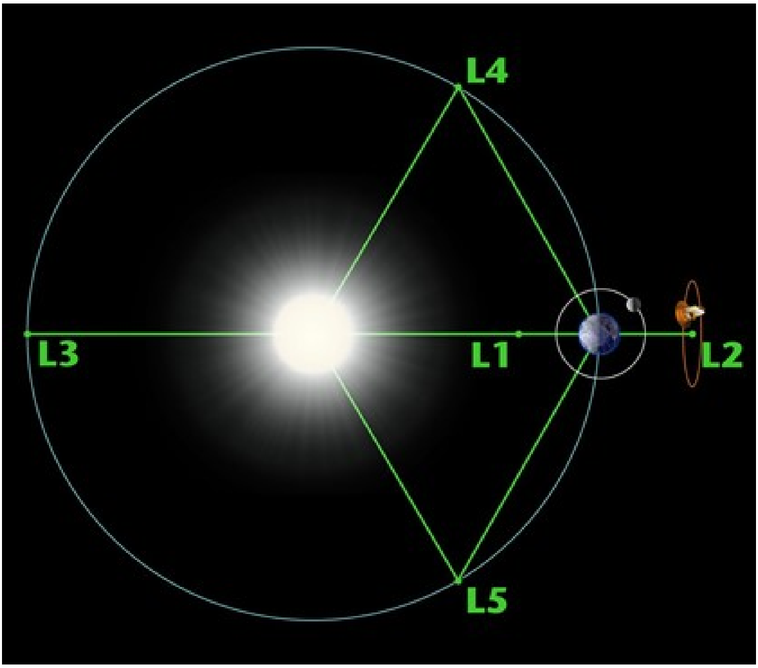
Figure 11-1 Cislunar Space



Source: (The Space Option, 2012)

There are five Lagrange points, referred to as Lx, where x is the numeric designator. "L1 lies between Earth and the sun at about 1 million miles from Earth; L2 also lies a million miles from Earth, but in the opposite direction of the sun." (Howell, 2017) These points are shown graphically in Figure 11-2.

Figure 11-2 Lagrange Points



Source: (Howell, 2017)

In cislunar space, there can be earth-orbiting systems, moon-orbiting systems, and moon-based systems, as well as systems that transit both orbital systems. The orbital and moon-based systems may be manned or unmanned. Sensors incorporated into these systems may be passive, such as telescopes and antennas, or active, such as radars and lasers. (Holzinger, Chow, & Garretson, 2021)

Applications

The promise of using space-based resources to help understand and manage the environment was an early concept in humanity's approach to space resources. The high ground of space not only provides an ability to observe a broader swath of the earth's surface, but it also provides the ability to observe and measure the atmosphere and weather patterns. As a result, early applications included launching satellites with specialized equipment for viewing the earth's surface, such as LandSat, and for monitoring the weather, such as the Television InfraRed Observational Satellite (TIROS). The TIROS-1 satellite was one of the earliest programs, having been launched in 1960 with the mission to collect weather data. (NASA, 2010) Landsat was launched in 1972 with the mission to collect "data on the forests, farms, urban areas and freshwater" of Earth. (NASA, 2022) From these early efforts, the ability to surveil and study the environment has grown tremendously, contributing to our knowledge and understanding of the planet we live on and the effects that humans have on both the environment and the climate.

Environmental monitoring from space started as a pretty straight-forward proposition: place instruments into orbit around the planet that collect specific types of data, transfer that data-to-data fusion centers, and analyze the information. But as the use of space became normalized, through things like global communications systems, people started to realize that there was more that could be done. Some of these applications included putting tracking devices on animals and placing terrestrial sensors in difficult to monitor locations: the data collected could be sent to satellites and then retransmitted to more convenient or better equipped terrestrial locations. In this approach, the earth-based target of study transmitted data to the satellite for relay. In a different approach, made available through the development of position-locating satellite systems, such as the Global Positioning System (GPS), the target of study receives signals from the satellites, which are then used to identify the locations at measurement intervals. With the increasing sophistication and miniaturization of electronic devices, the application of these general approaches to a wider body of problems has become possible.

Thus, the basic concepts of using space-based systems in applications associated with environmental monitoring include the following approaches:

1) equipping space-based systems, including satellites and orbiting laboratories, with instrumentation suitable for observing aspects of the environment, including climate and terrestrial features;

2) using space-based systems to relay data from terrestrial targets of research to terrestrial data analysis centers; and

3) using space-based systems to send data to terrestrial targets of research for later accession and analysis.

These approaches may also, of course, be used in combinations.

Current Systems

There are many current systems being used for environmental monitoring, wildlife tracking, and fire risk management. The business of observing the Earth is complex and can be expensive. Complicating things is the fact that there are only so many orbital positions: access to space must be coordinated and managed carefully. That makes international cooperation necessary. Such cooperation includes not only national and regional space authorities but also the companies building the sensors and the satellites as well as advocacy groups and researchers who use the resulting data.

Illustrative of the level of cooperation is the Group on Earth Observations (GEO), "is a partnership of more than 100 national governments and in excess of 100 Participating Organizations." (Group on Earth Observations, n.d.) The focus of GEO is coordinating the development of the Global Earth Observation System of Systems (GEOSS) in order to advance the international community's ability to collect and use data related to the following topics: biodiversity and ecosystem sustainability, disaster resilience, energy and mineral resource management, food security and sustainable agriculture, public health surveillance, infrastructure and transport management, sustainable urban development, and water resources management. As of 2022, there are 113 member governments representing the vast majority of the Earth's population. Additionally, there are 143 participating organizations, including those such as the Association of Geospatial Industries, the Arab States Research and Education

Network (ASREN), the European Association of Remote Sensing Companies (EARSC), and the World Ocean Council. (Group on Earth Observations, n.d.)

Very large countries, such as the United States, have established systems in place to contribute to the global earth sensing goals. The U.S.'s NASA has a program called the Earth Observation System (EOS) that has spanned decades of effort, including 48 completed missions. There are currently 33 active missions in NASA's Earth Fleet with an additional 17 missions planned (NASA, 2021). Similarly, the European Space Agency (ESA) has a program of missions for observing the Earth, which started in the 1970s (ESA, 2021), as do China (Jones, 2022) and India ((Indian Space Research Organization, n.d.)

With such active participation in Earth observation, it is impossible to catalog every effort. However, by looking at examples of activity, one can develop a better understanding of the scope and nature of the activities.

Water-Focused Topics

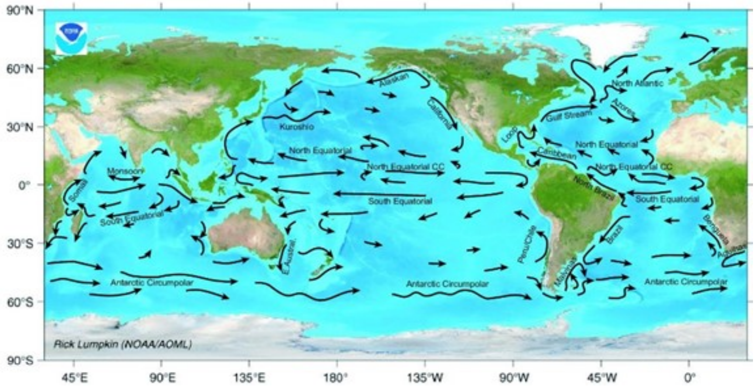
Water is a very important part of life on Earth. It is not only necessary to sustain life but the water in the oceans, in rivers, and in the atmosphere affect the weather and agricultural. There are many things we need to understand about the Earth's water, including but not limited to oceanic currents, marine mammals and fisheries, river systems, and sea levels.

Oceanic Currents

Oceanic currents, shown in Figure 11-3, are the rivers that flow through the ocean. Because of temperature and salinity, these currents can flow lower or higher in the oceans, which in turn affect evaporation rates, ice melt, and aquatic life movement. Oceanic currents affect the climate of the Earth, the life in the oceans, and localized ecosystems. Using satellites to monitor oceanic currents provides an important set of data to that being collected through ocean buoys and other terrestrial systems. How the currents actually work is very complicated:

“Winds, water density, and tides all drive ocean currents. Coastal and sea floor features influence their location, direction, and speed. Earth’s rotation results in the Coriolis effect which also influences ocean currents. Similar to a person trying to walk in a straight line across a spinning merry-go-round, winds and ocean waters get deflected from a straight-line path as they travel across the rotating Earth. This phenomenon causes ocean currents in the Northern Hemisphere to veer to the right and in the Southern Hemisphere to the left.” (NOAA, 2011)

Figure 11-3 Oceanic Currents



Source: (NOAA, 2011)

Ocean currents are studied to understand how they work, what affects their movement, and how they change over time. In 2012, NASA released a 20-minute video showing how ocean currents had evolved using data from 2005 to 2007. You can watch the video at this link (current August 2022): http://svs.gsfc.nasa.gov/goto?3827. An enormous amount of data was used to make that video. As described in the NASA announcement:

The Estimating the Circulation and Climate of the Ocean (ECCO) … model-data syntheses are being used to quantify the ocean's role in the global carbon cycle, to understand the recent evolution of the polar oceans, to monitor time-evolving heat, water, and chemical exchanges within and between different components of the Earth system, and for many other science applications. … Data used by the ECCO project include: **sea surface height** from NASA's Topex/Poseidon, Jason-1, and Ocean Surface Topography Mission/Jason-2 satellite altimeters; **gravity** from the NASA/German Aerospace Center Gravity Recovery and Climate Experiment mission; **surface wind stress** from NASA's QuikScat mission; **sea surface temperature** from the NASA/Japan Aerospace Exploration Agency Advanced Microwave Scanning Radiometer-EOS; **sea ice concentration** and **velocity** data from passive microwave radiometers; and **temperature and salinity** profiles from shipborne casts, moorings and the international Argo ocean observation system. (NASA, 2012)

Marine Mammals and Fisheries

Marine mammals, such as sea lions, whales, and seals, are important to understand because they reflect the health of the environment in which they exist. Important data for understanding marine mammal behavior includes tracking where they go, where and when they migrate, and proximity to other species. Some projects using satellites to assist in this research are described here. Figure 11-4 shows marine mammals fitted out with satellite tags that "the movements and location of the animal, dive data (the depth and length of the dive), water temperature and salinity of the water." (Pacific Marine Mammal Center, 2019)

Figure 11-4 Sea Lions Fitted with Satellite Tags

Source: (Pacific Marine Mammal Center, 2019)

The Alaska Ecosystems Program uses satellites to track radio signals from beacons attached to seals and sea lions. Because the animals swim hundreds of miles in the far north, a polar-inclined satellite is used to track the beacons. Additionally, another satellite makes it possible to correlate the movement of the animals to places more likely to have concentrations of prey. The combination of this data provides important insight into the health of the species. (JPL, 2001)

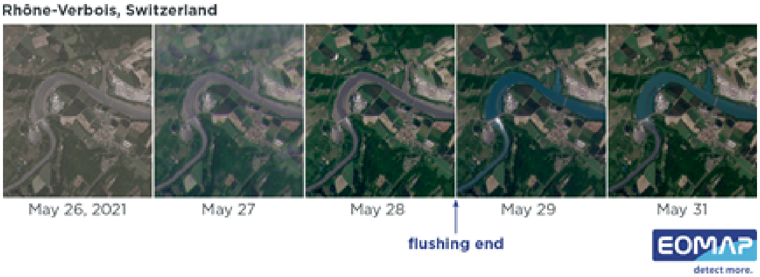
Fisheries are an important target for monitoring for several reasons. One reason is simply to monitor the health and sustainability of the fish. Another is to monitor human behavior, such as poaching and illegal fishing. Yet another is to monitor environmental threats to fisheries, such as oil spills. Satellite systems are uniquely placed above the Earth to provide unblinking observation of the activities of humans and of environmental problems. In fact, it was satellite systems that first provided the data that alerted authorities to an oil leak off the California coast in October 2021: imagery data from Landsat 8 and Operational Land Imager (OLI) combined with synthetic aperture radar imagery from Sentinel-1B were used to identify and locate the source of oil that had been discovered on the ocean surface near California a day earlier. The continual monitoring of the environment was key to the timely identification. (NASA, 2021)

River Systems

River systems are the lifeblood of the land. They bring water from mountain snows to farms and seas, they provide fresh water for drinking and agriculture, and they provide a natural movement of sediment from land to sea. But rivers change. Sometimes they change naturally, as when floods carve out new channels or when water sources dry up and rivers disappear. Other times they are changed by man, through dams, canals, or displacement. Satellite systems can track changes to river systems through visual, infrared, and radar imagery as well as through temperature and humidity measurements. In this way, everyday effects on wildlife, fisheries, and humans can be understood and managed.

As an example of satellite support to river management, there is a continual challenge presented to regions by the necessity to manage river dams. There is a specific problem from "excess sedimentation, like sand and gravel from floods or rivers that are deposited downstream into these systems" which "can build up over time, leading to a loss of water storage capacity and damaging hydropower dams, turbines, and water intakes. Sediment-related maintenance and removal costs can account for up to 40% of all maintenance costs." (Preston, 2022) Figure 11-5 shows "sediment levels before and after a river flushing event at the Verbois hydropower plant in Switzerland." (Preston, 2022)

Figure 11-5 Monitoring Dam Flushing from Space



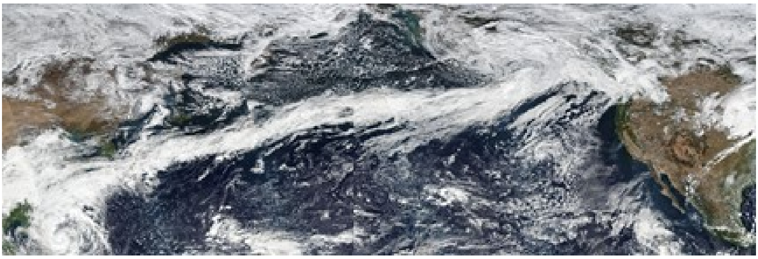
Source: (Preston, 2022)

Disasters are also a challenge. An important part of understanding and managing river systems is understanding precipitation and resulting floods or draughts. Too much rain and rivers flood. Too little rain and rivers, and lakes, dry up. Also, too little rain leads to increased risk of wildfires.

"The Global Precipitation Measurement (GPM) Core Observatory paints a picture of global precipitation every 30 minutes, with help from its other international satellite partners. It has provided innumerable insights into Earth's precipitation patterns, severe storms, and into the rain and snow particles within clouds. It has also helped farmers trying to increase crop yields, and aided researchers predicting the spread of fires." (Patel, 2019)

The ability to observe precipitation from space has also led to the development of the concept called "atmospheric rivers", which are "long, narrow bands of moisture in the air". (Patel, 2019) The difference between an atmospheric river and a storm is significant: the atmospheric river brings a steady stream of water to an area, just as a terrestrial river brings water to a specific area. It is a not a one-off event but a conveyor belt of moisture. Figure 11-6 shows an atmospheric river stretching from Asia to the West Coast of the North American continent.

Figure 11-6 Atmospheric River Between Asia and North America



Source: (NASA, 2017)

This photo is a composite of two images taken by "the Visible Infrared Imaging Radiometer Suite (VIIRS) on the Suomi NPP satellite." (NASA, 2017) The ability to actually see the atmospheric rivers from satellites has had an enormous impact on weather prediction, increasing the ability to predict when an atmospheric river will affect an area.

Sea Levels

There are many things that affect sea level, and it is a very real concern for the life of millions of people who live in threatened areas along coasts and on islands. The scientific community monitors many elements that can affect sea levels, including sea ice and sea temperatures.

"Sea ice is frozen seawater that floats on the ocean surface. It forms in both the Arctic and the Antarctic in each hemisphere's winter; it retreats in the summer but does not completely disappear. This floating ice has a profound influence on the polar environment, influencing ocean circulation, weather, and regional climate." (NASA, 2016)

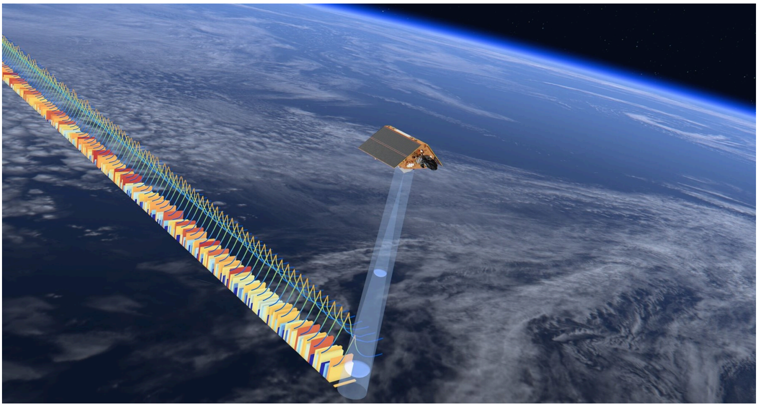
Although melting sea ice does not raise sea levels, because it is already in the water, it has a very important impact on the parts of the climate that can affect sea level: the temperature of the atmosphere and the amount of sunlight that is reflected back into space. Simply put bright white ice is highly reflective. When this ice becomes sooty from pollution, it becomes less reflective. When the ice melts entirely, it is not at all reflective – it doesn't exist. So, it is very important to understand and monitor sea ice.

"Once sea ice begins to melt, a self-reinforcing cycle often begins. As more ice melts and exposes more dark water, the water absorbs more sunlight. The sun-warmed water then melts more ice. Over several years, this positive feedback cycle (the ice-albedo feedback) can influence global climate." (NASA, 2016)

Sea ice is monitored through satellite imagery, radar, and infrared systems.

Monitoring sea levels is an important part of knowing how the levels are trending. These are also monitored from space through imagery and radar systems. Figure 11-7 shows a conceptual artist rendition of how radar altimetry technology is used to gather precision data on sea levels. (ESA, 2021)

Figure 11-7 conceptual artist rendition of how radar altimetry technology is used to gather precision data on sea levels



Source: (ESA, 2021)

Land-Focused Topics

Land is, of course, where humans live and primarily operate. Issues associated with land use include natural disasters (including fires and floods) and population density and movements.

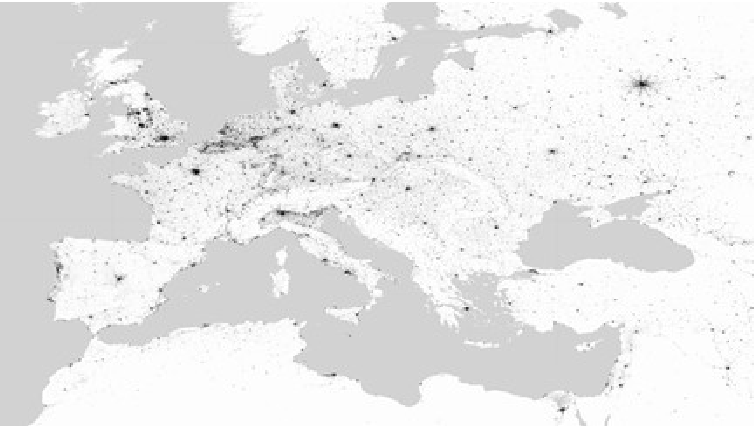
Natural Disasters

Large scale natural disasters differ from more localized disaster not only in the scale of the problem but also in the cascading issues that stem from the disaster. For example, the effects of Hurricane Katrina, while devastating to the Gulf Coast and New Orleans specifically, affected the entire oil and gas infrastructure that in turn affected both local and global markets. Monitoring the potential and actuality of a large-scale natural disaster, particularly those that occur in remote locations, is only possible from the high ground of space. NASA uses satellites to detect and monitor "global intensive risk events that span a range of natural hazards — not only wildfires but earthquakes, tsunamis, floods, landslides, severe weather, winter storms, tropical cyclones and volcanoes." (NASA, 2022) Since it is a global issue, there has been a focus on international cooperation in these efforts, leading to the development of "infrastructure and … new relationships between international, regional and local natural disaster response agencies and other Earth-observing space agencies around the world." (NASA, 2022)

Population Density and Movements

There are a lot of people on this earth and the competition for resources is stiff. Simply knowing where humans live a difficult question can be and yet it is critical for understanding how to create programs and policies to address issues like food security and disaster management. The European Space Agency has created a program designed to bring the power of space to mapping the global human footprint. The program, named the World Settlement Footprint, provides "continuous data streams of high quality and free of charge satellite observations such as the Sentinels of the European Copernicus program and the Landsat missions" in order to "monitor the changes and trends in urban development globally." (ESA, 2021) A sibling program, called the Global Urban Footprint, "shows not just urban centers, but also tiny rural hamlets." (ESA, 2016) Figure 11-8 shows a view of Europe provided by this effort.

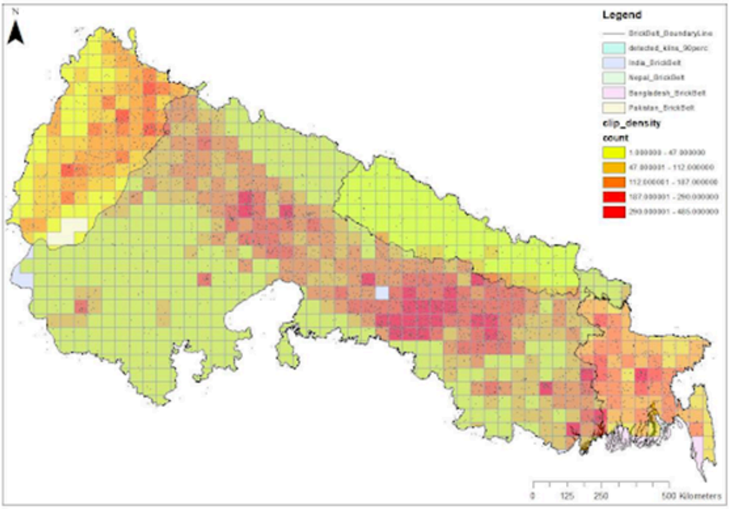
Figure 11-8 View of Europe – Global Urban Footprint



Source: (ESA, 2016)

Organizations are also using satellites to track human movements and identify areas in which human rights are being violated. “For example, across south Asia, there is a vast “Brick Belt” — a network of tens of thousands of brick kilns that employ some 23 million workers across India, Nepal, and Pakistan [that may be] rife with debt-bondage and child slavery.” (Zolli, 2018) “Researchers at the Rights Lab recently used satellite imagery and machine learning techniques to map the entire Brick Belt in unprecedented detail.” (Zolli, 2018) Figure 11-9 shows this map.

Figure 11-9 Map The Entire Brick Belt



Source: (Zolli, 2018)

These same techniques are being used to integrate many types of data to understand how humans move and why, such as linking movements to wide scale war, drought, or other issues.

Atmosphere Focused Missions

The makeup of the atmosphere controls how much radiation we are exposed to, how much heat is reflected from the Earth into space, and how well plants and animals survive on the planet. Issues with the atmosphere are extremely varied but also include lightning, atmospheric gases, the ozone layer, and the radiation shield.

Lightning

Monitoring lightning strikes around the world is more important than simply keeping track of them. "Lightning is a surprisingly elusive and complex natural phenomenon for the impact that it has on our daily lives. We are now at a place where we have excellent measurements of its many facets, which allow us to discover surprising new aspects of its behavior." (World Meteorological Organization, 2022)

Understanding the underlying phenomenon is key to prediction. Tracking lightning from space has not only assisted in gathering data to support research into lightning, but it has also expanded our knowledge of the many forms in which lightning occurs.

"Recent advances in space-based lightning mapping offer the ability to measure flash extent and duration continuously over broad geospatial domains. These new instruments include the Geostationary Lightning Mappers (GLMs) on the R-series Geostationary Operational Environmental Satellites (GOES-16 and 17) …, and their orbiting counterparts from Europe (the Meteosat Third Generation (MTG) Lightning Imager) and China (FY-4 Lightning Mapping Imager)." (World Meteorological Organization, 2022)

For example, it is now known that some storms can produce giant jets of lightning that go up to the edge of space. Figure 11-10 shows a recent example of one such jet, captured by the International Space Station in 2019.

Figure 11-10 Example Of One Such Jet, Captured By The International Space Station In 2019

Source: (Temming, 2021)

"Blue jets have been observed from the ground and aircraft for years, but it's hard to tell how they form without getting high above the clouds." (Temming, 2021) One can imagine the damage if one of these lightning bolts hit a satellite or an airborne system. They can also "affect how radio waves travel through the air — potentially impacting communication technologies." (Temming, 2021)

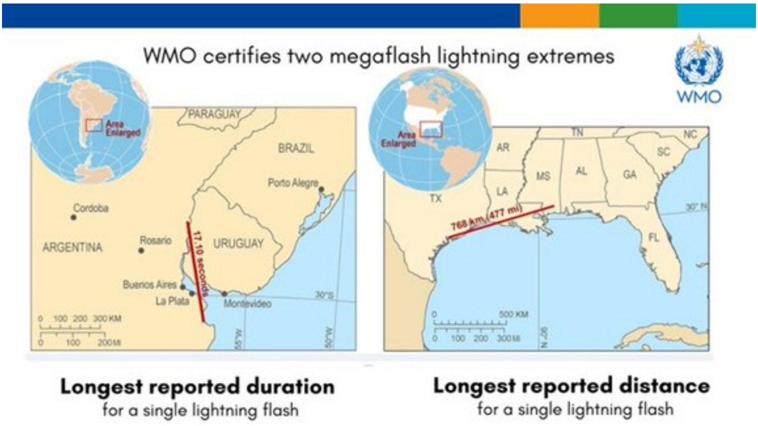
There is also a phenomenon called "megaflash" lightning, where a single flash of lightning occurs across a very large area. The World Meteorological Organization (WMO) certified two new records for megaflash lightning events in 2022 thanks to the ability to harness satellite technology to observe large areas of storms from above. These two records were for the largest area covered and for the longest duration of a single flash.

"The longest single flash that covered a horizontal distance of 768 ± 8 km (477.2 ± 5 miles) across parts of the southern

United States on 29 April 2020. This is equivalent to the distance between New York City and Columbus Ohio in the United States or between London and the German city of Hamburg. The greatest duration for a single lightning flash of 17.102 ± 0.002 seconds from the flash that developed continuously through a thunderstorm over Uruguay and northern Argentina on 18 June 2020." (World Meteorological Organization, 2022)

Figure 11-11 shows the location of the two record breaking strikes.

Figure 11-11 Record Breaking Mega-flash Lightning Events



Source: (World Meteorological Organization, 2022)

Atmospheric Gases and Particulates

Atmospheric gases pay a critical role in the survival of plants and animals on the earth. Most fundamentally, animals need a certain amount but not too much oxygen to survive. Too much oxygen can be deadly as well as a serious fire hazard. Plants need a certain amount but not too much carbon dioxide to survive. Too much carbon dioxide can be deadly as well as contributing to global climate change. Beyond the actual mixture of the gases in the air, there is also the question of particulates in the air. It is natural to have some dust and other microscopic things in the air but too much can lead to serious issues, such as lung cancer and acid rain. (World Health Organization, 2022)

Monitoring atmospheric gases has been a scientific focus for several hundred years. In 2023, a step forward will be taken with the launch of the first Carbon Mapper satellite. "The Carbon Mapper's Earth-orbiting imaging spectrometer will have a pixel size of about 30 meters (98 feet) square. Other imaging spectrometers currently in orbit have larger pixel sizes, making it hard to pinpoint the locations of sources that may not be visible on the ground, such as cracks in natural gas pipelines." (NASA, 2021) Figure 11-12 shows an example of the type of data that can be collected from space. This image was captured from the same types of sensing systems in an airborne platform.

Figure 11-12 Gas Plumes Captured with the Global Airborne Observatory over the Permian Basin in 2019

Source: (NASA, 2021)

Particulates come from both liquid air and material. Some of them naturally flow with the air currents over the earth, sometimes being precipitated out during storms. In some places, however, particulates can stay localized for long periods of time and cause problems to human health, crop cultivation, and even electronics.

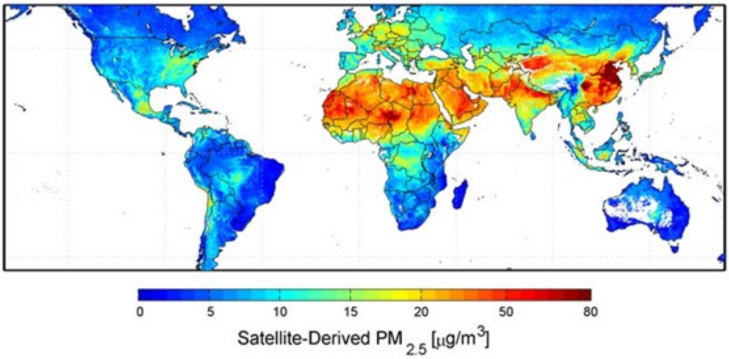
"Aerosol particle pollution—airborne solid particles and liquid droplets—comes in a range of sizes. Particles smaller than 2.5 micrometers pose the greatest risk to human health because they are small enough to be breathed deep into the lungs and, in some cases, enter the blood stream. These fine particles, about 30 times smaller than the width of a human hair, are also a major cause of poor visibility." (NASA, 2010)

It is important to realize that the vast majority of particulates come from natural sources, such as volcanoes, forest fires, and even plants. However, the naturally produced particulates tend to be larger sized. Manmade particulates tend to be smaller and more pervasive where humans live.

"Automobiles, incinerators, smelters, and power plants are prolific producers of sulfates, nitrates, black carbon, and other particles. Deforestation, overgrazing, drought, and excessive irrigation can alter the land surface, increasing the rate at which dust aerosols enter the atmosphere. Even indoors, cigarettes, cooking stoves, fireplaces, and candles are sources of aerosols." (NASA, 2010)

What is in the air can move with the wind. Pollution in one region can spread to other regions. It is a global issue. Treating it like a global issue requires a global surveillance ability. This simply cannot be done from the ground since some countries lack the resources to collect data. While "satellites [can] provide a global perspective, satellite instruments have generally struggled to achieve accurate measurements of the particles in near-surface air. The problem: Most satellite instruments can't distinguish particles close to the ground from those high in the atmosphere. In addition, clouds tend to obscure the view. And bright land surfaces, such as snow, desert sand, and those found in certain urban areas can mar measurements." (NASA, 2010) This problem has been partially solved by fusing multiple sources of data and by the deployment of better sensing systems. As a result, it is possible to create a global view of particulates in Earth's atmosphere, as shown in Figure 11-13. This image shows a global satellite-derived map of PM2.5 averaged over 2001-2006.

Figure 11-13 Global Satellite-Derived Map Of PM2.5 Averaged Over 2001-2006.



Source: (NASA, 2010)

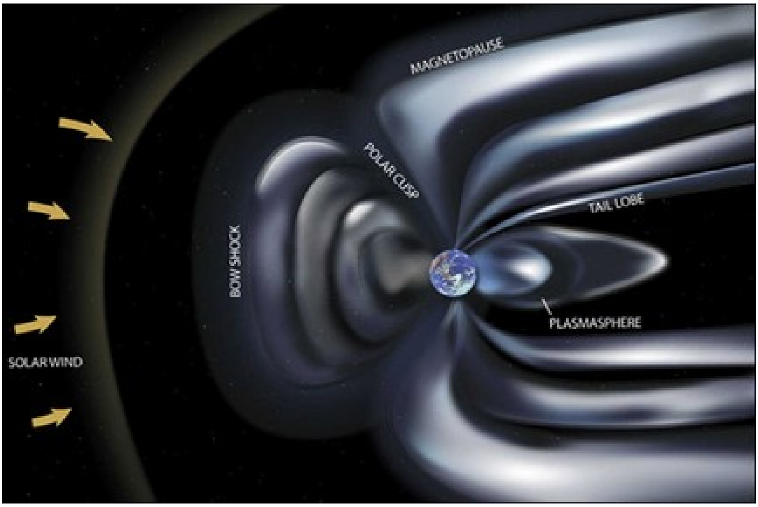
Ozone layer

The ozone layer is critical to life on earth as we know it, since it "blocks UV radiation that can damage living tissue, including plants." (NASA, 2021) The Ozone Monitoring Instrument (OMI) is an international collaborative project that brings together scientists and space agencies to collect data in order to understand how to measure challenges to the ozone layer and to develop countermeasures that are actually effective. It "measures criteria pollutants such as nitrogen dioxide (NO2), sulfur dioxide (SO2), bromine oxide (BrO), and aerosol characteristics … [and] provides mapping of pollution products from an urban to super-regional scale." (NASA, 2022)

Magnetic shield

The earth's magnetic shield is a product of the electrical currents that run through the Earth. Also known as the "magnetoshield," it is a critical protective barrier shielding the Earth from sunspots and other radiative hazards. Figure 11-14 portrays an artistic conception of the magnetosphere.

Figure 11-14 Portrays An Artistic Conception Of The Magnetosphere



Source: (Buis, 2021)

The magnetosphere is constantly changing, however, because the molten core of Earth, which generates the currents that create the magnetic north and south poles, is constantly moving and even occasionally flipping over. The more immediate issue is when space weather causes "geomagnetic storms that can penetrate our atmosphere, threatening spacecraft and astronauts, disrupting navigation systems and wreaking havoc on power grids." (Buis, 2021) Monitoring the magnetosphere can provide some advance warning of such events as well as contribute to our understanding of how the greater system works. Satellites are crucial to this effort. One such effort is from the European Space Agency, which launched a 3 satellite "Swarm constellation [to provide] new insights into the workings of Earth's global magnetic field." (Buis, 2021)

References

Buis, A. (2021, August 3). *Earth's Magnetosphere: Protecting Our Planet from Harmful Space Energy*. Retrieved August 12, 2022, from NASA Global Climate Change: https://climate.nasa.gov/news/3105/earths-magnetosphere-protecting-our-planet-from-harmful-space-energy/

CSIS. (2017, November 30). *Popular Orbits 101*. Retrieved August 7, 2022, from Aerospace Security: https://aerospace.csis.org/aerospace101/earth-orbit-101/

ESA. (2016, November 18). *New map offers precise snapshot of human life on Earth*. Retrieved August 12, 2022, from ESA Observing the Earth: https://www.esa.int/Applications/Observing_the_Earth/New_map_offers_precise_snapshot_of_human_life_on_Earth

ESA. (2021, January 19). *ESA-developed Earth observation* *missions*. Retrieved August 8, 2022, from European Space Agency: https://www.esa.int/Applications/Observing_the_Earth/Earth_observing_missions

ESA. (2021, November 11). *Mapping our human footprint from space*. Retrieved August 12, 2022, from ESA Observing the Earth: https://www.esa.int/Applications/Observing_the_Earth/Mapping_our_human_footprint_from_space

ESA. (2021, June 26). *New Sea-level Monitoring Satellite Goes Live*. Retrieved August 12, 2022, from ESA / Applications / Observing the Earth / Copernicus / Sentinel-6: https://www.esa.int/Applications/Observing_the_Earth/Copernicus/Sentinel-6/New_sea-level_monitoring_satellite_goes_live

Group on Earth Observations. (n.d.). *About Us*. Retrieved August 8, 2022, from Group on Earth Observations: https://www.earthobservations.org/geo_community.php

Holzinger, M. J., Chow, C. C., & Garretson, P. (2021, May 3). *AFRL Portal*. Retrieved August 7, 2022, from A Primer on Cislunar Space: https://www.afrl.af.mil/Portals/90/Documents/RV/A%20Primer%20on%20Cislunar%20Space_Dist%20A_PA2021-1271.pdf?ver=vs6e0sE4PuJ51QC-15DEfg%3D%3D

Howell, E. (2017, August 21). *Lagrange Points: Parking Places in Space*. Retrieved August 7, 2022, from Space.com: https://www.space.com/30302-lagrange-points.html

Hudson, K. E. (1990). *Communications Satellites: Their Development and Impact.* New York, NY: Macmillan Inc.

Indian Space Research Organization. (n.d.). *Earth Observation Applications*. Retrieved August 8, 2022, from Indian Space Research Organization: https://www.isro.gov.in/earth-observation/applications

Jones, A. (2022, July 1). *China launches new Gaofen 12 Earth observation satellite*. Retrieved August 8, 2022, from Space.com: https://www.space.com/china-launches-gaofen-12-satellite

JPL. (2001, November 3). *Joint Propulsion Lab*. Retrieved August 9, 2022, from Seals, Sea Lions and Satellites: https://www.jpl.nasa.gov/news/seals-sea-lions-and-satellites

NASA. (2010, November 9). *Global View of Fine Aerosol Particles*. Retrieved August 12, 2022, from NASA Earth Observatory: https://earthobservatory.nasa.gov/images/46823/global-view-of-fine-aerosol-particles

NASA. (2010, September 22). *New Map Offers a Global View of Health-Sapping Air Pollution*. Retrieved August 12, 2022, from NASA Earth Observatory: https://www.nasa.gov/topics/earth/features/health-sapping.html

NASA. (2010, April 1). *TIROS, the Nation's First Weather Satellite*. Retrieved August 6, 2022, from NASA History: https://www.nasa.gov/multimedia/imagegallery/image_feature_1627.html

NASA. (2012, April 9). *NASA Views Our Perpetual Ocean*. Retrieved August 9, 2022, from NASA:

https://www.nasa.gov/topics/earth/features/perpetual-ocean.html

NASA. (2016, September 16). *Sea Ice*. Retrieved August 9, 2022, from NASA Earth Observatory: https://earthobservatory.nasa.gov/features/SeaIce/page1.php

NASA. (2017, October 26). *A River of Rain Connecting Asia and North America*. Retrieved August 12, 2022, from NASA Earth Observatory: https://earthobservatory.nasa.gov/images/91175/a-river-of-rain-connecting-asia-and-north-america

NASA. (2021, June 23). *Earth Observing System Project Science Office*. Retrieved August 8, 2022, from NASA: https://eospso.nasa.gov/content/nasas-earth-observing-system-project-science-office

NASA. (2021, April 15). *NASA-Built Instrument Will Help to Spot Greenhouse Gas Super-Emitters*. Retrieved August 12, 2022, from NASA: https://www.nasa.gov/feature/jpl/nasa-built-instrument-will-help-to-spot-greenhouse-gas-super-emitters

NASA. (2021, August 25). *Protecting the Ozone Layer Also Protects Earth's Ability to Sequester Carbon*. Retrieved August 12, 2022, from NASA: https://www.nasa.gov/feature/goddard/esnt/2021/protecting-the-ozone-layer-also-protects-earth-s-ability-to-sequester-carbon

NASA. (2021, October). *Satellites View California Oil Spill*. Retrieved August 9, 2022, from NASA Earth

Observatory: https://earthobservatory.nasa.gov/images/148929/satellites-view-california-oil-spill

NASA. (2022, July 22). *50 Years of Landsat*. Retrieved August 6, 2022, from NASA History: https://www.nasa.gov/image-feature/50-years-of-landsat

NASA. (2022). *Aqua Earth-observing Satellite Mission*. Retrieved August 8, 2022, from NASA Earth Observing Systems: https://aqua.nasa.gov

NASA. (2022). *NASA Covers Wildfires Using Many Sources*. Retrieved August 12, 2022, from NASA Earth Observatory: https://www.nasa.gov/mission_pages/fires/main/missions/index.html

NASA. (2022). *Ozone Monitoring Instrument (OMI)*. Retrieved August 12, 2022, from NASA Aura: https://aura.gsfc.nasa.gov/omi.html

NOAA. (2011, August 1). *Ocean Currents*. Retrieved August 9, 2022, from National Oceanic and Atmospheric Administration (NOAA): https://www.noaa.gov/education/resource-collections/ocean-coasts/ocean-currents

Pacific Marine Mammal Center. (2019, January 2). *Satellite Tracking*. Retrieved August 12, 2022, from Pacific Marine Mammal Center: https://www.pacificmmc.org/satellite-tracking

Parker, J. S., & Anderson, R. L. (2013, July). *Transfers to Low Lunar Orbits*. Retrieved August 7, 2022, from JPL DESCANSO Book Series: https://descanso.jpl.nasa.gov/

monograph/series12/
LunarTraj–05Chapter4TransferstoLowLunarOrbits.pdf

Patel, K. (2019, March 1). *5 Stories from 5 Years of Precipitation Measurements from Space*. Retrieved August 9, 2022, from NASA Earth Observatory: https://earthobservatory.nasa.gov/blogs/earthmatters/2019/03/01/5-stories-from-5-years-of-precipitation-measurements-from-space/

Preston, S. (2022, April 26). *Monitoring River Flushing And Hydropower From Space*. Retrieved 2022, from Planet Pulse: https://www.planet.com/pulse/monitoring-river-flushing-and-hydropower-from-space/

Temming, M. (2021, January 21). *Space Station Detectors Found the Source of Weird 'Blue Jet' Lightning*. Retrieved August 12, 2022, from Science News: https://www.sciencenews.org/article/space-station-detectors-found-source-weird-blue-jet-lightning

The Space Option. (2012, October 1). *Cislunar Space*. Retrieved August 7, 2022, from The Space Option: https://thespaceoption.com/portfolio/cislunar-space/

World Health Organization. (2022). *Air Pollution*. Retrieved August 12, 2022, from WHO Health Topics: https://www.who.int/health-topics/air-pollution#tab=tab_1

World Meteorological Organization. (2022, February 1). *WMO certifies two megaflash lightning records*. Retrieved August 12, 2022, from World Meteorological Organization:

https://public.wmo.int/en/media/press-release/wmo-certifies-two-megaflash-lightning-records

Zolli, A. (2018, December 10). *Monitoring Human Rights from Space* . Retrieved August 12, 2022, from Planet: https://medium.com/planet-stories/monitoring-human-rights-from-space-a07b0a8cb613

12.

HUMANITARIAN USE OF SPACE TECHNOLOGIES TO IMPROVE GLOBAL FOOD SUPPLY & CATTLE MANAGEMENT (LARSON)

Student Learning Objectives

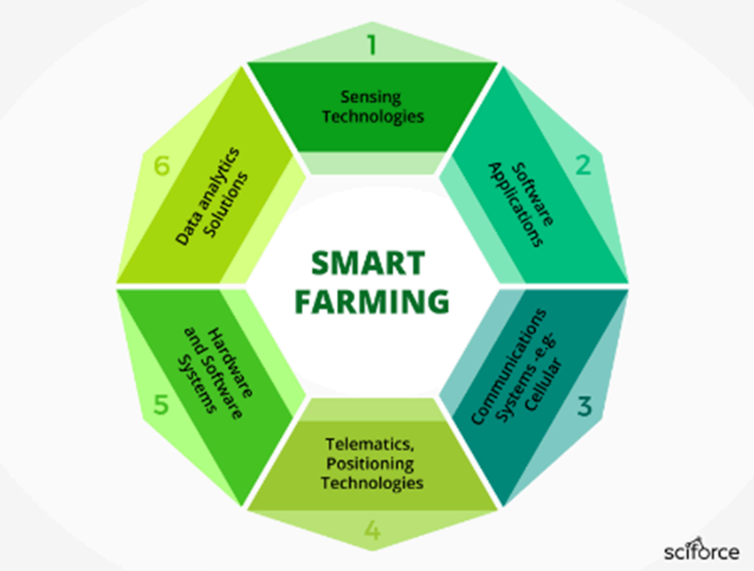
The student will gain an understanding of how space technologies are being used to improve global food supply and cattle management. Concepts discussed include using space technologies for surveying and mapping, environmental stewardship, animal health, and filling labor voids in modern agriculture.

History of space technology used for agriculture

The development of human civilization occurred alongside the discovery of agricultural practices. As humans drifted away from the hunter-gatherer lifestyle, they developed science of growing and harvesting food. This shift in food accessibility allowed humans to produce food for a growing urban environment. Through the years, the labor-intense lifestyle of traditional agricultural practices has deterred people from the field. This labor shortage has presented itself as a barrier to increasing the food supply.

The demand for improved agricultural practices paved the way for the rise of smart agriculture. Smart agriculture is defined as the integration of innovative farming technologies used to increase the quantity and quality of agricultural products (Goel & Yadav, 2021). The movement is based on three platforms: science, innovation, and space technology. For smart agriculture to be successful, sensing technologies, software applications, communication systems, positioning technologies, hardware and software systems, and data analytics solutions must align for the enhancement of the food product supply system (Figure 12-1).

Figure 12-1. Components of a successful smart farming initiative


1
Sensing Technologies
2
Software Applications
3
Communications Systems -e.g- Cellular
4
Telematics, Positioning Technologies
5
Hardware and Software Systems
6
Data analytics Solutions
SMART FARMING
sciforce

Source: (Sciforce, 2020)

Although few space technologies exist in the current market space without connections to these mentioned facets of smart agriculture, it is important to note that historically, it was not always the case. For example, the first satellite developed for remote sensing applications in the agricultural space is known as LANDSAT 1. The LANDSAT 1 satellite, launched by NASA, was used in agriculture to collect data estimating biomass (Yang, 2020) and crop output (Doraiswamy & Moulin, 2003). Although the implementation of this satellite in the agricultural space was revolutionary for the field of agriculture, its use had limitations. Limitations included spatial resolution of the imaging system, return visit frequency and a number of spectral bands available for analysis, and lacking integration of multiple remote sensor inputs. It did not consider input from sensors gathering data on soil monitoring (Sullivan & Shaw, 2005), water stress management (Zarco-Tejada, 2012), weed infestation (Gómez-Casero & Castillejo-González, 2010), chlorophyll and nitrogen content of leaf, crop height, plant species and growth rate (Castillejo-González, 2009); (Donoghue, 2007); (Enclona, 2004); (Peña-Barragán, 2008)). Other countries, such as India, saw the benefits of using space technology like LANDSAT for agricultural purposes and launched their satellites regardless of the limitations.

Integration of multiple sensor inputs presented a monumental shift in the application of space technology for agricultural purposes. A multiple sensor approach enhances output precision to capture better the multi-factor decision-making process food producers are tasked with. Applications in the agricultural space began to demand more than remote sensing platforms like satellites and unmanned aircraft vehicles (UAV). Integration of remote sensors (for example, optical and near-infrared (NIR) sensors or radio detection and ranging (RADAR)) changed the potential for what information the remote sensing platforms could deliver to the producer. In addition, spatial resolution improved, and return frequency increased, allowing satellite platforms to gather more data with increased accuracy. The shift from basic image gathering toward data analysis of multiple sensor inputs defines the needs of the precision agriculture movement. By enhancing the precision and effectiveness of agricultural practices, food producers are enabled to optimize environmental conditions to maximize crop yield, resulting in more food production per unit of land.

Key areas of success in implementing space technology in agriculture

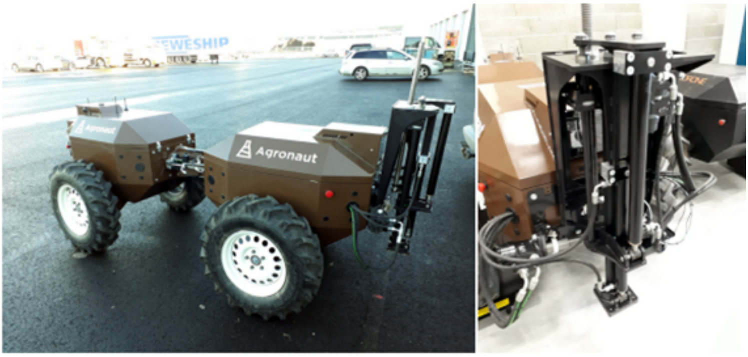
Those involved in the agriculture industry have prided themselves on being stewards of the land for generations. Farmers take pride in understanding that "today's generation must protect and nourish the environment for the betterment of today and tomorrow's generation" (Bansod & Singh, 2017). Implementation of space technology, in particular, the partnership of satellite remote sensing and proximal remote sensing, provides opportunities for increased food production using methods that work to enhance previous land stewardship practices. This section will discuss key areas of success when implementing space technology into the field of agriculture in two loose groups: geographical information systems and remote sensor monitoring (specifically applications of on-farm weather sensors).

Geographical information systems – Surveying and mapping

Geographical information systems (GIS) represent the original implementation of space technology in the field of agriculture. The use of satellites and UAVs for monitoring in the agricultural space continues to emerge as technologies that can deliver value to the food production industry enter the market space. Three categories loosely define areas of success for current and emerging GIS technologies with application to agriculture: surveying and mapping, environmental pollutant monitoring, and circumventing labor challenges in agriculture.

Surveying and mapping capabilities have been greatly refined since the original days of LANDSAT 1. The big-picture perspective of satellite imagery has long exercised its effectiveness in creating topographical maps of remote agricultural regions. With the additions of proximal GIS technology such as UAV and multiple sensor inputs into these GIS technologies, capabilities to deduce more than the basic topographical map has emerged. Multiple data inputs provide insight to geographically inform the producer on variations in soil type and quality, water saturation, and plant density. Unmanned ground vehicles (UGV) have been designed to autonomously navigate agricultural regions using GPS coordinates while pulling samples and relaying information on present conditions. Figure 12-2 shows a UGV prototype developed specifically for automated soil sampling to examine nutrient content's presence and deduce the need for fertilizer and water within the designated sampling region (Vaeljaots, 2018). Understanding the nutrient presence, soil type, and water holding capacity better enables producers to understand the needs of their agricultural region by providing information to describe how many plants that plot of land can support. This cascades to many decisions made by the producer during the food growing period, such as how close to place seeds when planting, how much water is needed to be applied using irrigation technology, and whether or not additional fertilizer needs to be applied to support plant growth nutritionally.

Figure 12-2. Unmanned ground vehicle designed for autonomous soil sample collection by Estonian University of Life Sciences



Source: (Vaeljaots, 2018)

Data analytics are used to aid the decision process in smart agriculture. Analysis of the various sensor/sampling outputs is sequentially inputted into satellite mapping to create management zones that may use different strategies (for fertilizer application, water requirements, or pesticide application) to maximize crop yields in that area.

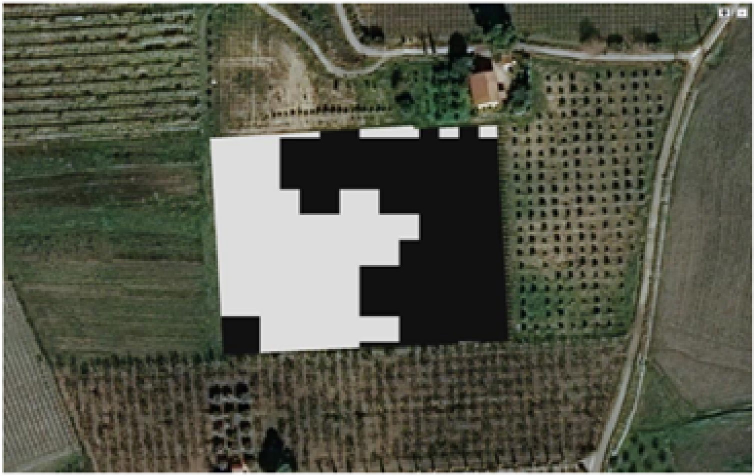
Although the use of UAV and UGV is likely to continue in the agricultural space for the collection of field-specific data, satellite technology has the potential to limit the complexity of data collection protocols (e.g., number of sensor inputs) if the image quality provided has proven computationally stable to provide the insight required (Meyers & Dokoozlian, 2020). Determining which imagery platform is used (Satellite or UAV/UGV) depends largely on spatial accuracy needs and consumer willingness to pay. When equipped properly, UAV/UGV has demonstrated an ability to deliver high spatial accuracy and is effective for surveying smaller target regions. However, there has been less development to date on standardized procedures in the data analytics space. In comparison, satellite imagery is generally lower resolution, but satellite capabilities to revisit in equally spaced intervals without weather restrictions (e.g., wind, precipitation) that negatively impact UAV (except for cloud level factors) to provide consistent autonomous data (Comparetti, 2022).

Emerging technologies integrating data from UAV/UGV sensors with satellite mapping capacities are gaining interest in the precision agriculture market space. Variable Rate Technology (VRT) allows producers to customize the application of fertilizer, seed planting density, irrigation quantity, and pesticide applications to the sensor-identified needs of the sampled agricultural region. Satellites play a critical role in producing within-field maps to create the spatially variable rate input application maps to be used by

GPS monitored equipment (see Figure 12-3; (Comparetti, 2022) allowing UAV/UGV to provide additional sensor inputs to define the agricultural region. By identifying regions requiring alternative management conditions, food producers can better maximize the quality and quantity of the food grown in those regions. In certain regions, the automated characterization of specific management needs could mean producing a more uniform crop and maximizing the profit of high-value food products, while in other regions of the world could be the difference for a population attempting to produce enough food to sustain themselves through non-growing seasons. The global implications of GIS technologies for surveying designated agricultural regions present unique opportunities in the agricultural sector to enhance global food supply – quantitatively and qualitatively, depending upon the designated market. As the market for connected sensors connected to GIS technologies continues to grow, the "smart agriculture" movement and enhancement of space technologies for agricultural applications will continue to provide novel solutions for increasing global food supply in a way that maintains the expectation for land stewardship set forth by generations of farmers before.

Figure 12-3. Spatially variable rate fertilization map in a Sicilian vineyard developed using Sentinel-2 Satellite. Two management zones are represented: black cells representing areas of high vegetative vigor and

high-water content; white cells representing areas of low vegetative vigor and low water content.



Source: (Comparetti, 2022)

Geographical information systems – Environmental Stewardship

Emphasis placed on the importance of environmental stewardship by food producers ensures technological advancements using GIS technology for monitoring environmental pollutants will be a continuous field of interest. Various laws highly regulate agriculture in the United States, acts, and guidance documents encompassing many facets of agricultural operations (United States Environmental Protection Agency, 2022). Regulation exists for aquaculture discharges; concentrated animal feeding operations' water use and manure disposal; cropland pesticide application and use; farm facilities, fuel, and equipment compliance; and a few.

The satellite used for emissions detections is currently being used in many facets: climate, natural disasters, health, and air quality, water resources, and others. Models such as the United States Environmentally-Extended Input-Output model (USEEIO) used by the EPA "melds data on economic transactions between 389 industry sectors with environmental data for these sectors covering land, water, energy, and mineral usage and emissions of greenhouse gases, criteria air pollutants, nutrients, and toxics, to build a life cycle model of 385 US goods and services" (Yang, 2020). Efforts by EPA have begun to automate the environmental compliance inspections by deploying unmanned aircraft systems (UAS) technology equipped with high-resolution imagery, geophysics and remote sensing, and gas sensors. Data from sensor-equipped UAS is transmitted in real-time using the ERT VIPER monitoring system for data analysis and visualization by the user (United States Environmental Protection Agency., 2022).

With the EPA using this level of detail in their risk-benefit-based analysis, the agricultural industry must maintain a high level of control on agricultural operations related to regulated activities. Activities in particular that demand increased precision are the application of pesticides to cropland, application of inorganic fertilizer as well as manure based on nutrient quantity, and irrigation of crops. The use of UAV technology for applying pesticides, especially when integrated with VRT using satellite GIS mapping, provides food producers with valuable tools to maintain compliance by only targeting areas infected with pests or where the disease is present. Figure 12-4 depicts an example of leading-edge aerial technologies pesticide applicator UAV. Hurdles for initial vehicle system development of this emerging technology described the weight of the pesticide solution as challenging for the UAV to carry and influencing vehicle control. Therefore, the integration with spatial GIS mapping for VRT was monumental for reducing the total quantity of products needing to be applied in the field. The use of VRT to guide UAV pesticide application serves as a benefit for both reducing environmental pollutants and decreasing costs for the producer, all while increasing crop yields due to pest and disease management (Hafeez, 2022). The ease of implementation decreased human exposure to chemicals, and increased product effectiveness with less environmental contamination has made producer uptake of this product successful. The global market size for agricultural drones in 2020 is estimated to be USD 0.88 billion, with projections supporting the market reaching USD 5.89 billion by 2030 (Wankhede, 2021).

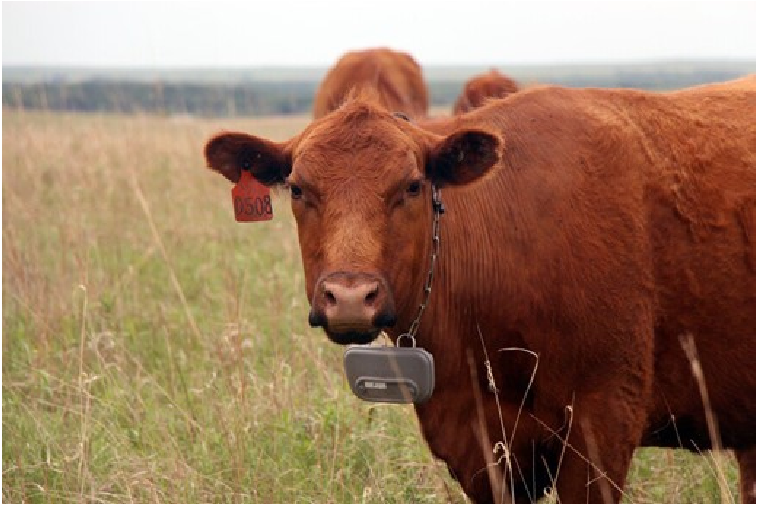
Figure 12-4. Image of Precision Vision 35X as an example of an unmanned air vehicle (UAV) with pesticide application abilities in the agricultural space

Source: (Reynolds, 2022)

Beyond pesticides, another area of stewardship that farmers have long been concerned about is fertilizer management. While fertilizer application using technology equipped with VRT drawing from satellite mapping and GPS control is present in the market and readily available by service providers. Estimates of adoption were 81% of producers in the United States applying single nutrients using VRT technology in 2017 (Lowenberg-Deboer, 2019). The critical point to highlight concerning the success of VRT inorganic fertilizer application is the concept that each nutrient is being applied individually. Growing crops to maximize yield requires a specific ratio of nitrogen, phosphorous, and potash, which can vary based on the type of crop the producer intends to plant that year. When applied individually, the producer can calculate the need for each nutrient to be added based on what nutrients are present in the soil samples. However, when working with more complex fertilizer sources, such as manure or compost, where all three required nutrients are present, producers must apply based on the soil's need for one of those nutrients. So there may be an over or under abundance of one of the other two nutrients. This adds a level of complexity when studying the effectiveness of VRT for manure applications. The variation in the success rate of meeting crop nitrogen needs has been explained as one of the reasons for the limited uptake of the technology in the livestock manure space. Still, phosphorus data has been promising (Mallarino, 2010). Equipping UAVs with emerging imaging and sensor technology capable of correlating plant nitrogen status to projected grain yield adds versatility for producers looking to apply manure or inorganic fertilizer (Maresma & Ariza, 2016). In the *Geographical information systems – Surveying and mapping* section of this chapter, the use of UGVs for collecting soil samples integrating with GIS mapping capabilities was described. It's important to note the environmental stewardship story when using space technology's role in UGV soil sampling paired with satellite map creation. Most obviously, when mapping capabilities are integrated with multisensory inputs (such as soil analysis, water content, etc.) and used for variable rate application of fertilizer and water improvement, the efficiency of the tillable land is increased. Within the constraints of the earth's atmosphere, the quantity of tillable land has little room for drastic increases without other severe environmental impacts. Therefore, an increase in tillable land efficiency should be considered an exceptional benefit to feeding the growing world population.

However, the land stewardship story extends beyond increasing efficiency and yield. The big picture capabilities to create a map conscious of the environment surrounding the agricultural region help food producers better integrate solutions for limiting erosion, protecting endangered ecosystems, as well as understanding sources of fertilizer runoff into the surrounding natural ecosystem. Conservation groups are partnering with cattle producers to understand better the stewardship story that space technology is creating on the Kansas Prairie. Third-generation rancher Daniel Mushrush joined a nature conservancy project partnered with Kansas State University to explore the application of emerging space technology to cattle management for two main reasons: labor and maintenance challenges with traditional fences as well as a "moral obligation to treat [Flint Hills grass] like it's sacred. Because it is. There's not much left." (Llopis-Jepsen, 2022). The initiative examines emerging technology that uses GPS technology to create virtual cattle fences. The project's goals are to evaluate: "whether the devices can save ranchers money and simultaneously help ailing bird populations, reduce water pollution and increase the resilience and diversity of grasslands" (Llopis-Jepsen, 2022). Figure 12-5 depicts a cow from Mushrush's herd wearing a GPS-equipped collar that guides the animal using satellite-derived GIS mapping technology (Llopis-Jepsen, 2022). Using this technology, cattle producers have the ability to set and move virtual fences to consider the stage of grass growth (i.e., food availability for cattle), accommodate the presence of disappearing species (e.g., prairie chickens), reduce the number of time cattle spend near bodies of water (i.e., reduce erosion induced by cattle trampling riverbanks), and various other applications depending upon cattle operation.

Figure 12-5. Red Angus cow wearing a GPS-equipped collar that responds to virtual fencing boundaries created using satellite-derived geographical information systems maps controllable virtually by the cattle producer



Source: (Llopis-Jepsen, 2022).

In an interview with Ben Veres, Chief of Staff, and Jeff Kafka, Director of Sales and Business Development for Vence, sustainability was mentioned as the greatest area of impact from using space technologies like virtual fencing. "Minute-by-minute GPS data can be paired with soil and vegetation data to paint an incredibly rich picture of the impacts of cattle on the landscape. There is often a lot of blame placed on livestock for grassland degradation – but without real cattle location data, the analysis is one-sided" (Veres, 2022). Opportunities for the use of virtual fencing technology were forecasted to evolve in 3 phases: Tracking (i.e., GPS location of animals), fencing (i.e., reducing physical fencings limitations and decreasing cost and labor), and animal health (which will be further discussed later in section: *Integration of space technology into cattle management*). Veres and Kafka state, "All of these things combined can create a much richer feedback cycle for the rancher – not only can they see where and how their cattle are doing, but they can easily adjust the cattle's grazing plans and monitor the impacts of these changes. The feedback cycle is also much shorter – on large ranches, some cattle will go months between check-ins. This technology allows ranchers to be closer with their animals" (Veres, 2022). With regulative agencies like EPA incorporating space technology into the surveillance of environmental stewardship practices, emerging technologies like virtual fencing arm food producers with the power of knowledge to accurately diagnose and provide solutions for environmental challenges in their operations.

Geographical information systems – changing labor force in agriculture

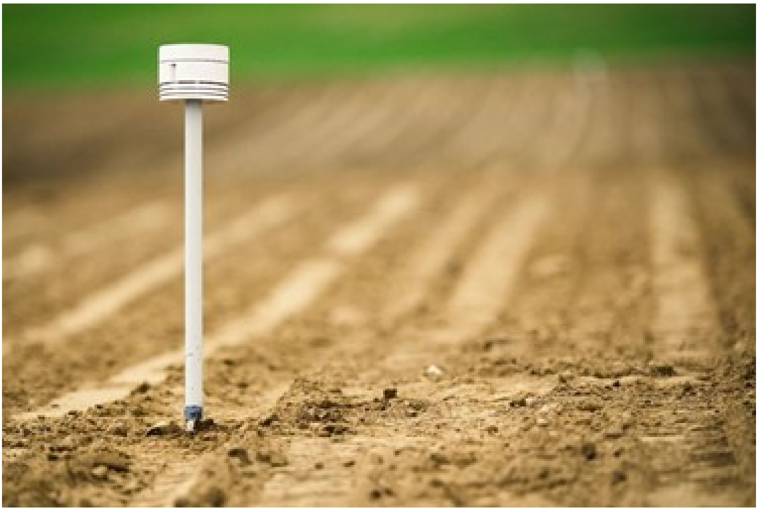
Ryan Cryan, a chief economist for the American Farm Bureau Federation, captures the industry status well with his statement, "American Agriculture has every resource to grow and prosper and contribute to global food security – except for labor" (Bacon, 2022). The disappearance of the family farm, decrease in interest in the rural lifestyle and increase in mechanization contribute to the 76% reduction in self-employed and family farm workers seen between 1948 and 2017 (Wang, 2022). However, data also suggest that agricultural output increased by nearly 187% (Wang, 2022). Much of this success can be attributed to developments in technology. Precision technology reduces labor hours of the agricultural workforce for labor-intensive tasks while opening opportunities for skilled labor to enter the agricultural space in other ways (e.g., to maintain and operate implemented technology). In 2017, 40% of farm labor hours worked were executed by workers with at least some college education, compared to 4% in 1950 (Wang, 2022). Implementation of autonomous and semi-autonomous GPS monitoring equipment has been one of the most widely recognized successes in this area. While John Deere's autonomous tractor reveal in 2022 still has space reserved for a driver, it will no longer require a driver presence to operate its desired tasks. Automating tasks such as preparing the ground for planting and, perhaps one day, even more complex tasks such as planting or harvesting play a large role in helping change the labor force required in agriculture. In the livestock space, similar emerging technologies are entering the market space. Still, as a whole, the industry is behind the crop production sector due to challenges with the costs of implementation. Examples of technology emerging in the livestock space will be provided later in this chapter in the section: *Opportunities for integration of space technology into cattle management.*

Regardless of the agriculture industry sector to which these emerging technologies are applied, they play a key role in removing barriers to human labor requirements, increasing the accuracy of planting and harvesting, and improving the efficiency of time spent on tasks. These contributing factors are convincing evidence for demonstrating how emerging precision technology adds value to the agricultural industry and increases the global food supply.

Remote sensors for weather monitoring

Since the Farmer's Almanac, the impact of weather on food production has been heavily respected in agriculture. With the increasing uptake of smart agricultural practices, a growing interest by both producers and agricultural tech companies in personalizing weather-related information to specific agricultural operations emerged. Personalization of weather-related data has significant value to food producers, especially for rural locations where the closest weather tower collecting information may not be pertinent for real-time weather-related challenges. Implementing on-site weather sensors provides food producers with information that can optimize irrigation schedules and determine the best timing to plant and apply fertilizer. Figure 12-6 shows an in situ weather sensor marketed by OneSoil with capabilities to monitor soil temperature and moisture as well as air, barometric pressure, and illumination every 2 to 30 min on the farm (Timmermans, 2022).

Figure 12-6. OneSoil Agricultural in-ground weather sensor monitors soil moisture and temperature



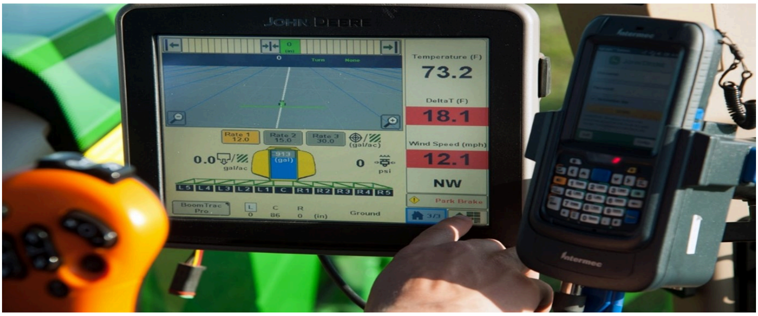
Source: (Timmermans, 2022)

Beyond using this technology as a stand-alone offering to producers, perhaps more valuable is the integration of weather sensors into data analytics platforms for interpretable producer outputs. Agricultural giant John Deere has demonstrated this value with their mobile weather technology. This sensor technology (Figure 12-7) feeds information to the producer interface (Figure 12-8) to guide the equipment when applying crop protectants according to regulations and maintain compliance and quality record keeping (John Deere., 2022).

Figure 12-7. John Deere Mobile weather sensor technology mounted on the hood of self-propelled sprayer

Source: (John Deere., 2022)

Figure 12-8. John Deere mobile weather technology user interface



Source: (John Deere., 2022)

The value of real-time recognition of weather events can prove extremely valuable to food producers, especially when coupled with personalized data analytics output, measurements of wind speed and direction, temperature, humidity, rainfall, and on-farm producers with the knowledge to maintain environmental compliance standards and put emergency preparedness plans into place if necessary. For livestock producers, in particular, storm management plans are a key tool to maintain animal welfare standards when technology cannot overcome the forces of nature (e.g., power outages, significant snowfall or flooding, high winds, or significant heat events). Food producers in the livestock space are obligated to their animals, extending beyond whatever mother nature throws them. Standardization of data analytics procedures with recognizable producer indices, such as the Livestock Weather Safety Index (LWSI), allows universal use and interpretation of remote weather sensor technology data (Mader, 2006).

Integration of space technology into cattle management

Much like many of the agricultural solutions presented in this chapter, space technologies used in cattle management also rely on incorporating multi-sensor inputs for successful integration into the market space. Like crop and produce production, cattle management practices present numerous opportunities for emerging space technologies to impact the industry. Space technology has opportunities for success in the cattle industry because:

1. Animals are primarily housed in outdoor areas (e.g., satellite and UAV technologies can access the region with limited interference)
2. Industry labor shortages with limited automation present (e.g., unlike the skilled labor shift that's occurred in other parts of agriculture, the lack of basic laborers has forced skilled laborers to be used inefficiently for more entry-level roles rather than what they were trained for)

3. Complex animal health concerns (e.g., complex pathogens like those causing Bovine Respiratory Disease can be challenging to identify during ideal treatment windows)
4. Navigation of environmental regulations (e.g., Regulations for manure and water are monitored closely in the cattle industry)
5. Longer time to market and greater monetary value of an individual animal compared to other livestock (e.g., the longer period spent in the feedlot presents a greater risk for something happening to a high-value animal)

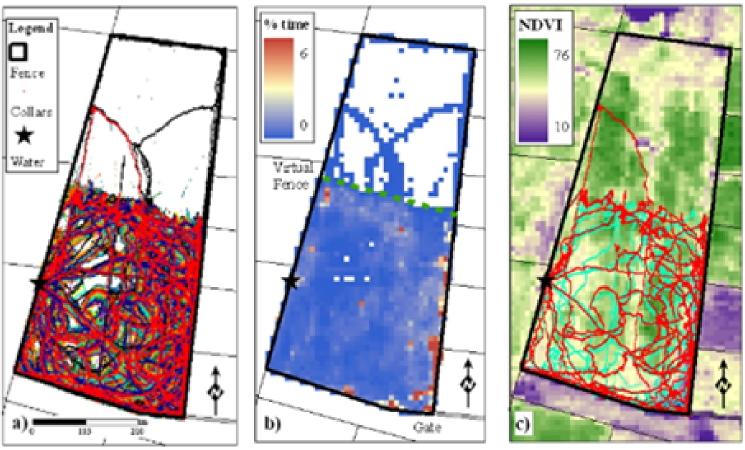
Although there is room in the market for developing technologies to assist the cattle industry, skepticism does plague this industry due to high investment costs. Therefore, understanding and demonstrating the valued added proposition of emerging technologies in this space is critical for developers. This section will focus on three key areas of space technology development for cattle management: satellite systems, remote health sensors, and feed management equipment. The technology mentioned in this section is not an exhaustive list and includes examples of both space-based technologies and remote sensors for integration with space technology offerings.

Emerging cattle management technology: satellite systems

Satellite systems have two main functionalities explored most commonly with application to cattle management: GPS monitoring and imagery. The direct use of GPS monitoring cattle via the virtual fencing industry has been described earlier in the section: *Geographical information systems – Environmental Stewardship.* It is important to emphasize that despite its implications for environmental stewardship, for virtual fencing to continue uptake by industry producers, it must continue to demonstrate value to cattle feeding operations monetarily. Eliminating costs of labor and supplies for fence management is a key benefit, especially for cattle grazing in the remote country when human access is challenging. Another potential output of the technology that broadly opens the targeted market is the recognition of cattle movement for animal health purposes. Changes in movement patterns of animals could detect calving status, disease presence, or dangerous threats (e.g., predator, environmental barriers, etc.). Access to this information helps cattle producers understand when intervention is necessary (Handcock, 2009).

GPS technology application to animals is arguably not in its infancy in the market like other technologies discussed in this chapter. GPS technology has been applied to animals since its emergence in the citizen space, specifically for ecologists' and conservationists' use in tracking terrestrial wildlife. But, commercialization of the technology for cattle has since accelerated the development of its capabilities beyond simple measurements to include animal behavior inferences (e.g., grazing, traveling, and resting activities) (Ungar & Henkin, 2005). Correlation of herd movement and activity with satellite imagery to predict biomass available using standardized vegetation indices (VI) provides producers even more information on decisions herds are making and where they are choosing to spend their time, especially for animals grazed in remote locations (Figure 12-9; (Handcock, 2009)).

Figure 12-9. (a) Movement of 36 cattle over three days in GPS-monitored paddock. (b) percentage of time spent in the region represented by pixel in satellite image (c) overlay of movement of cattle with normalized difference vegetation index (NDVI)



Source: (Handcock, 2009)

Data analytics have taken the interpretation of these satellite images a step further. Live weight gain prediction capabilities have been explored for cattle grazing paddocks using satellite-derived VI data as primary data input for the model (Pearson, 2021). There is great value for cattle producers to understand the biomass available. Knowing the quantity of vegetation available for grazing (and the potential to translate to an animal weight change) provides the cattle producer with an understanding of when additional management interventions (e.g., supplemental feed during dry season) are needed.

Emerging cattle management technology: remote health sensors

The ability to identify animals feeling unwell within the treatment window to ensure disease will not have lasting impacts on that animal's life is truly an art. Finding (and retaining) labor with this valuable skill set in the cattle industry is proving harder than the art itself. In response to this animal welfare concern, agriculture technology companies and animal health companies have partnered to develop a variety of sensors that can simplify disease detection methods. "There will always be a need for skilled producers to engage with and deeply understand the cattle they are raising. No technology will replace the need for ranchers to get their hands dirty. Rather these technologies will be tools that will assist them in those efforts" (Veres, 2022). QuantifiedAg Tag is part of the SenseHub customer offering by Merck Animal Health. The smart tag (Figure 12-10) measures temperature and animal activity and has an LED indicator light on a tag to easily identify animals for treatment (Armstrong, 2016). The information collected by sensors built into the animal's ear tag is relayed to a user interface where a list of animals needing treatment is located. To ease cattle handling, animals with values outside baseline for temperature and activity trigger an LED light on the ear tag making sick animal identification much more straightforward for cattle operation workers.

Figure 12-10. QuantifiedAg Tag measures animal temperature and activity level to provide inputs for the producer interface, where a list of sick animals to treat is generated. The indicator light on the tag identifies which animals need treatment.

Source: (Armstrong, 2016)

MOOnitor is a collar equipped with sensors for measuring resting, feeding, rumination (i.e., chewing cud), head position, and restlessness of each animal, as well as monitoring for optimal breeding time (Figure 12-11). These sensor outputs relay back to the user interface, giving the producer a snapshot of the animal's overall health. The sensitivity of MOOnitor sensors paired with its GPS module for movement tracking has proven to have the accuracy, precision, sensitivity, and specificity for effectively differentiating behaviors such as standing, lying, standing and ruminating, lying and ruminating, walking and walking, and grazing (Dutta, 2022). Effectively recognizing animal movements indicates that these remote health sensor technologies may be very effective in determining cows' optimal breeding time, identifying disease presence, and/or detecting deviation from the herd's baseline health standards.

Figure 12-11. MOOnitor collar is equipped with remote sensors as well as a GPS module for measuring animal movement, feeding, rumination, head position, etc. for monitoring general animal health as well as detecting optimal breeding time for females

Source: (Fox, 2019)

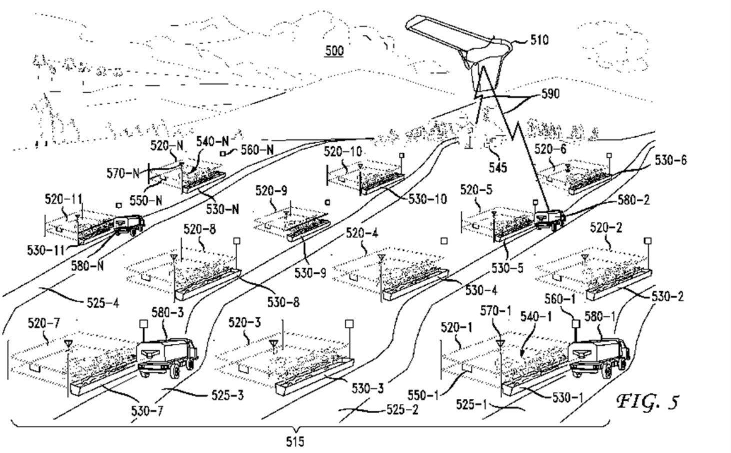
With the animal agriculture industry under a microscope by the public media concerning the treatment of animals and animal health standards, implementing these types of remote sensor technologies will hopefully arm producers with data related to animal welfare standards within their operation. Perhaps most impactful to the cattle producer is these tools' ability to circumvent challenges that exist with skilled labor shortages for on-farm animal health management.

Emerging cattle management technology: feed management equipment

In the beef feedlot sector, a critical role for skilled labor is an employee with the ability to "read bunks" – a process by which the animals' feed trough is inspected for the presence of the previous day's feed offering. Based on the bunk score assigned by the bunk reader, the feed offered to that cattle pen could increase or decrease in the present day. Reading bunks is a time-intensive step in cattle management for large operations with limited labor. The accuracy of the call is also critical as feed costs are the major expense to any cattle operation. The critical nature of this task has piqued the interest of multiple agriculture technology developers. Efforts to develop computer visioning for bunk management with stationary cameras have succeeded with prediction accuracies for detecting the quantity of feed in the bunk (accuracy of prediction ranged from 81.8% to 90%) (Dorea, 2019). Accuracy of prediction of cattle behavior using the same technology resulted in a lower range with increased variability (accuracy of prediction ranged from 66.6% to 86.6%) (Dorea, 2019). However, these results are not surprising. Detection and analysis of a moving target (such as a live animal) is not an easy feat for any technology. Still, it is understood by agricultural workers that understanding cattle behavior at the bunk is just as important as the amount of feed remaining.

A patent granted to Digi Star LLC in 2019 but not yet available in public market space explores the idea of using UAVs equipped with sensor technology to automate bunk reading (Figure 12-12). The UAV sensor output is then relayed back to a feed delivery truck to dispense the intended amount of feed for that group of animals based on the previous day's remaining feed (Patent No. Agricultural drone for use in livestock feeding. In: Google Patents., 2019). Although truly innovative in its field, the delay in development may be limited producer interest in the uptake of UAV technology for critical daily tasks – as weather may create an environment unfit for UAV operations. Still, bunk calls must be made regardless of the weather.

Figure 12-12. Explanatory diagram of the use of unmanned air vehicle (UAV) to determine feed remaining in cattle bunk with capabilities to relay real-time information to feed delivery truck

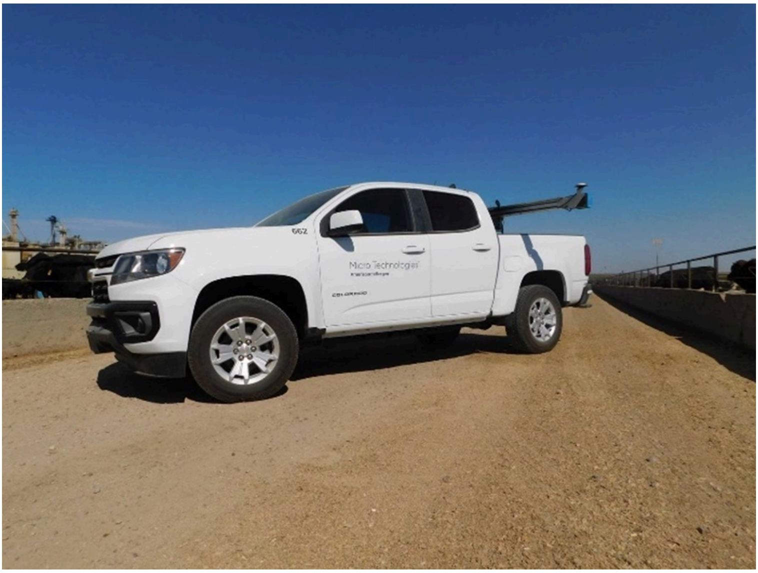


Source: (Patent No. Agricultural drone for use in livestock feeding. In: Google Patents., 2019)

One of the pioneer space technologies in cattle management is the use of GPS guiding feed truck equipment. Micro Technologies launched their first GPS-guided Feed Truck System, integrated with interfacing capabilities between feed truck computer and feed truck scale, in 1998 (Micro Technologies: Our History – Innovation in Motion. , 2022). This technology was revolutionary for decreasing the skill required to accurately deliver the correct amount of feed – saving time and money associated with incorrect feed deliveries. As regulations of in-feed animal drugs have tightened after the passing of the veterinary feed directive, the GPS-monitored Feed Truck System has ensured that drugs are being dispensed to the correct group of animals in the correct amounts – increasing the accuracy of record keeping with regards to animal health drugs.

Micro Technologies continues offering cattle producers at the forefront of precision agriculture. In 2022, they announced the launch of Accu-Trac Vision – a truck-mounted arm with a sensor detecting feed left in the bunk (Figure 12-13). This sensor output relays the bunk call to the feed dispatch center, guiding the feed delivery by GPS-monitored feed trucks. It has not been described whether or not this technology considers animal behavior and the estimated quantity of feed remaining – however, it is viewed as a disruptive technology for the cattle industry because of the opportunities to decrease skilled labor and increase consistency in bunk calls.

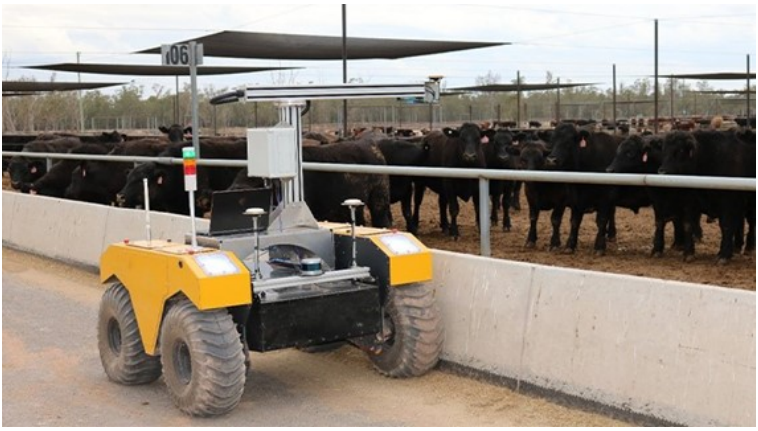
Figure 12-13. Accu-Trac Vision bunk scanner arm for estimating cattle feed remaining from the previous day



Source: (Micro Technologies: Our History – Innovation in Motion. , 2022)

Complete autonomous bunk calling and feed delivery solutions have also emerged in the cattle industry. The Australian-based company, Manabotix, has developed a sensor with bunk reading capabilities similar to Micro Technologies Accu-Trac Vision. This sensor is being tested as part of a UGV for automated robotic bunk calling (Figure 12-14). BunkBot has been well received for allowing skilled labor to be better used in other roles on the feedlot and increasing the amount of data available on animal feed intake.

Figure 12-14 Autonomous unmanned ground vehicle (UGV), BunkBot, equipped with sensor technology for estimating feed remaining in cattle bunk



Source: (McMeniman, 2021)

The selected feed management technology described in this section demonstrates the complex variation of emerging technologies in the cattle feeding management sector. Although these new technologies have captured the interest of producers, product uptake will be heavily dependent upon the product's value proposition and, ultimately, what value cattle producers put on circumventing labor challenges that plague the industry.

Developer considerations for end-user of emerging technology

This chapter highlights emerging technologies in the agriculture industry with connections to space. Although there is no doubt developers are busy innovating in this space, uptake by producers is not consistent across technology types. Automated technologies have shown sooner adoption by food producers after coming to the commercial market than more data-intensive technologies (Ofori, 2020). But data-intensive technologies are the lifeblood of larger applications such as VRT. Uptake of VRT by producers is estimated between 20-30% of American food producers – demonstrating interest on the part of the producer but that perhaps the technology has not yet fully found its value proposition for the food producer (Lowenberg-Deboer, 2019). Value to the producer will always be pivotal to the success of emerging technologies in the agriculture industry. Increasing the quality and/or quantity of food products produced equates to more revenue from food producers. As emerging space technologies continue to navigate the challenges facing the modern agriculture industry, there is no doubt these innovations will profoundly impact the quality and quantity of food producers for the growing population.

Conclusions

As the age of smart agriculture ensues, the toolbox of emerging space technologies appears to be at the cutting edge of industry advancement. The advancing global population, increasing environmental challenges, and (relatively) static tillable acres presents the industry with innovation opportunities to shoot for the stars in an effort to keep up with demand for increased food production. The examples demonstrated in this chapter have provided evidence that original innovators of space technologies may have rarely had the chance to put their theories into agricultural practice themselves; but from the perspective of the agricultural sector, those technologies have the ability to change lives by increasing the quantity and quality of food this world can produce.

References

Armstrong, R. (2016). *Quantified Ag's LED tags light up to identify sick cattle.* . Retrieved from https://siliconprairienews.com/: https://siliconprairienews.com/2016/08/quantified-ag-led-tags-light-up-identify-sick-cattle/

Bacon, S. (2022). Reading the signs: Annual agricultural symposium examines effect of labor shortages on long-term outlook. *Ten Magazine*, pp. 18(1), 28 – 34. doi:https://www.kansascityfed.org/TEN/documents/8874/ten_summer2022.pdf

Bansod, B., & Singh, R. T. (2017). A comparison between satellite-based and drone-based remote sensing technology to achieve sustainable development: a review. *Journal of Agriculture and Environment for International Development*, 11(2), 383-407. doi:https://doi.org/10.12895/jaeid.20172.690

Castillejo-González, I. L.-G.-F.-B.-E.-A. (2009). Object- and pixel-based analysis for mapping crops and their agro-environmental associated measures using QuickBird imagery. *Computers and electronics in agriculture.*, 68(2), 207. doi:https://doi.org/10.1016/j.compag.2009.06.004

Comparetti, A. &. (2022). Use of Sentinel-2 Satellite for Spatially Variable Rate Fertiliser Management in a Sicilian Vineyard. *Sustainability*, 14(3), 1688. doi:https://doi.org/10.3390/su14031688

Donoghue, D. W. (2007). Remote sensing of species mixtures in conifer plantations using LiDAR height and intensity data. *Remote sensing of environment*, 110(4), 509-522. doi:https://doi.org/10.1016/j.rse.2007.02.032

Doraiswamy, P. C., & Moulin, S. C. (2003). Crop Yield Assessment from Remote Sensing. . *Photogrammetric Engineering & Remote Sensing*, pp. 69(6), 665-674. . doi:https://doi.org/10.14358/pers.69.6.665

Dorea, J. R. (2019). PSXI-2 A computer vision system for feed bunk management in beef cattle feedlot. *Journal of animal science.*, 97(Supplement_3), 389-390. doi:https://doi.org/10.1093/jas/skz258.776

Dutta, D. N. (2022). MOOnitor: An IoT-based multisensory intelligent device for cattle activity monitoring. *Sensors and actuators*, 333, 113271. doi:https://doi.org/10.1016/j.sna.2021.113271

Enclona, E. A. (2004). Within-field wheat yield prediction from IKONOS data: a new matrix approach. *International* *journal of remote sensing*, 25(2), 377-388. doi:https://doi.org/10.1080/0143116031000102485

Fox, C. (2019). Dairymaster MooMonitor+ first in class for monitoring cow behavior. *Farming Independent* . doi:https://www.independent.ie/business/farming/agri-business/companies/dairymaster-moomonitor-first-in-class-for-monitoring-cow-behavior-38095157.html

Goel, R. K., & Yadav, C. S. (2021). Smart agriculture – Urgent need of the day in developing countries. *Sustainable Computing: Informatics and Systems*, 30, 100512. doi:https://doi.org/10.1016/j.suscom.2021.100512

Gómez-Casero, M. T., & Castillejo-González, I. L.-F.-B.-E.-T.-G. (2010). Spectral discrimination of wild oat and canary grass in wheat fields for less herbicide application. *Agronomy for Sustainable Development*, 30(3), 689-699. doi:https://doi.org/10.1051/agro/2009052

Hafeez, A. H. (2022). Implementation of drone technology for farm monitoring & pesticide spraying: A review. *Information Processing in Agriculture*. doi:https://doi.org/10.1016/j.inpa.2022.02.002

Handcock, R. S.-H. (2009). Monitoring Animal Behaviour and Environmental Interactions Using Wireless Sensor Networks, GPS Collars, and Satellite Remote Sensing. *Sensors*, 9(5), 3586-3603. . doi:https://doi.org/10.3390/s90503586

Horton, C. V. (2019). *Patent No. Agricultural drone for use in livestock feeding. In: Google Patents.*

John Deere. (2022). *John Deere Mobile Weather.* John Deere.

Llopis-Jepsen, C. (2022). *How Satellite-Guided Cows Might Save the Kansas Prairie and Make Ranchers More Money .* Retrieved from ksnewsservice.org: ksnewsservice.org

Lowenberg-Deboer, J. &. (2019). Setting the Record Straight on Precision Agriculture Adoption. *Agronomy Journal*, 111(4), 1552-1569. . doi:https://doi.org/10.2134/agronj2018.12.0779

Mader, T. L.-B. (2006). Environmental factors influencing heat stress in feedlot cattle1,2. . *Journal of Animal Science*, 84(3), 712-719. doi:https://doi.org/10.2527/2006.843712x

Mallarino, A. P. (2010). Crop Yield and Soil Phosphorus as Affected by Liquid Swine Manure Phosphorus Application Using Variable-Rate Technology. *Soil Science Society of America Journal*, 74(6), 2230-2238. . doi:https://doi.org/10.2136/sssaj2009

Maresma, Á., & Ariza, M. M.-C. (2016). Analysis of Vegetation Indices to Determine Nitrogen Application and Yield Prediction in Maize (Zea mays L.) from a Standard UAV Service. *Remote Sensing*, 8(12), 973. doi:https://doi.org/10.3390/rs8120973

McMeniman, J. (2021). *BunkBot adoption demonstrations begin.* Retrieved from Meat & Livestock Australia: https://www.mla.com.au/news-and-events/industry-news/bunkbot-adoption-demonstrations-begin/#:~:text=An%20integrated%20system%20developed%20by,accurate%20and%20precise%20than%20humans.

Meyers, J. M., & Dokoozlian, N. R. (2020). A New, Satellite NDVI-Based Sampling Protocol for Grape Maturation Monitoring. *Remote Sensing*, 12(7), 1159. . doi:https://doi.org/10.3390/rs12071159

Micro Technologies: Our History – Innovation in Motion. . (2022). Micro Technologies Amerisource Bergen. .

Ofori, E. G. (2020). Duration analyses of precision agriculture technology adoption: what's influencing farmers' time-to-adoption decisions? Agricultural finance review., 80(5), 647-664. https://doi.org/10.1108/AFR-11-2019-0121. *Agricultural finance review.*, 80(5), 647-664. . doi:https://doi.org/10.1108/AFR-11-2019-0121

Pearson, C. F. (2021). The Relationship between Satellite-Derived Vegetation Indices and Live Weight Changes of Beef Cattle in Extensive Grazing Conditions. *Remote Sensing*, 13(20), 4132. . doi:https://doi.org/10.3390/rs13204132

Peña-Barragán, J. M.-G.-T.-E.-F. (2008). Discriminating cropping systems and agro-environmental measures by remote sensing. *Agronomy for Sustainable Development*, 28(2), 355-362. doi:https://doi.org/10.1051/agro:2007049

Reynolds, B. R. (2022). *PrecisionVision 35 X Unmanned aircraft system (UAS).* Retrieved from https://leaaerialtech.com/precisionvision-35x/: https://leaaerialtech.com/precisionvision-35x/

Sciforce. (2020). *Smart Farming: The Future of Agriculture.*

IoT for all. Retrieved from https://www.iotforall.com/: Sciforce. (2020). Smart Farming: The Future of Agriculture. IoT for all. https://www.iotforall.com/smart-farming-future-of-agriculture

Sullivan, D. G., & Shaw, J. N. (2005). IKONOS Imagery to Estimate Surface Soil Property Variability in Two Alabama Physiographies. . *Soil Science Society of America Journal*, *69*(6), 1789-1798. doi:https://doi.org/10.2136/sssaj2005.0071

Timmermans, R. (2022). *4 New Technologies in Agriculture That Are Helping Farmers. Groundstation.* Retrieved from www.groundstation.space:
https://www.groundstation.space/4-new-technologies-in-agriculture-that-are-helping-farmers/

Ungar, E. D., & Henkin, Z. G. (2005). Inference of Animal Activity From GPS Collar Data on Free-Ranging Cattle. *Rangeland ecology & management.*, 58(3), 256-266. doi:https://doi.org/10.2111/
1551-5028(2005)58[256:IOAAFG]2.0.CO;2

United States Environmental Protection Agency. (2022, June 13). *Laws and Regulations that Apply to Your Agricultural Operation by Farm Activity.* Retrieved from https://www.epa.gov/: https://www.epa.gov/agriculture/laws-and-regulations-apply-your-agricultural-operation-farm-activity

United States Environmental Protection Agency. (2022, August 23). *EPA Unmanned Aircraft Systems (UAS) Program.*

Retrieved from www.epa.gov/: https://www.epa.gov/geospatial/epa-unmanned-aircraft-systems-uas-program

Vaeljaots, E. L. (2018). Soil sampling automation case-study using unmanned ground vehicle. . *Eng. Rural Dev*, pp. 17, 982-987. .

Veres, B. &. (2022). Insight into emerging space system technologies on the market for cattle management applications . (D. H. Larson, Interviewer)

Wang, S. R. (2022, Feb). *"Farm Labor, Human Capital, and Agricultural Productivity in the United States," ERR-302, U.S. Department of Agriculture, Economic Research Service.* Retrieved from https://www.ers.usda.gov/: https://www.ers.usda.gov/authors/ers-staff-directory/sun-ling-wang/

Wankhede, S. J. (2021). Agricultural Drones Market by Offering, Component, and Application: Opportunity Analysis and Industry Forecast 2021-2030. *(A04722)*, 286. doi:https://www.alliedmarketresearch.com/agricultural-drone-market

Yang, C. &. (2020). Mapping Grain Sorghum Yield Variability Using Airborne Digital Videography. . *Precision Agriculture*, pp. 2(1), 7-23. . doi:https://doi.org/10.1023/a:1009928431735

Zarco-Tejada, P. J.-D. (2012). Fluorescence, temperature and narrow-band indices acquired from a UAV platform for water stress detection using a micro-hyperspectral imager and a thermal camera. *Remote sensing of environment*, 117, 322-337. . doi:https://doi.org/10.1016/j.rse.2011.10.007