Fall 8-15-2023

Cyber-Human Systems, Space Technologies, and Threats

Randall K. Nichols
Kansas State University

Candice M. Carter

Jerry V. Drew II

Max Farcot

John-Paul Hood

See next page for additional authors

Recommended Citation

Nichols, Randall K.; Carter, Candice M.; Drew, Jerry V. II; Farcot, Max; Hood, John-Paul; Jackson, Mark J.; Johnson, Peter D.; Joseph, Siny; Kahn, Saeed; Lonstein, Wayne D.; McCreight, Robert; Muehlfelder, Trevor W.; Mumm, Hans C.; Diebold, Carter; Ryan, Juole J.C.H.; Sincavage, Suzanne M.; Solfer, William; and Toebes, John, "Cyber-Human Systems, Space Technologies, and Threats" (2023). *NPP eBooks*. 52.
https://newprairiepress.org/ebooks/52

Authors

Randall K. Nichols, Candice M. Carter, Jerry V. Drew II, Max Farcot, John-Paul Hood, Mark J. Jackson, Peter D. Johnson, Siny Joseph, Saeed Kahn, Wayne D. Lonstein, Robert McCreight, Trevor W. Muehlfelder, Hans C. Mumm, Carter Diebold, Juole J.C.H. Ryan, Suzanne M. Sincavage, William Solfer, and John Toebes

Cyber-Human Systems, Space Technologies, and Threats

CYBER-HUMAN SYSTEMS, SPACE TECHNOLOGIES, AND THREATS

PROFESSOR RANDALL K. NICHOLS; CANDICE M. CARTER; JERRY V. DREW II; MAX FARCOT; CAPTAIN JOHN-PAUL HOOD; DR. MARK J. JACKSON; PETER D. JOHNSON; DR. SINY JOSEPH; DR. SAEED KAHN; WAYNE D. LONSTEIN; DR. ROBERT MCCREIGHT; TREVOR W. MUEHLFELDER; DR. HANS C. MUMM; CARTER DIEBOLD; DR. JULIE J.C.H. RYAN; DR. SUZANNE M. SINCAVAGE; WILLIAM SLOFER; AND JOHN TOEBES

COLONEL JOEL D. ANDERSON

New Prairie Press
Manhattan, KS

Cover design by Dr. Suzanne M. Sincavage and Trevor Muehlfelder and should be cited as follows:

Sincavage, S. M., & Muehlfelder, T. (2023). Final Cover for Book 8 Nichols (Ed). *Cyber- Human Systems, Space Technologies, and Threats.* KSU – NPP, Manhattan, KS.

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

Electronic edition available online at: http://newprairiepress.org/ebooks/52

Ebook ISBN: 978-1-944548-54-4

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

CONTENTS

CYBER-HUMAN SYSTEMS, SPACE TECHNOLOGIES AND THREATS

CYBER-HUMAN SYSTEMS, SPACE TECHNOLOGIES AND THREATS

BY

KSU WILDCAT TEAM

NICHOLS; CARTER, DIEBOLD, DREW, FARCOT, HOOD, JACKSON, JOHNSON, JOSEPH, KHAN, LONSTEIN, MCCREIGHT, MUEHLFELDER, MUMM, RYAN, SINCAVAGE, SLOFER, TOEBES

"The growth of our science and education will be enriched by new knowledge of our universe and environment, by new techniques of learning and mapping and observation, by new tools and computers for industry, medicine, the home as well as the school." **"We Choose the Moon" in his 1962 speech, President John F. Kennedy.**

TITLE PAGE

A PDF version of this book is available at [https://www.newprairiepress.org/ebooks/52/]

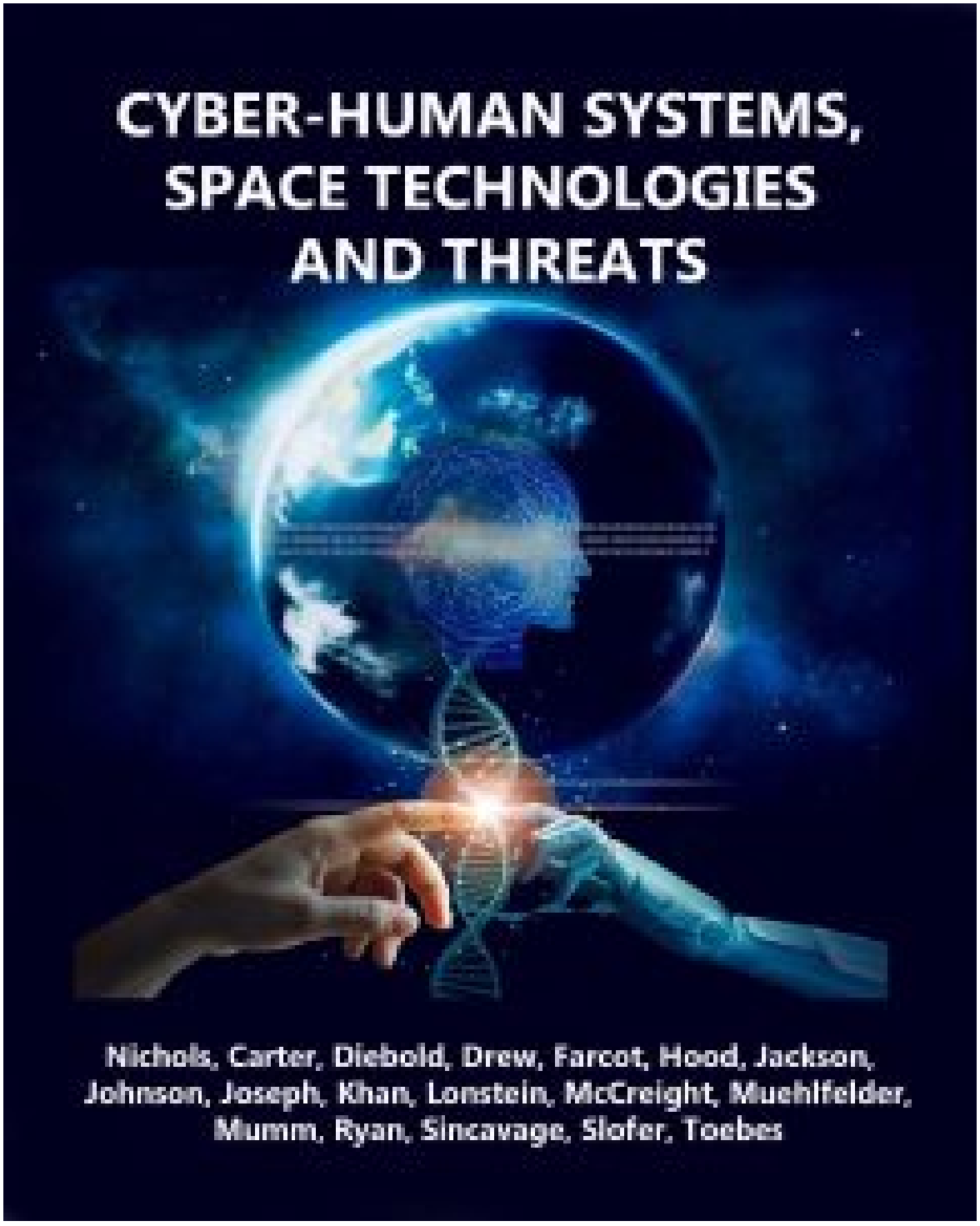
Cover design by Dr. Suzanne M. Sincavage and Trevor Muehlfelder

Courtesy of

New Prairie Press
Kansas State University Libraries
Manhattan, Kansas

E-books ISBN: 978-1-944548-54-4

Cover Art



COVER ART

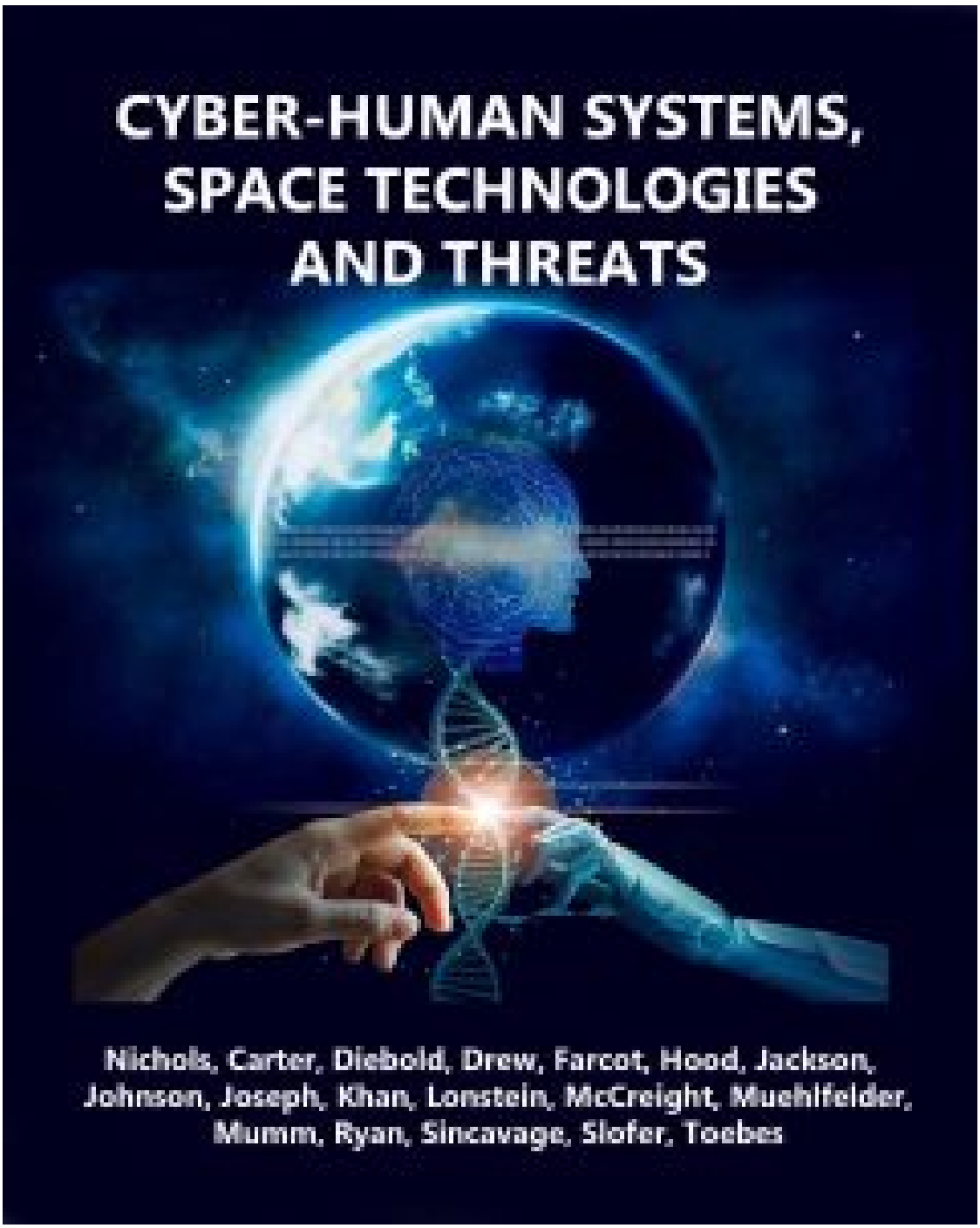
CYBER-HUMAN SYSTEMS, SPACE TECHNOLOGIES AND THREATS

BY

NICHOLS; CARTER, DIEBOLD, DREW, FARCOT, HOOD, JACKSON, JOHNSON, JOSEPH, KHAN, LONSTEIN, MCCREIGHT, MUEHLFELDER, MUMM, RYAN, SINCAVAGE, SLOFER, TOEBES

Cover design by Dr. Suzanne M. Sincavage and Trevor Muehlfelder

Cover image:



Courtesy of (Sincavage & Muehlfelder, 2023)

New Prairie Press

Kansas State University Libraries

Manhattan, Kansas #52

Pressbooks ISBN: 978-1-944548-54-4

Bibliography

Sincavage, S. M., & Muehlfelder, T. (2023). Final Cover for Book 8 Nichols (Ed). *Cyber- Human Systems, Space Technologies, and Threats.* KSU – NPP, Manhattan, KS.

COPYRIGHT / PUBLICATION PAGE

CYBER-HUMAN SYSTEMS, SPACE TECHNOLOGIES AND THREATS

BY

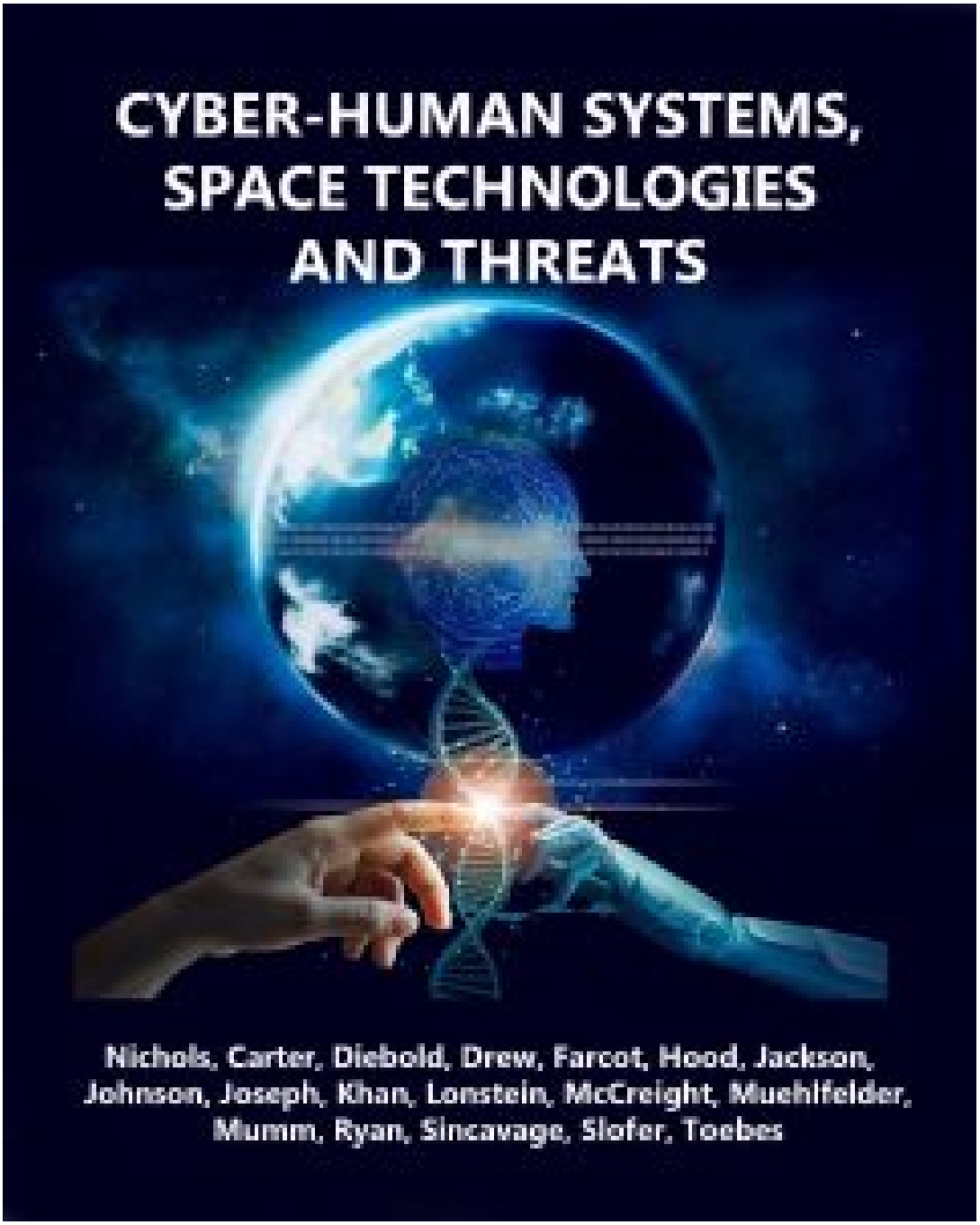
NICHOLS; CARTER, DIEBOLD, DREW, FARCOT, HOOD, JACKSON, JOHNSON, JOSEPH, KHAN, LONSTEIN, MCCREIGHT, MUEHLFELDER, MUMM, RYAN, SINCAVAGE, SLOFER, TOEBES

A PDF version of this book is available at

[https://www.newprairiepress.org/ebooks/52/]

Cover design by Dr. Suzanne M. Sincavage and Trevor Muehlfelder

Cover image:



Courtesy of (Sincavage & Muehlfelder, 2023)
New Prairie Press
Kansas State University Libraries
Manhattan, Kansas #52

E-books ISBN: 978-1-944548-54-4

Bibliography

Sincavage, S. M., & Muehlfelder, T. (2023). Final Cover for Book 8 Nichols (Ed). *Cyber- Human Systems, Space Technologies, and Threats.* KSU – NPP, Manhattan, KS.

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

Nichols, R. K.; Carter, C.M., Diebold, C., Drew, J. , Farcot, M., Hood, J.P, Jackson, M.J., Johnson, P., Joseph, S., Khan, S., Lonstein, W.D., McCreight, R., Muehlfelder, T., Mumm, H.C., Ryan, J.C.H., Sincavage, S. M., Slofer, W., & Toebes, J. ***Cyber Human Systems, Space Technologies, and Threats*** **(2023)** Copyright © 2023 All Rights Reserved. Manuscript available at: https://kstatelibraries.pressbooks.pub/cyberhumansystems/ & NPP eBooks. #52. https://newprairiepress.org/ebooks/52/

Nichols, R. K., Carter, C. M., Hood, J. P., Jackson, M. J., Joseph, S., Larson, H., Lonstein, W. D., Mai, R. W., McCreight, R., Mumm, H. C., Oetken, M. L., Pritchard, M. J., Ryan, J., J.C.H., Sincavage, S. M., Slofer, W. ***Space Systems: Emerging Technologies and Operations*** (2022) Copyright © 2022 All Rights Reserved. NPP eBooks. 47. https://newprairiepress.org/ebooks/47/

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/

Barnhart, R.K., Marshall, D.M. & Shappee, E. (2021) **INTRODUCTION TO UNMANNED AIRCRAFT SYSTEMS, 3RD ED**, *Nichols, R.K.* in ***Chapter 18: Cybersecurity Counter Unmanned Aircraft Systems (C-UAS) and Artificial Intelligence*** **(AI) CRC Press.**

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

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

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

R.K. Nichols, J.J.C.H. Ryan, H.C. Mumm, C. Carter, W.D. Lonstein, J.P. Hood, (2019) ***Unmanned Aircraft Systems in the Cyber Domain Protecting USA's Advanced Air Assets***, 2nd Ed. 26 July

2019, Copyright 2019-2021, All Rights Reserved, Manhattan: New Prairie Press (NPP eBooks 31). ISBN:978-1-944548-15-5. https://newprairiepress.org/ebooks/27

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

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

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

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

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

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

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

DEDICATIONS

FROM PROFESSOR RANDALL K. NICHOLS:

I dedicate this book to **All USA serving and retired military personnel**, and federal, state and local law enforcement for keeping our blessed Country safe; to my Angel wife of 39 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 members Kira Nichols; grandson Greyson Kent Nichols; and finally, to all my students (over 52 years ~11,500 Dragons / Dragonesses in the field) who are securing our United States from terrorism and evil.

It is my sincere wish that our Cyber and Space technology writings may be used not only to defend our Country but to envision humanitarian ways to more efficiently feed our expanding global population. Just dream – if we could increase agricultural production by 1-1.5 %. Think how many millions of families we could improve living conditions for!

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 loved ones 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 KSU 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. I cannot thank you all enough for your dedication.

FROM DR. SUZANNE M. 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 K. Nichols for his leadership, mentorship, integrity, and significant contributions to uncharted spaces and for bringing together once again the WILDCAT team in our pursuit of excellence; To Julie J.C.H. Ryan for devoting an incredible amount of time to supporting me in my work; To Trevor Muehlfelder, my esteemed co-author for whose unwavering commitment, expertise and collaboration have been invaluable in the creation of this book and its cover. To my sons Trevor, Cole Muehlfelder an (Aspiring ERAU Professor), and Jacquie for bringing Callum into this world, and David a (Master Machinist) for their loving encouragement, To Dr. Steve Herrick, and the entire Herrick family

for their belief and support in me, To Candice Carter, a loyal colleague and friend, & Co-Chair for "The Foundation for Biodefense Research", her devotion and support are invaluable, and to Mila Bonner, a life-time friend who is an expert in Life-work balance.

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 M. 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 continued 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 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. The American warfighters are the heart and soul of the fight against evil oppressors.

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:

As usual, I would like to thank God for the opportunities and pathways he has made available and the inspiration that led to the crafting of this work. A thank you to all the service men and women past and present for their commitment and service. To Dr. Korn, Dr. H. Bell, and Charles Marrow for their inspiration resulting in the physics and math principles used in this content. Also, a special thanks to Charlene Jones for her support and technical editing and my daughter Jessica for her continued support, encouragement, and partnership in lifelong learning which helped with this research.

FROM LTC JERRY V. DREW USARMY CAC (USA):

I would like to dedicate this work to my son Jerry. He will be 39- the age I am now – in 2048. The future will be different than we can know, but we are trying to make it a good one.

FROM TREVOR MUEHLFELDER:

This work is dedicated to the support and opportunity provided by Dr. Suzanne Sincavage, Professor Randall K. Nichols, and the many friends and family that encourage me to go farther. It is dedicated to the pursuit of knowledge and the tireless efforts of scholars, researchers, and authors who have contributed to the vast wealth of information found in print encyclopedias, non-fiction books, academic journals, and dictionaries.

FROM JOHN TOEBES:

I dedicate my chapter to my wife, Mary Ellen, who tirelessly works with me to coach the FIRST Tech Challenge robotics teams that our daughter, Margaret, had the amazing foresight to start. To our other daughter, Ann Marie, I am grateful for keeping me apprised of the latest in medical technology. To all of the students who have come through the FIRST program, we challenge you to use what you have learned to make the world a better place.

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. SAEED KHAN:

I would like to dedicate this humble work to my big sister, Dina Sultana, who recently passed away leaving an emptiness in our hearts. She was great at mathematics, winning performance awards at school and also found time to be good at painting. She will be missed by all those who knew and loved her.

FROM MAX FARCOT:

I dedicate my chapter to my fellow Dragon teammates from previous KSU academic projects: Justin Redetzke, Jeff Harris, and Professor Randall K. Nichols. I would also like to give special thanks to the rest of the members of our KSU author's team.

FROM MAJOR CARTER DIEBOLD:

My chapter is dedicated to the Soldiers of Echo Company, who have continuously motivated and inspired me through their relentless commitment to America's Joint Forces operating far from home. Additionally, this chapter could not have been possible without the love and support of Megan, who stood by me through years of late nights and time away from home. Finally, I would like to thank Professor Randy Nichols, my instructor for the last year and leader of this project. Without his personal motivation, leadership, and guidance, I would never have attempted to tackle such a complex topic, much less attempt to write about it. I am forever grateful for the opportunity to be a part of this team.

FROM PETER D. JOHNSON:

I would like to dedicate my chapter to the Soldiers, Civilians, and Law Enforcement Professionals who are diligently serving and protecting our shores, stepping into the arena to keep us safe at night. To Carter D, for support and guidance on Prof Nichols' wild ride. To Prof Nichols for providing the confidence, the challenge, and the push outside my comfort zone. And most importantly to my wife Laura and children Jillian, Christopher, and Avery for providing me the confidence and support in my professional and personal endeavors, often sacrificing more than anyone will ever know.

DISCLAIMERS [LONSTEIN]

Information contained in this work has been obtained by the authors from sources believed to be accurate and reliable. However, New Prairie Press, Pressbooks, Professor Randall K. Nichols (Managing Editor / Co-Author / 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, underwater and Space, Cyber-Human Systems, Space Technologies and Threats; drone delivery of chemical threats, biological threat agents, radiation threats, nuclear threats, cyberwar, information warfare, electronic warfare, cybersecurity, directed energy weapons, hypersonics, CHS sensors, artificial brains, robotics, AI, VR, EW, Metaverse, wireless power systems, 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, space system 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. Although the author and publisher have made every effort to ensure that the information in this book was correct at press time, the author and publisher do not assume and hereby disclaim any liability to any party for any loss, damage, or disruption caused by errors or omissions, whether such errors or omissions result from negligence, accident, or any other cause.

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 [COL. JOEL D. ANDERSON (RET) - KSU OVPR (RET)]

When I was asked to do this forward, I was in the process of retiring from academia after 10 years in the scientific, technical and research arena of higher education. At first, I was hesitant to accept this honor but reminded myself that I had amassed nearly 5 decades of experience relevant to the topics covered in this text. I reminded myself that I had been designated a subject matter expert (SME) by the Homeland Defense & Security Information Analysis Center (HDIAC) while at Kansas State University. I considered that before arriving at Kansas State University I had spent three years in industry supporting technical innovation efforts as both a technical director for a major international corporation, and as the inaugural director for a small company leading its autonomous systems group (ASG). I reminded myself that I had enjoyed a 26 ½ year career as an intelligence professional, imagery officer, space operations officer, a DAWIA level III certified program manager, and as a strategic intelligence planner.

I decided that my past experiences provided me with potentially unique insights into strategic, operational, tactical, and technical intelligence and research related to the topics discussed herein. In reviewing the sections I did so not only looking at the value of its content for the student, but in assessing broader critical insights that the text might provide to others in government, industry and academia having served in each sector.

Cyber-Human Systems, Space Technologies and Threats is the 8th in a series of seminal texts focused on influencing student and workforce development, critical thinking, and discovery. I found the topics in this text to accurately reflect the complexity and realities of the emerging human machine world we live in here on earth and in newfound discoveries that await us in space. A world where human/machine interactions are blending and merging in ways that were unimaginable just a few short years ago. This text focuses on important considerations for highly technical and demanding disciplines associated with cyber-human systems, space technologies and real and emerging threats. Each section and chapter covers a myriad of deeply insightful topics and considerations from expert practitioners in their respective fields. It provides a logical and practical framework for learning not only for the student, but for those already in the workforce looking for continuing education, certification, and credentials necessary to support national security at the critical emerging technology level. The authors have effectively captured topics of critical importance to our sustaining technological competitiveness, national security, economic growth, and workforce development.

In 1962, during his "We Choose the Moon" speech, President John F. Kennedy stated that "*The growth of our science and education will be enriched by new knowledge of our universe and environment, by new techniques of learning and mapping and observation, by new tools and computers for industry, medicine, the home as well as the school.*" He proceeded to articulate this simply by stating "We choose to go to the moon....and do the other

things, not because they are easy but because they are hard…." This text embodies this message in its fullest. We have come a long way since 1962. We still have a long way to go.

In laying out this text, the authors have chosen to tackle hard subjects that we must consider for our next generation of leaders and practitioners. They have done so in a manner that not only captures a current understanding of the technological and threat playing field, but have artfully set their sights outward to the future by logically laying out things to consider and, where needed, challenging conventional norms. As I reviewed the content, not only was I pleased with the technical expertise of the authors, but found that each chapter left me wanting more. It reminded me of a phrase that Neil deGrasse Tyson is attributed as saying: "There are times, at least for now, when we must be content to love the questions themselves."

I am confident that you will find the subject matter relevant, deeply enriching, and as either student or practitioner–leaving you with a thirst for wanting more. I am confident that those using this text will find answers in the material provided and energized by its content. I am also confident that in using this text, you will also find yourself asking many questions as you work through this now and hopefully many more in the future.

I applaud the authors for assembling its content and commend ***Cyber-Human Systems, Space Technologies and Threats*** for wide distribution and use. They have not only provided the facts and answers, but they will have also stimulated the questions of a new generation.

I am hopeful that in using this text you not only learn from it, but do so knowing that at one point in time we chose the moon.

Enjoy, learn, challenge and be challenged.

Joel D Anderson
Colonel USMC (Ret)
KSU (Ret)

PREFACE (NICHOLS)

CYBER-HUMAN SYSTEMS, SPACE TECHNOLOGIES AND THREATS*is* our eighth textbook in a series covering the world of UASs / CUAS/ UUVs / SPACE. Other textbooks in our series are **Space Systems: Emerging Technologies and Operations;** ***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 seven titles have received considerable global recognition in the field. (Nichols & Carter, CYBER-HUMAN SYSTEMS, SPACE TECHNOLOGIES AND THREATS, 2023) (Nichols R. K., 2022) (Nichols & Carter, Drone Delivery of CBNRECy – DEW Weapons: Emerging Threats of Mini-Weapons of Mass Destruction and Disruption (WMDD), 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 eighth title takes on a new purview of Cyber-Human Systems (CHS) and their effects on our world. The textbook is broken down into three sections: Cyber-Human Systems; Space Technologies, Space Threats (CHS used in Space vehicles and exploration and Space warfare, hypersonics and materials needed for off world travel.)

Section 1 looks at our technological future and how humans are merging with machines. The misuse of technology is addressed in a chapter on CHS sensors and the law. Another chapter looks at the artificial brain and body – specifically the levels of autonomy that can practically be achieved. Chapter 4 addresses a serious concern – feeding a globally growing population. How? By applying artificial intelligence (AI) and machine language programming (ML) to food production / distribution / and protection cycle. The next chapter zeros in on Cyborgs, singularity, and their use in space. We drop back in the next chapter to touch on history with the Turing legacy. Another chapter covers the reality of managing mixed machine – human teams. The section ends with a serious look at Neurostrike and CHATGPT.

Section 2 is devoted to space and threats. One chapter terrifies the reader with biological threats and distribution from space vehicles. Another presents the elements of space electronic warfare with interest in jamming and spoofing GPS signals. Still another looks at Space systems modeling and simulation. Five major tools are presented. The author takes on the problem of conducting Deep Space Warfare and Space Dominance. This is a fascinating and complex logistics theater of warfare.

Section 3 continues the theme of space warfare and adds hypersonics and materials of construction for space vehicles. Our resident expert on hypersonic missiles and space defense gives the reader another bite on the apple

from Book 7. We continue our review of cyber threats in space and speculate on the future of cyberwarfare. Space missions have an economic framework, and this is covered in chapter 15. Quantum technologies are making a big splash. We address their applicability to space operations. Our final chapter is a brilliant look at inventions for transferring wireless power for space applications.

State-of-the-Art research by a team of eighteen 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, DTM
Professor of Practice
Director, GC Space Systems and Operations (SSO) &
Director, GC Aerospace Cyber Operations (ACO)
Managing Editor / Co-Author, UAS / CUAS/ UUV / Space Textbook Series
Kansas State University Salina – Aerospace and Technologies Campus &
Professor Emeritus – Graduate Cybersecurity & Forensics, Utica College
LinkedIn Profile:
www.linkedin.com/in/randall-nichols-2222a691
Illi nunquam cedunt.
"We Never Yield"

REFERENCES

Nichols, & Carter, D. D. ,et.al. (2023). *CYBER-HUMAN SYSTEMS, SPACE TECHNOLOGIES AND THREATS.* Manhattan, KS: New Prairie Press #52. Manuscript Available at: https://kstatelibraries.pressbooks.pub/cyberhumansystems/

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. (2022). *SPACE SYSTEMS: EMERGING TECHNOLOGIES AND OPERATIONS.* Manhattan, KS: NPP #47.

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/.

[1] As of 09 August 2023, the PlumX statistics from NPP: **Countries: 172 Institutions: 1817 Downloads: 56,800 Meta page Hits: 15,958 Abstract views: 12,082 Referrers: 433 Rate ~ 621 -1250 per month Estimate by end 2023 = ~ 70,000 with Book 8 in inventory.**

ACKNOWLEDGEMENTS

Books such as this are the products of contributions by many people, not just the authors' musings. ***CYBER-HUMAN SYSTEMS, SPACE TECHNOLOGIES AND THREATS*** (Nichols & et.al, Cyber-Human Systems, Space Technologies, and Threats, 2023) has benefited from the review of numerous experts in the field, who gave generously of their time and expertise. In addition to invited Subject Matter Experts, this book was reviewed by sources in the two federal agencies, who must remain anonymous and by export / procedural / security /OVRP / management and library committees at KSU. U.S Army and U.S. Air Force reviewing procedures were adhered to. 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 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. Alysia Starkey, Dean & CEO of KSU-AT; Dr. Kurt C. Barnhart, prior Associate Dean of Research and Executive Director of the UAS Research Laboratory KSU-AT; Dr. Michael Pritchard, Associate Dean and creator of the new Space Technologies Masters and four Graduate Certificate programs; 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. Carolyn S. Jackson at New Prairie Press and Pressbooks; Col. (ret) Joel Anderson, KSU OVPR and Research Director; Randall Mai, Research Technologist for KSU, a Dragon convert with years of experience in the UAS field operations; Dr. Haley Larson, KSU expert in agriculture and cattle feeding and science. Dr. Michael Oetken our in-house expert in virtual reality, extended reality, and robotics. Special thanks to Col. (ret) Jonathan Snowden, KSU FSO and RVP who has generously helped us on potential security issues.

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 and Dr. Siny Joseph KSU-AT Professor of economics and policy.

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)*

We thank and give full attribution to author John C. Wright for his superb analysis and U.S. Navy model of deep space warfare characteristics. (Wright, 2020) His work inspired Chapter 12 for our students.

No one could be prouder of the textbooks my KSU Wildcat team produced between 2018-2023. ***CYBER-HUMAN SYSTEMS, SPACE TECHNOLOGIES AND THREATS*** *is* our eighth textbook in a textbook series covering the world of Cyber-Human Systems, AI, Cyborgs, Robots, Automation, Space Technologies and Threats.[1] Other textbooks in our series are **Space Systems: Emerging Technologies and Operations; *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 seven titles have received considerable global recognition in the field. (Nichols & Carter, CYBER-HUMAN SYSTEMS, SPACE TECHNOLOGIES AND THREATS, 2023) (Nichols R. K., 2022) (Nichols & Carter, Drone Delivery of CBNRECy – DEW Weapons: Emerging Threats of Mini-Weapons of Mass Destruction and Disruption (WMDD), 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)**

Next comes our expanded Wildcat writing team: Dr. Suzanne M. 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 SME on management of UAS weapons – a lethal combination; Dr. Wayne C. Lonstein, Esq., a previous Dragon (Nichols' student) has gained recognition (licenses and certifications) in both law and cybersecurity as well as heads up his own legal firm addressing social disinformation; 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. Major 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; Dr. Mark Jackson, SME in UUV, naval architecture, nanotechnologies and space manufacturing systems; Dr. Siny Joseph, an expert in space economies, Robert McCreight, a specialist in U.S. Army Special Operations and National Security Expert in Defense programs associated with nuclear and biological defense matters; Prof. William Slofer, Dragon and SME in radar and Hypersonic technologies. We appreciate all of their contributions. Dr. Saeed Khan, Professor, SIS KSU-AT demonstrated original research on wireless power transfer in space vehicles. We are Honored to have engaged LTC Jerry Drew, U.S. ARMY CGSC to write a chapter. 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 In addition, we are blessed to have two current KSU GC ACO Dragons, both U.S. Army, Major Carter Diebold and SGM (Ret.) Peter D. Johnson currently CUAS Specialist and one former Dragon. SGM Johnson gave us a fun chapter on Cyborgs. Major Diebold taught us about space simulations. Max Farcot generously shared experiences in engaging chapter on cyber threats in space. Dr John Toebes, SME, and holder of 150 U.S. Patents in the robotics industry. He authored our lead-off chapter. Special thanks to CEO Joel Coulter, Chief Safety Pilot Justin Redetzke, CEO Mike Monnik, EVP Richard Lescalleet and SMSGT Jeremy Shay for their special council and excellent advice on a wide variety of topics.

We were fortunate to have Dr. Sincavage and Trevor Muehlfelder build our beautiful cover art. They also collaborated with Prof. Carter on the chapter covering biological threats and growth in space. Trevor was especially helpful in the editing and crisis mode toward the end of our project.

We are Honored to have engaged Col (ret.) Joel D. Anderson USAF OVPR to write our Foreword. Col. Anderson has years of experience to understand our priorities and hope for the future in Space. He has been a wonderful friend / Mentor to the KSU Wildcat author team for more than 7 years. We hold LTC Col. (ret), USAF, Jonathan Snowden, KSU Research Security Officer and FSO in the highest regard as he has been a security beacon for our writings.

Special thanks to Gwen Sibley, Assistant Professor, Scholarly Communications and Copyright Librarian, Ryan Otto, Associate Professor, Scholarly Communications and Copyright Librarian, Carolyn Jackson, Scholarly Communications / OER Librarian, and Laura Bonella, Department Head, Academic Services for making our book a reality at New Prairie Press with Pressbooks.

Professor Randall K. Nichols is Managing Editor/Author/Co-author with his Wildcat Team of fifteen textbooks and developer of six Master's and Certificate programs in Cybersecurity, Intelligence, Forensics, Aerospace Cyber Operations, and UAS/CUAS/UUV/Space at Utica College and Kansas State University. Nichols serves as Professor of Practice, Director, GC Space Systems and Operations (SSO) & Director, GC Aerospace Cyber Operations (ACO) graduate programs. He has five decades of management and technical experience in multiple disciplines training resources to protect the United States from terrorism.

Finally, Mrs. Montine Nichols, my God-given Angel of 39 years, deserves a commendation for her help on the final drafts and copy edit work for our book and a living (surviving) this long with a real Dragon who hardly sleeps.

Randall K Nichols, DTM
Professor of Practice
Director, GC Space Systems and Operations (SSO) &
Director, GC Aerospace Cyber Operations (ACO)
Managing Editor / Co-Author, UAS / CUAS/ UUV Space Textbook Series

Kansas State University Salina – Aerospace and Technologies Campus &
Professor Emeritus – Graduate Cybersecurity & Forensics, Utica College
LinkedIn Profile:
www.linkedin.com/in/randall-nichols-2222a691
Illi nunquam cedunt.
"We Never Yield"

References

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

Nichols, & Carter, D. D., et.al (2023). *CYBER-HUMAN SYSTEMS, SPACE TECHNOLOGIES AND THREATS.* Manhattan, KS: New Prairie Press #52.

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. (2022). *SPACE SYSTEMS: EMERGING TECHNOLOGIES AND OPERATIONS.* Manhattan, KS: NPP #47.

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.

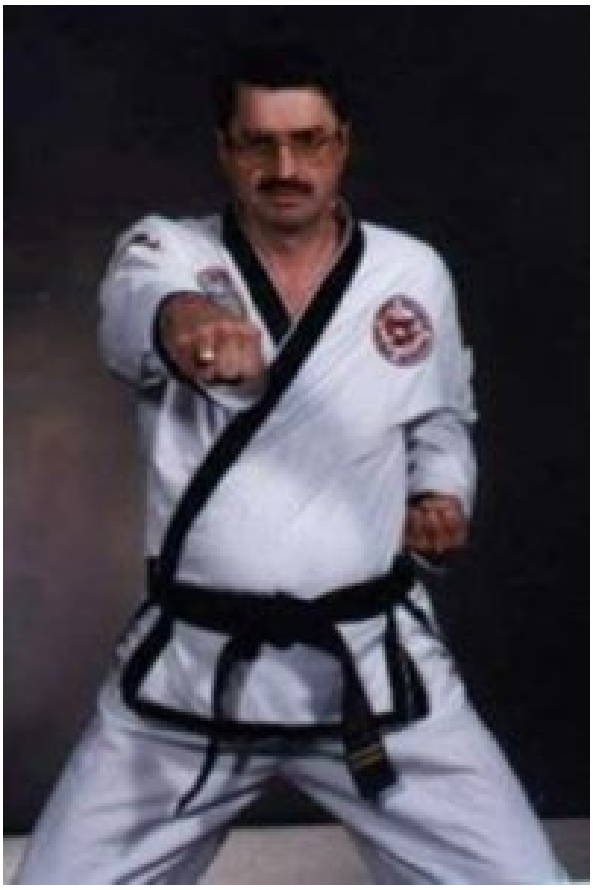
Nichols, R., Ryan, J., Mumm, H., Lonstein, W., Carter, C., & Hood, J. (2019). *Unmanned Aircraft Systems in Cyber Domain: Protecting USA's Advanced Air Assets, 2nd edition.* Manhattan, KS: https://newprairiepress.org/ebooks/27/.

Wright, J. C. (2020). *Deep Space Warfare: Military Strategy Beyond Orbit.* Jefferson, NC: McFarland & Co. Inc.

[1] All eight textbooks in the series are available free of charge via e-books from New Prairie Press. Our team only asks that full attribution to be given to the KSU Wildcat authors and respect the CC licenses requirements.

LIST OF 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 Space Systems and Operations (SSO) and Director, GC Aerospace Cyber Operations Programs. Nichols is internationally respected, with 53 years of experience in leadership roles in cryptography, counterintelligence, INFOSEC, and sensitive computer applications. Throughout his career, Nichols has published *fifteen* 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: MS / Certificate in Aerospace Cyber Operations (ACO)
- Program Director: GC Space Systems & Operations (SSO) &
- Program Director / Author / Developer: GC Aerospace Cyber Operations (ACO)

- 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/SPACE Series:

Cyber Human Systems, Space Technologies, and Threats. (2023) Manhattan, KS: New Prairie Press #52. Available as a free book at: **http://newprairiepress.org/ebooks/52/**

Space Systems: Emerging Technologies and Operations.* (2022)** Manhattan, KS: New Prairie Press #47. Available as a free book at: ***http://newprairiepress.org/ebooks/47/

***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**

Barnhart, R.K., Marshall, D.M. & Shappee, E. (2021) Introduction To Unmanned Aircraft Systems, 3rd Ed, *Nichols, R.K.* in *Chapter 18: Cybersecurity Counter Unmanned Aircraft Systems (C-UAS) and Artificial Intelligence* (AI) CRC Press.

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.
- Space Electronic Warfare & ECD Jamming / Spoofing Countermeasures
- Humanitarian use of Space Technologies to improve global food availability

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

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

DR. HANS C. MUMM (CO-AUTHOR)

Dr. Mumm has spent a combined twenty-nine 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 supporting 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, and the long-range planning for next-generation systems, including 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, post-quantum cyber security, AI/machine learning, advanced fuel systems, cognitive scientific research, and all aspects of the military intelligence communities. He has nine published books and many whitepapers and research studies to his credit in both the scientific and social science arenas. He 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 and granted a US Patent and Trademark for How to Harmonize the Speed of Innovation and Change with the Human Spirit's Need for Leadership. In 2005, Dr. Mumm was recognized as one of the "Ten Outstanding Young Americans." In 2003, he was awarded the National Defense PAC "American Patriot Ingenuity Award" for his service during "Operation Iraqi Freedom."

Dr. Mumm is an adjunct professor at Penn West in California, Pennsylvania, instructing Homeland Security courses in the Criminal Justice Department.

He recently Co-Authored "Space Systems: Emerging Technologies and Operations" the seventh book in a series of textbooks, which includes two editions titled "Unmanned Aircraft in the Cyber Domain; Protecting

USA's Advanced Air Assets," Drone Delivery of CBNRECy – DEW WEAPONS -Emerging Threats of Mini-Weapons of Mass Destruction and Disruption (WMDD) "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)

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. 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 papers and presentations.

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, 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 Technologies 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 Technologies 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, CHS & SPACE TECHNOLOGIES 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 a 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, collaborating 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.

DR. SUZANNE M. 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
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 (FOREWORD, WMDD; INTEGRATED STUDIES DEPT HEAD)

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.

DR. 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. Bill is an SME on Hypersonic vehicles and missiles.

Formal education includes:

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

BS, Business Administration / Computer Science

LIEUTENANT COLONEL JERRY V. DREW II

SPACE OPERATIONS OFFICER, U.S. ARMY (FOREWORD SS:ET&O, CO-AUTHOR CHS & SPACE TECHNOLOGIES & THREATS)

Lieutenant Colonel Jerry Drew, U.S. Army, is an instructor in the Department of Joint, Interagency, and Multinational operations at the U.S. Army Command and General Staff College. 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 thesis work focused on applied robotic manipulation using small spacecraft. Lieutenant Colonel Drew is a 2017 Art of War Scholar and a 2018 graduate of the School of Advanced Military Studies. He is currently enrolled as a PhD student in the Colorado School of Mines' Space Resource program.

As a professional soldier, Lieutenant Colonel Drew has served in numerous operational and institutional assignments. During his time as the lead space planner for the U.S. Army Space and Missile Defense Command from 2018-2019, he served as an original member of the planning team that established U.S. Space Command and is considered a founding member of the Space Force for helping plan the new service's creation. 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 LTC Drew as our Foreword writer for *Space Systems: Emerging Technologies and Operations* **(SS:ET&O**) and Co-Author on our current effort.

MAX FARCOT (CO-AUTHOR)

Max Farcot is a talented KSU Wildcat researcher who graduated from Kansas State University – Salina in July 2022 with *Graduate Certificate in Unmanned Aircraft Systems Information Assurance.* Max was appointed team leader for the important Fusion class. He led a team in assembling and presenting an elaborate briefing assessing the risks of conflict in the South China Seas. Max completed his undergraduate study at Embry-Riddle Aeronautical University, Daytona Beach, FL, graduating in Dec. 2020 with B.S. in Unmanned Aircraft Systems, minoring in UAS Safety – Summa Cum Laude. Max was a valued researcher for and contributor to the KSU textbook published in 2022: *Drone Delivery of CBNRE – Direct-Energy Weapons: Emerging Threats of Mini-Weapons of Mass Destruction and Disruption (WMDD).* The WMDD textbook *is* a required staple in the new Aerospace Cyber Operations (ACO) graduate program.

In 2019, Max Farcot worked as a *UAS Crewmember, Student Operator for* Service-Learning & Cooperative Education for Disaster Relief in OK & TX:

- Coordinated with Oklahoma Emergency Management Operations and Department of Wildlife Conservation efforts to survey large flooding activity, as well as tornado aftermath in Oklahoma
- Operated the Phantom IV, using Pix4D and live streaming software to collect data and imagery remotely
- Gained a deeper understanding of the operational requirements and coordination associated with UAS in support of disaster relief
- Gained experience with UAS flight crew positions, including PMC, Visual Observer, & Crew Chief roles

Max Farcot holds the following professional certifications:

FAA Remote Pilot Certificate (Part 107)	December 2019
FAA Student Pilot Certificate (Part 61)	July 2015

TREVOR WILLIAM MUEHLFELDER (CO-AUTHOR)

Trevor Muehlfelder is an accomplished social scientist. He currently consults for IDIQ Inc., a consulting firm devoted to advancing collaboration with government, academia, non-profits, and industry to meet critical needs. Within the company he currently advances scientific and technology standards and provides policy support within the national security and intelligence communities. In 2021, he supported the development of a unique foundry; The Foundation for Biodefence Research [501(c)3] and is currently involved in building a use inspired social-eco-impact model for technology innovation through translational and convergent research.

His educational training began at Santa Barbara City College where he received several associate degrees in different fields of study including Criminology, Psychology, and Sociology. He also attended special programs and educational training with George Mason University and attended diplomacy pursuits into China covering a broad range of issues including international relations and pending political atmospheres. Trevor completed his education at the University of California, Irvine where he excelled in courses such as Criminal Justice, Forensic Science, and Legal Research and earned his degree in Criminology, Law, and Society. There, he also received multiple honors and was integrated into several honor societies and programs.

After completing his degree, he served for several years in the Washington D.C. Metro Area as a Business Liaison and as the Director of Investigations for a legal firm. There, he gained international experience and knowledge with investigations, asset management and legal analysis. While in Washington, he also supplied critical analysis for Families of Homicide Victims and Missing Persons (FOHVAMP). He also succeeded in creating a customized mathematical formulation outlining monetary costs of psychological effects in corporate working spaces with Legacy Business Cultures.

Due to his interests in biological sciences, Trevor assisted in the development of nutraceuticals and was the Chief Operations Officer of an international nutraceutical company. There he aided in obtaining patents for nutraceutical formulations and aided in the biological research needed to develop dietary supplements.

MAJOR CARTER DIEBOLD

Military Intelligence Officer, U.S. Army (Co-Author)

Carter Diebold is the first graduate of Kansas State University's Aerospace Cyber Operations Graduate Certificate Program. He also holds a Master of Operational Studies degree from the U.S. Army Command and General Staff College and a Bachelor of Science in Informatics from Indiana University. Carter's most recent research focuses on the impact of Unmanned Aircraft Systems (UAS) in the Russo-Ukrainian War and the Western Pacific as well as threats to undersea cable networks.

Carter is a career Army Officer that has served in numerous command and staff positions from the Company to Brigade levels with the 101st Airborne Division (Air Assault), 160th Special Operations Aviation Regiment (Airborne), and the 1st Multi-Domain Task Force. He is also a veteran of the Afghanistan and Iraq wars, conflict in Northwest Africa, and operations in the Indo-Pacific theater.

Carter lives in Clarksville, Tennessee, with his life partner Megan and dog Argo. He holds certifications as an FAA Remote Pilot and Bourbon Steward.

JOHN TOEBES (CO-AUTHOR)

John Toebes has over 150 patents issued Worldwide in many areas including distributed computing, virtual reality, data and video compression, robotics, user experience and recommendation systems.

With over 35 years of industry experience, John has taken on many roles and responsibilities. After serving as a 2Lt in the Air Force stationed at the Pentagon, John has had leadership roles at SAS, Cisco, and Extreme Networks. At SAS, he was the founder and VP of Research and Development for SouthPeak, a SAS company. There he led development of the Video Realty™ technology and was producer for Men in Black: The Game. While at Cisco he led the development of multiple advanced technology groups. He was a leader in Cisco's Technology Center from 1999-2006 where he personally had issued 59 patents and his team generated 100's more to help position Cisco's patent portfolio as top in the industry.

John went on to advance to Senior Director with the Cisco Intellectual Property team which put in place processes and tools to streamline the patenting at Cisco. Cisco achieved receiving its 10,000th US patent during John's tenure which had dramatically ramped Cisco's patent portfolio. Also, during this time, John was invited by Director Seema Rao of the USPTO to present at the USPTO Software Partnership meeting on the topic of prior art searching on December 5, 2013. This utilized learning from Cisco's IP practice and enhancements that he implemented in order to improve prior art searching to eliminate bad software patents.

Most recently John is the co-founder and CTO of Escape Velocity Inc., a Triangle based technology startup focused on applying deep analytics to accelerate demand and growth for the next generation of big companies. He also serves as CTO for Gotham Studios, focusing on the Goji Geotainment® Hollywood-quality inflight experience platform.

Throughout his career, John has been an invited speaker and writer on a wide variety of topics. He was a regular C Language Columnist for The Amigan Apprentice and Journeyman, Technical Reviewer for AmigaWorld Tech Journal, writer for Transactor for the Amiga including premier issue and Assembly

language optimization tricks. He was a regular speaker at American and European Amiga Developer Conferences.

He was a speaker at Game Networks conference April 27,2004 and presented the Video Reality technology at the 1997 Computer Game Developer Conference.

At the W3C Video on the Web Workshop he presented: Enabling A Richer Video Experience With Metadata – A position paper for the W3C Video on the Web Workshop 12-13 December 2007. This paper and talk was a key motivator for the W3C making Video a first-class part of the HTML5 standard. He was the keynote speaker Second IEEE International Conference on Semantic Computing, August 6, 2008, and a panel speaker "The Knowledge Worker of the Future" OOPSLA, 27 October 2009. Speaker at the NCSU ASSIST Center – Recognizing and Generating Patentable Inventions – October 31, 2013

John is passionate about STEM and has coached Robotics and Science Olympiad with his wife, Mary Ellen at Cardinal Gibbons for the past fifteen years. During that time John initiated the design for and led a geographically dispersed team to create the Samantha Wi-Fi Adapter for the Lego Mindstorms that was ultimately used by thousands of High School Robotics teams. As a result, he was awarded Volunteer of the Year in 2011 at the FIRST World Championship. He continues to serve as a Wi-Fi Technical Advisor for FIRST Tech Challenge worldwide Championship for the past 10 years.

He continues to give back, encourage, and excite the next generation of engineers. He established the Maker Space at Cardinal Gibbons to expose their students to engineering.

John also serves as the National Event Supervisor for Science Olympiad Codebusters in which students solve ciphers. In this role he has been responsible for designing the rules for competition and implementing a series of web-based tools for dynamically generating tests used in the events by over 15,000 students and coaches in all 50 states.

In 2018, as a result of John's impact on the community and industry, John was inducted into the NCSU Computer Science Hall of Fame.

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. SAEED KHAN (CO-AUTHOR)

Saeed Khan has a Ph.D. in Electrical Engineering. He has industrial experience in the design of antenna systems for military guidance systems, GPS systems, and wireless communication systems. Saeed has several refereed publications and conference papers in the areas of Antennas and Propagation, Radar Scattering, and Novel Materials. He has been a key player in bringing programmable logic devices and VHDL into the curriculum. Recently he has focused on developing mixed signal concepts using SIMULINK and MALAB. Saeed has multiple papers, a patent, and a patent pending in the field of wireless power Saeed Khan has a Ph.D. in Electrical Engineering. He has industrial experience in the design of antenna systems for military guidance systems, GPS systems, and wireless communication systems. Saeed has several refereed publications and conference papers in the areas of Antennas and Propagation, Radar Scattering, and Novel Materials. He has been a key player in bringing programmable logic devices and VHDL into the curriculum. Recently he has focused on developing mixed signal concepts using SIMULINK and MALAB. Saeed has multiple papers, a patent, and a patent pending in the field of wireless power transfer.

Currently focused on the Integrated Development of Automated Near-field Wireless Power Transfer (WPT) Systems using Novel Polyimide/Ferrite Nanocomposite Absorber Shields for eVTOL Aircraft. A safe Wireless Power Transfer (WPT) automated system for eVTOL aircraft can bring about improvements in turnaround time for flight operations without the need for human intervention. In support of our campus expertise in the emerging aerospace ecosystem — focused on Advanced Air Mobility (AAM) and the design of a safe, highly efficient near-field wireless power transfer (WPT) system for eVTOL.

PETER D. JOHNSON (CO-AUTHOR)

Pete Johnson is a counter-threats specialist in counter-drone operations. His current focus is Counter-UAS operations advising the DoD and Federal Law Enforcement on commercial and government off the shelf systems supporting force protection for the military, law enforcement, and critical infrastructure.

Culminating 25 years of service to our nation, retiring as a Sergeants Major from the US Army. He is a career Paratrooper and Infantryman, serving in Anti-Armor, Light, Stryker & Airborne Infantry units, Long Range Reconnaissance, and the Asymmetric Warfare Group. Joining the Army to see the world, his duty postings include North Carolina, Maryland, Hawaii, Italy and Germany with deployments supporting combat and contingency operations spanning Bosnia, Sierra Leone, Iraq, Afghanistan, the Middle East, North Africa and Eastern Europe.

Pete continues to serve and give back. Since retiring, his work continues with roles in combat advising against current and emerging asymmetric threats, the commercial CUAS industry and as a CUAS trainer. When able, he volunteers with Team Rubicon. He holds a B.S. in Strategic Studies and Defense Analysis (Summa Cum Laude) from Norwich University and is currently enrolled in the Master Graduate Certificate in Aerospace Cyber Operations from Kansas State University.

In his free time, Pete enjoys the sea and mountains of North Carolina with wife Laura, children Jillian, Christopher and Avery, their bulldog and black lab.

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
ABS	Acrylonitrile butadiene styrene (material
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
A/C FD	Aircraft flood denial

ADS-B Automatic Dependent Surveillance-Broadcast systems

AFRL Air Force Research Lab

A-GPS Assisted GPS

Ag Agriculture sector

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)

AI The ability of machines and technological devices, programs, and creations to sense, process, learn, and adapt to information from their surroundings. (Wright, 2020)

AIS Automated Identification System for Collision Avoidance

A/J Anti-jam

ALBM Ballistic missile launched from a B-47

AMI Agonist-antagonist Myo-neural Interface

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

APAC Asian Pacific Region

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

ARC Adaptive robot chassis

ARW Anti-radiation weapons

ASAT Anti-satellite weapons / Anti-satellite missile system

ASM Attack surface management

ASREN Association of Geospatial Industries, the Arab States Research and Education Network

ASG Autonomous Systems Group

ASW Anti-Satellite Weapons

ATC Air Traffic Control / Air traffic Control Signals

ATCC Air Traffic Control Center

ATHENA Advanced test high energy asset

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.

BASE Bimodal artificial sensory neuron

B&B Branch & bound

B.C. Before Christ

BC Ballistic Coefficient

BCI Brain Control Interface

BEAR Battlefield Extraction-Assist Robot

BEST Biomolecule Extraction and Sequencing Technology

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

BMI Brain Machine Interface

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

CAGR Compound annual growth rate

CAI Counter AI

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

CHATGPT AIs referred to as GPTs (Generative Pre-Trained Transformer)

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

CIWS Close-in weapon system

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

CNSA China National Space Administration

CO-ASAT *Co-orbital (Co-ASAT)* missile system

COMINT Communications intelligence

COMJAM Communications Jamming

COMINT Communications Intelligence

COMSEC Communications Security / Cryptographic 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

COSPAR The Committee on Space Research

COTS Commercial off-the-shelf / Commercial Orbital Transportation Services (COTS)

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)

CRISPR Clustered Regularly Interspaced Short Palindromic Repeats

CSI Crime scene investigation

CSIS Center for strategic and International Studies

CSLM Quench furnace for studying coarsening in metals

CT Counterterrorism / Counter-Terrorism Mission

CTI Computerized Tomography Image (scan)

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.

CYBORG CYBernetic ORGanism coined by Manfred Clynes (1960) – the increase in human capability through mechanical or electrical means resulting in improved biological, biomechanical or neurological human abilities (Clynes & & Kilne, 1960)

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

DAWIA III Defense Acquisition University Certification Level III – Senior or Advanced

Dazzle Cause temporary blindness with Laser

DBC Digital to Biological Converter

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

DE Dark Energy /Directed energy

DEFCON Defense condition

DEW Directed energy weapons (also, DE) (Nichols & Sincavage, 2022)

DF Direction-finding

DFI Digital Forensic Investigation

DHS Department of Homeland Security

DLL Diode Laser Levelling System

DM Dark Matter

DNA A molecule inside cells that contains the genetic information responsible for the development and function of an organism. DNA molecules allow this information to be passed on from one generation to the next. (Deoxyribonucleic acid)

DOF Degrees of Freedom

DOS Denial of Service attack

DPRK Democratic People's Republic of Korea

DS Deep Space

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

ECET Electronic and Computer Engineering Technology (ECET) program Kansas State University Aerospace and Technology campus

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

ECS Environmental control systems

ECoG Electrocorticography

EEG Electroencephalograms

EHC Extra high voltage

EHS Electromagnetic hypersensitivity

EIV Electronic Vehicles

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 / Extremely low electromagnetic fields

EMI Electromagnetic interference

EMP Electromagnetic pulse – electromagnetic energy.

EMR Electromagnetic radiation

EMRG electromagnetic railguns

EMS Electromagnetic spectrum

EMSEC Emissions security

EN electronic nose

EO Electro-optical system

EOS Earth Observation Satellites

EPSRC European Physical Sciences Research Council

ESA European Space Agency

ESG Environmental, social, & corporate governance

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)

ESA European Space Energy

ET Extraterrestrial

EUMETSAT European Organization for the Exploitation of Meteorological Satellites

EXOMARS Joint mission between ESA & ROSCOSMOS to find signs of life on Mars

FAA Federal Aviation Agency

FC First Contact

FDM Fused Deposition Modeling technique

FES Functional Electrical Stimulation

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

FSS Frequency Selective Surfaces

FY-4 China (FY-4) Lightning Mapping Imager

G G is the gravitational constant, N x m2 / kg2 ; N= Newtons, G = 6.067 X 10-11

GAO Government Accountability Office

GCS Ground control station

GEE Google Earth Engine

GEO Group on Earth Observations

GIS Geographical information system

GLGP Gun-launched guided projectile

GLM Geostationary Lightning Mappers

GLONASS Global Navigation Satellite System

GNC Guidance navigation control

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

GPR General Purpose Robots

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)

HAZMAT Hazardous Materials (may refer to special personnel protective equipment)

HBTSS Hypersonic and ballistic tracking space sensor

HCM Hypersonic cruise missile

HDIAC Homeland Defense & Security Information Analysis Center

HGV Hypersonic glide vehicle

HEAT High-explosive anti-tank warhead

HEL High energy Laser

HELCAP High energy laser counter ASCM program

HELIOS High-energy laser with integrated optical dazzler and surveillance

HPM High powered microwave

HMS Heat management system

HOW Hand-over-word satellite data timestamp defined in (IS-GPS-200G, 2013)

HTV Hypersonic test vehicle

HUMINT Human Intelligence

HVM Hostile vehicle mitigation

HVP High velocity projectile

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

IEEE Institute of Electrical and Electronics Engineers

IFF Identify Friend or Foe

IIIM International, Impartial, and Independent Mechanism

IMU Inertial Measurement Unit

IND Improvised nuclear device

INFOSEC Information security

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

IPM Integrated Pest management

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

LCRD Laser Communications Relay Demonstration

LED Light emitting diodes

LENS Laser-engineered net shaping

LDEF Long Duration Exposure Facility

LGF Low Gradient Furnace

LH Left hand

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

LLCD Lunar Laser Communications Demonstration

LLTR Low-level transit route

LM or L.M. Loitering munitions

LMM Lightweight Multi-role Missiles

LNT Lethal non-trackable debris

LPI Low Probability of Intercept

LPD Low Probability of detection

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

LRL Lunar Receiving Laboratory

LSP Launch Service Providers

LuGRE NASA Lunar GNSS Receiver Experiment

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

MASINT Measurement Intelligence

MAST Micro Autonomous Systems & Technology

MDR Motion detection and recognition

MEA Micro electrode array

MEDUSA (Mob Excess Deterrent Using Silent Audio)

MEMS Micro-electro-mechanical systems

MeRT Magnetic Resonance Therapy

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

MO-1 Microbial Observatory-1

MOA Minute of angle in degrees

MOB Man overboard*

MOPP Mission Oriented Protective Posture (MOPP) Gear

MoU Memorandum of Understanding

MRI Magnetic Resonance Imaging

MRVs Multiple Re-entry Vehicles

mTBI mild Traumatic Brain Injury

MRG Europe – Meteosat Third Generation Lightning Imager

MSFC NASA Marshall Space Flight Center

MSL MARS Science Laboratory

MSRA Methicillin-Resistant Staphylococcus aureus

MT-1 Microbial Tracking-1

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

NEUROSTRIKE Series of cognitive impairment events caused by Cyber, Cognitive, Nanotech, Electronic Gateways, Metaverse and CHATGPT

NGB National Guard Board

NGS NGS = Next generation sequencing – replaces DNA approach in the food security region.

NGO Nongovernmental organization

NHTSA National Highway Traffic Safety Administration

NIEHS National Institute of Environmental Health Sciences

NIR Near Infrared

NKW non-kinetic warfare

NLP Natural language processing

NMA Navigation Message Authentication

NMHA Normal Mode Helical Antenna

NO2 Nitrogen dioxide

NOAA National Oceanic & Atmospheric Agency

NPK amount of nitrogen, phosphorus, and potassium (NPK) in soil

NSA National Security Agency

NV Neurological vulnerability

OCONUS Outside Continental United States

OCSD Optical Communications and Sensor Demonstration

ODNI Office of Deputy National Intelligence

OLI Operational Land Imager

OMAR On-Orbit Manufacture, Assembly and Recycling

OMI Ozone Monitoring Instrument

OODA Observe, Orient, Decide, and Act decision loops

OPALS Optical Payload for Lasercomm Science

OPCW Organization for the Prohibition of Chemical Weapons

OPIR Overhead persistent Infrared satellites

OPSEC Operational Security

OSINT Open-source intelligence (also OSI)

OSMA NASA's Office of Safety and Mission Assurance

OST Outer Space Treaty of 1967

OTH Over-the-horizon

PDA Personal digital assistant

PEACOQ Performance-Enhanced Array for Counting Optical Quanta

PFMI Pore formation and mobility investigation furnace / low-temperature furnace for solidification and remelting of transparent materials

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

PNS Peripheral Nerve Stimulation

PNT Positioning, navigation, and timing systems

POV Point of view

PPE Personal protective equipment

PRAM Photovoltaic Radio-frequency Antenna Module technology

PRN Pseudo-Random Noise

PSA Protective security advisors

PSR Primary Surveillance Radar

PSYOPS Psychological warfare operations

QKD Quantum Key Distribution

Quantum Supremacy The point at which quantum computing power outpaces traditional computing power

QUBIT A basic unit of quantum information. A two-state (or two-level) quantum-mechanical system

RAI Responsible Artificial Intelligence

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)

RGB Red Green Blue color band

RH Right hand

RID Remote identification of ID

RIMPAC Rim of the Pacific

RKA Chinese Relativistic Klystron Amplifier

RLLR RLLR indicates only parasitic elements are left-handed

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

ROSCOSMOS Russian Federal Space Agency

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

RRRR RRRR indicates for four-tier system components are all right-handed

RS Remote sensing

RSS Received signal strength / Remote Sensing & Surveillance

RTOS Real time operating system

RTU Remote terminal units

RV Re-entry vehicle

SA Situational Awareness

SAA Sense and Avoid

SAM Surface to Air missile

SAR Synthetic aperture radar

SAR Specific absorption rate – a measure of the rate of RF energy absorbed by the body from the source measured

SATINT Satellite intelligence

SATCOM Satellite communications

SBIRs Space-based Infrared System

SBLM Submarine-launched ballistic missile

SCADA Supervisory Control and Data Acquisition systems

SCMR Strongly Coupled Magnetic Resonant System

SCRAM JET a ram jet in which combustion takes place in a stream of gas moving at supersonic speed

SCS Shipboard control system (or station) / Stereo Camera System / South China Seas

SCS Spinal cord stimulation

SD Space Dominance

SDA Space Domain Awareness / Pentagon Space Development Agency

SDR Software-defined radio

SEAQUE Space Entanglement And Annealing Quantum Experiment

SEAD Suppression of enemy defenses

SECDEF Secretary of Defense (USA)

SIC Successive Signal Interference Cancellation

SICKKIDS Hospital for Sick Children

SIGINT Signals Intelligence

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

SINGULARITY Merger of man and machine (Barfield, 2015)

SM Soil monitoring

SMAs Shape metal alloys

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

SOAD Space Operational Art and Design

Soft damage DEW disruption to a UAS computer

SOCID Self Optimizing Clean In Place

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.

SS Space Shuttle

SSBN Strategic nuclear-powered ballistic missile submarine

SSL Solid state laser

SSLT Seamless satellite-lock takeover spoofing attack

SSN US 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/ SUBSA vertical gradient furnace (transparent growth zone)

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

SWAT Space Warfare Analysis Tools; Special Weapons and Tactics

T & T Track and Traceability

T2AR T2 Augmented Reality project

Taiwan ROC Taiwan is officially the Republic of China

TALOS Tactical assault light operator suit

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.

TED Technology, Entertainment, Design "Talks"

THOR Tactical high-power operational responder

TIROS Television InfraRed Observational Satellite

TMS Transcranial magnetic stimulation

TNT Trinitrotoluene

TO Theater of Operations

TOA Time of arrival

ToF Time of flight

TPAI Third Party Created (invented)

TPS Thermal protective system

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

Un United Nations

UNOOSA The United Nations Office for Outer Space Affairs

USDA US Department of Agriculture

USV Unmanned Surface Vessel

UUV Unmanned underwater vehicle

UWB Ultrawideband

VAR Visual-aural Range

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

WHO World Health Organization

WLAN Wide Local area network

WMD Weapons of Mass Destruction

WMDD Mini-Weapons of Mass Destruction and Disruption

WMO World Meteorological Organization

WPT Wireless Power Transfer

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)

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.

Drake Equation. An equation proposed by Cornell astronomer Frank Drake in 1961, what attempts to calculate the number of sentient species which could exist and are potential contacts during the life of our civilization.

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)[3]

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

- C*ountermeasures:* 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., Unmanned Vehicle Systems and Operations on Air, Sea, and Land, 2020)

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:

$$\mathbf{Cxcorr}(a, b, d) = \sum_{I=0}^{N-1} ai \cdot bI + d \bmod N \qquad \textbf{Eq. 3-1}$$

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 Ǒ (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 the 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)

GO VS. CHESS – Space Dominance should be thought of as a game of GO,[7] NOT chess. In the former, the opponent aims to encircle (strangle) the opponent and deny him his strategic maneuver capability; in the latter, the opponent aims to completely deprive him of individual pieces (assets) or prevent defensive movement so that he can slaughter his ruler (king). (Wright, 2020)

ISR – Intelligence, Surveillance, and Reconnaissance [8]

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.

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).

Light-year – 5.879 x 1012 miles

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)

Sentient – The ability of an organism to perceive and feel things. This definition implies that said organism is capable of rational thought and decision-making.

State – A state can mean a country, a government, or political authority. It means absolute control over a fixed territory on Earth.

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 A Second 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.

Barfield, W. (2015). *Cyber- Humans Our Future with Machines.* NYC: Springer.

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 Dection. *In IGNSS Symposium*, 15-17.

Closas, P., & al., e. (2007). Maximum likelyhood estimation of position in GNSS. *IEEE Signal processing Letters* (pp. 14(5): 359-362). IEEE.

Clynes, M., & & Kilne, N. (1960). Cyborgs and Space. *Astronautics*, sept.

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

87McCallie, 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 .

2628Lopez-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 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, & Carter, H. J. (2022). *Space Systems: Emerging Technologies and Operations.* Manhattan, KS: New Prairie Press.

Nichols, R. &. (2022). Space Electronic Warfare, Jamming Spoofing and ECD. In R. Nichols, & e. al, *Space Systems: Emerging Technologies and Operations* (pp. 112 – 232). Manhattan, KS: New Prairie Press #47.

Nichols, R. K. (2017, October 4). DRONE WARS THREATS, VULNERABILITIES AND HOSTILE USE of UAS. *Presentation at WSU Technology Symposium, Rev 15A*. Wichita, KS, USA.

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

Nichols, R. K. (2021). *SPOOF–PROOF GPS AND ADS-B SECURITY CONSIDERATIONS Rev 12A 09062021.* Carlisle, PA: KSU.

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

Nichols, R. K., & 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. (2022). *Space Systems: Emerging Technologies and Operations.* Manhattan, KS: New Prairie Press # 47.

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

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

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.

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

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

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.*

Szymanski, P. (2019). *How to Fight and Win the Coming Space War.* Retrieved from https://satellitewarcom-my.sharepoint.com/: https://satellitewarcom-my.sharepoint.com/personal/paul_szymanski_satellitewar_com/_layouts/15/onedrive.aspx?id=%2Fpersonal%2Fpaul%5Fszymanski%5Fsatellitewar%5Fcom%2FDocuments%2FPrime%20Briefs%2FHow%20to%20Fight%20and%20Win%20the%20Coming%20Space%20War%20

Szymanski, P. (2020, Jan 27). *Space Operational Art and Design (SOAD).* Retrieved from https://www.dropbox.com: https://www.dropbox.com/s/9jlrjxgbigm7lsv/Space%20Operational%20Art%20and%20Design%20(SOAD)%20-%202020-01-27.xlsx?dl=0

Szymanski, P. (2020, Feb 7). *Space Warfare Analysis Tools (SWAT) Summary.* Retrieved from https://satellitewarcom-my.sharepoint.com/: https://satellitewarcom-my.sharepoint.com/:p:/g/personal/paul_szymanski_satellitewar_com/EYdnXVqvalxPjR6hzOp-C60B9ujGIyIWXtRHWn-5mwaJsw?rtime=Aoc78-sP20g

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

USA, J. C. (2020). *Joint Publication 5-0, "Joint Planning" Doctrine.* Washington: JCS.

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

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.

Wright, J. C. (2020). *Deep Space Warfare: Military Strategy Beyond Orbit.* Jefferson, NC: McFarland & Company.

1026Ng & 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) and the Wildcat UAS/CUAS/UUV/Space textbook series 2017-2023 unless otherwise noted.

[2] EM definitions from (Wolff, 2022)

[3] Since 1998, Christian Wolff has maintained the educational website www.radartutorial.eu

[4] Ơ = 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] AKA wei qi or baduk in Chinese and Korean, respectively.

[8] ISR defined from the USA Army POV only.

TABLE OF CONTENTS

SECTION 2: SPACE THREATS

SECTION 3: SPACE WARFARE, HYPERSONICS, & MATERIALS

TABLE OF FIGURES

SECTION 1: CYBER-HUMAN SYSTEMS (CHS)

SECTION 3: SPACE WARFARE, HYPERSONICS, & MATERIALS

APPENDIX A dB MATH AND PLANE / SPHERICAL TRIGONOMETRY PRIMER

TABLE OF TABLES

SECTION 1: CYBER-HUMAN SYSTEMS (CHS)

SECTION 2: SPACE THREATS

SECTION 3: SPACE WARFARE, HYPERSONICS, & MATERIALS

TABLE OF EQUATIONS

SECTION 1: CYBER-HUMAN SYSTEMS (CHS)

1. The Technological Future – Merging with Machines [Toebes] √
2. CHS Sensors and the Law (Lonstein) √
3. Artificial Brains and Body (Mumm) √
4. Future of Robotics and AI in Space Operations (Hood) √
5. The Reality of Cyborgs and the Look of the Future (Johnson) √

5-1 Risk = Threats X Vulnerabilities X Impacts / Countermeasures

5-2 Risk = Threats / Countermeasures

6. Machines Hacking Machines – Turing's Legacy (C. Carter) √
7. Management Challenges for Mixed Human-Machine Teams (Ryan) √
8. NeuroStrike – The Cyber, Cognitive, Nanotech and Electronic Gateway to Mindfully impaired Metaverse (McCreight) √

SECTION 2: SPACE THREATS

9. Biological Threats and Growth in Space (Sincavage) √
10. Space Electronic Warfare (Nichols) √

10-1 Kepler's Third Law

10-2 The Elevation From The Nadir And Range To A Threat From A Satellite Can Be

10-3 Formula For Received Power To The Receiver

10-4 One-Way Link Equation Gives The Received Power PR In Terms Of The Other Link Components (In Decibel Units).

10-5 One-Way Link Equation Gives The Received Power PR In Terms Of The Other Link Components, In Linear (Non-Decibel Units),

10-6 Power Received By The Satellite Payload Receiver In The Presence Of A Hostile Transmitter

10-7 Power Received By The Ground-Based Receiver Or Hostile Receiver

10-8 Jammed Link Equation

10-9 The *Jamming-To-Signal Ratio (J/S)*

SECTION 3: SPACE WARFARE, HYPERSONICS, & MATERIALS

APPENDIX A DB MATH AND PLANE / SPHERICAL TRIGONOMETRY PRIMER

A-10 $\cos A = \text{cotan } c \tan b$

A-11 $\cos c = \cos a \cos b$

A-12 $\sin a = \sin A \sin c$

PART I

PART 1: CYBER-HUMAN SYSTEMS (CHS)

1.

THE TECHNOLOGICAL FUTURE - MERGING WITH MACHINES [TOEBES]

OBJECTIVES

- Students shall comprehend the different forms of integration of the human body with machines.
- Students shall understand the differences between Replacement of body parts, Augmentation to go beyond human limits and Simulation to fool our senses as well as our Connection to the machines of the world.

INTRODUCTION

The world continues to evolve, and people have always sought to improve how to live and control their interactions with that changing world. With integration between the human body and the many machines that we create, we seek to improve both our longevity and how we experience and perceive everything around us.

This level of integration can be broken into three approaches: *Replacement*, *Augmentation* and *Simulation*. Each of these strategies affect our connection to the world.

In the simplest form, *Replacement* is about substitution of an external creation for a failing or missing part. From life sustaining parts such as artificial hearts to functional prosthetic limbs, the goal is to bring a body up to an expected level of performance.

Taking the next step with *Augmentation* is to make the replacement part perform a function better than what was originally done such as a bionic eye or to add a new function to the body such as infrared vision or magnetic sensing. It is worth noting that there is a fine line between *Replacement* and *Augmentation* based on the intention.

At the extreme, *Simulation* allows feeding external stimuli directly into the body fooling it into believing that something artificial is actually happening. While images of movies like The Matrix may come to mind, this last category is well entrenched in today's youth through online gaming which strives to provide a more realistic and encompassing experience.

All of these strategies for integrating with the machines of the world are predicated on the human mind still being in control. Note that strategies with an Artificially Intelligent entity are addressed in the next chapter.

REPLACEMENT – MECHATRONICS

We have always had a need to replace the functionality of a lost body part to varying degrees. The most obvious being the loss of a limb being replaced by a prosthetic equivalent. It should be no surprise that the oldest known prosthetic is over 3,000 years old: the Greville Chester Great Toe [Figure 1-1] (Daley, 2017) (Choi, 2007) (Dvorsky, 2017) which was made from wood and leather that was made for a 50-60 year old woman. What is significant about this early prosthetic is that it was designed to operate like the body part it replaced unlike earlier ones which were just an imitation of the part but not functional and hence difficult to wear over an extended period.

Figure 1-1: Ancient Egyptian Prosthetic Toe

Image: Dr Jacky Finch, courtesy of the Egyptian Museum, Cairo
Source: https://cdn.mos.cms.futurecdn.net/3g5JAizfnWiPduq9LSJxW8-1200-80.jpg.webp

Another early attempt at replacing a missing limb is the Capua Leg from 300 BC (Copy of Roman artificial leg, London, England, 1905-1915) which was created in bronze. While this was one of the earliest known

leg prosthetics, the construction of it from bronze would have made it uncomfortable to wear. Although the original was destroyed during an Air Raid in World War II, modern 3D printing techniques have allowed researchers at the Peter Osypka Institute of Medical Engineering (Otte & Hazubski, 2019) to create a replica to understand how it originally operated.

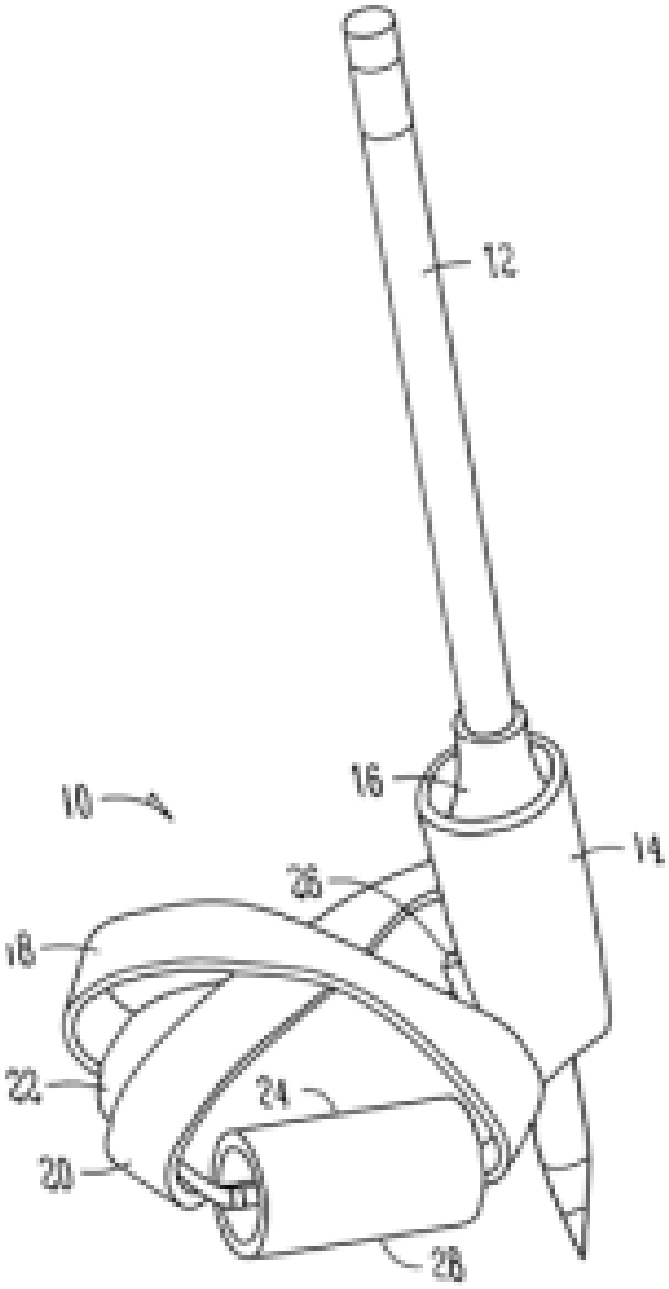
Figure 1-2: Capua Leg – 300BC

Credit: Copy of Roman artificial leg, London, England, 1905-1915. Science Museum, London.
Source: https://wellcomecollection.org/works/kyjgqfuh/images?id=ja6vhwvc

3D PRINTING REPLACEMENT PARTS

It is only in the past couple of decades that 3D printing has progressed to the level that it can be used to create replacement prosthetics. In fact, 3D printing has made it possible for the average person to create a viable substitute limb and digits. We have seen simple designs from six girls on a Girl Scouts based FIRST Lego League team (Iowa Girl Scouts, 2011) who created a prosthetic hand device to enable a 3-year old girl (Figure 1-3) to write (Boyle, 2011). (United States of America Patent No. 8,840,157, 2014)

Figure 1-3: Prosthetic Hand device to enable writing



Source: (United States of America Patent No. 8,840,157, 2014)

Other robotics teams have created more complex designs working with the e-nable organization (Enabling The Future). Based on the e-nablev designs, a FIRST Robotics team of 25 high school students 3D printed a functioning prosthetic hand (Figure 1-4). (FIRST Robotics, 2021)

Figure 1-4: 3D Printed Prosthetic Hand

Source: https://community.firstinspires.org/hubfs/201224202633-01-high-school-robotics-custom-prosthesis-trnd-exlarge-169-1.jpg
From https://community.firstinspires.org/first-robotics-competition-team-creates-prosthetic-hand

Another group has taken the e-nable design to the next level creating an Iron Man themed functioning prosthetic arm (Figure 1-5) (Grunewald, 2016). By creating a series of superhero themed prosthetic limbs, not only have the recipient gained use of a missing limb, the themed prosthetics often cause them to become the envy of their classmates.

Figure 1-5: 3D Printed parts for Iron Man Prosthetic Arm

Source: https://3dprint.com/wp-content/uploads/2016/02/3dp_ironman_enable_parts-e1455887598231.jpg

An advantage of many of these 3D printed prosthetics is that they are inexpensive to manufacture and replace as well as simple to maintain because they rely on existing muscles to control them. However, other advancements in technology have allowed for much more complex control of the replacement parts. It is important to note that for much of the population, a high-quality prosthetic can be out of reach from a cost perspective. It is for this reason that there continues to be innovation in low-end and open-source technologies. Often work goes in both directions to produce high end prosthetics while at the same time using those learnings in order to produce a more cost-effective version.

It is also worth noting that people with replacement parts can perform at some of the highest levels of athletics. Already in the Paralympics we have competitors with prosthetic limbs or wheelchair bound coming close to or even beating Olympic times (Buchholz, 2021). In fact, the performance and perceived advantage of blade running athletes has led to the Olympics committee banning such athletes from competing against athletes without prosthetics, but a study published in the Royal Society Open Science shows that no such advantage exists. (Beck, Taboga, & Grabowski, 2022) The fact that we are having to have this level of discussion attests to the advancement of *Replacement* and shows how we are very quickly moving into the realm of *Augmentation*.

BIOMECHATRONICS

As the technology for replacement of body parts goes beyond the simple mechanical replacement of a body part with another physical replica, the integration of the replacement into the body requires additional technologies applied. This is the realm of biomechatronics in which the biological and mechanical disciplines are combined.

Sometimes the learnings from a full biomechatronic implementation can be used to benefit a fully mechanical implementation.

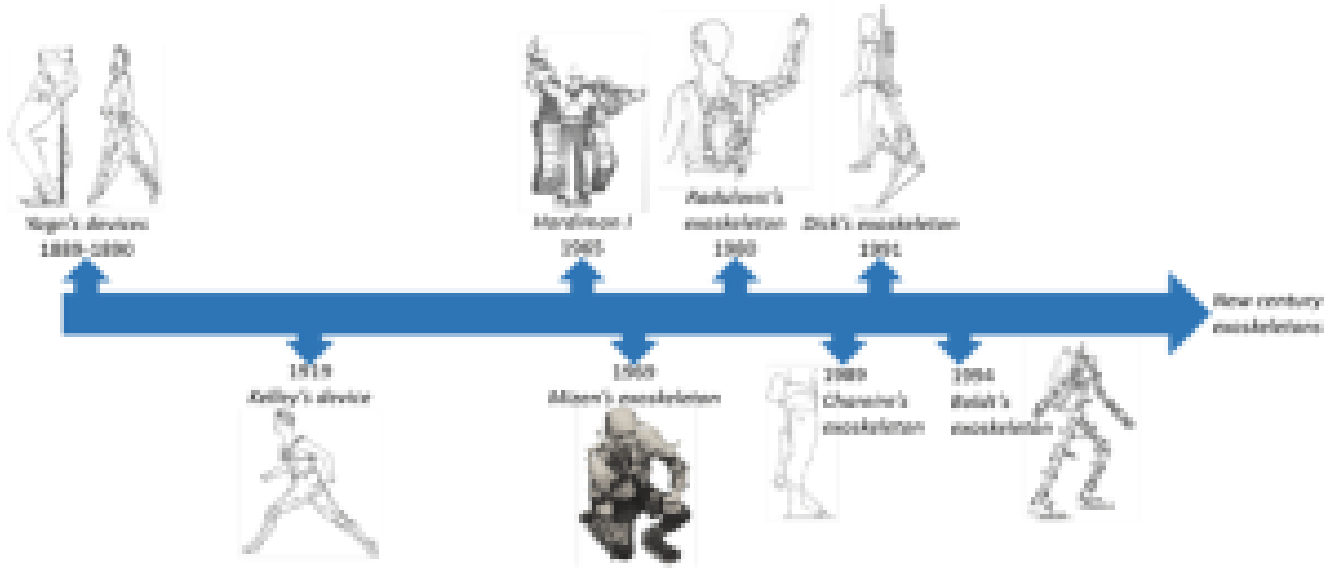
One such example is at MIT where work has been done at both ends of the spectrum. At one end we have the MIT Media Lab biomechatronics group (MIT Media Lab) which has done extensive research on the augmentation front in ways to power a prosthetic knee (MIT Media Lab) and even have engineers who have built their own bionic leg (MIT Media Lab, 2019). At the other end of replacement, they also have teams creating a more cost-effective prosthetic knee which is powered only by springs and gears. (MIT News, 2015) (MIT GEAR Lab) (Chu, 2015)

In addition to MIT, some of the top biomechatronics researchers include the Shirley Ryan AbilityLab (Shirley Ryan AbilityLab) the University of California at Berkeley (University of California at Berkeley), Stanford University (Stanford University), and University of Twente in the Netherlands (University of Twente, 2020). These researchers have been focusing on the critical data gathering necessary to make functioning replacements. This data gathering includes analyzing the complex human motions, determining how to interface electronic components to the human nervous system and experimenting with living muscle tissues as potential actuators for electronic devices.

EXOSKELETONS

While replacement of missing limbs is one approach for allowing people to use them again, when a limb or part of the body becomes paralyzed, another approach to regain use is through an exoskeleton. While this seems like it may be a new technology, in fact the concept of an exoskeleton was first patented in 1890 by Russian inventor Nicholas Yagn (YAGN, 1890). This early exoskeleton was designed as an Augmentation to walking, running, and jumping powered by a combination of springs and compressed fluid. Almost 20 years later, Leslie Kelley patented the Pedomotor (Kelley, 1919) which used steam power to augment human motion with artificial ligaments. Since then, there have been many attempts at exoskeletons as can be seen in Figure 1-6. (Qui, Pei, & Wang, 2022)

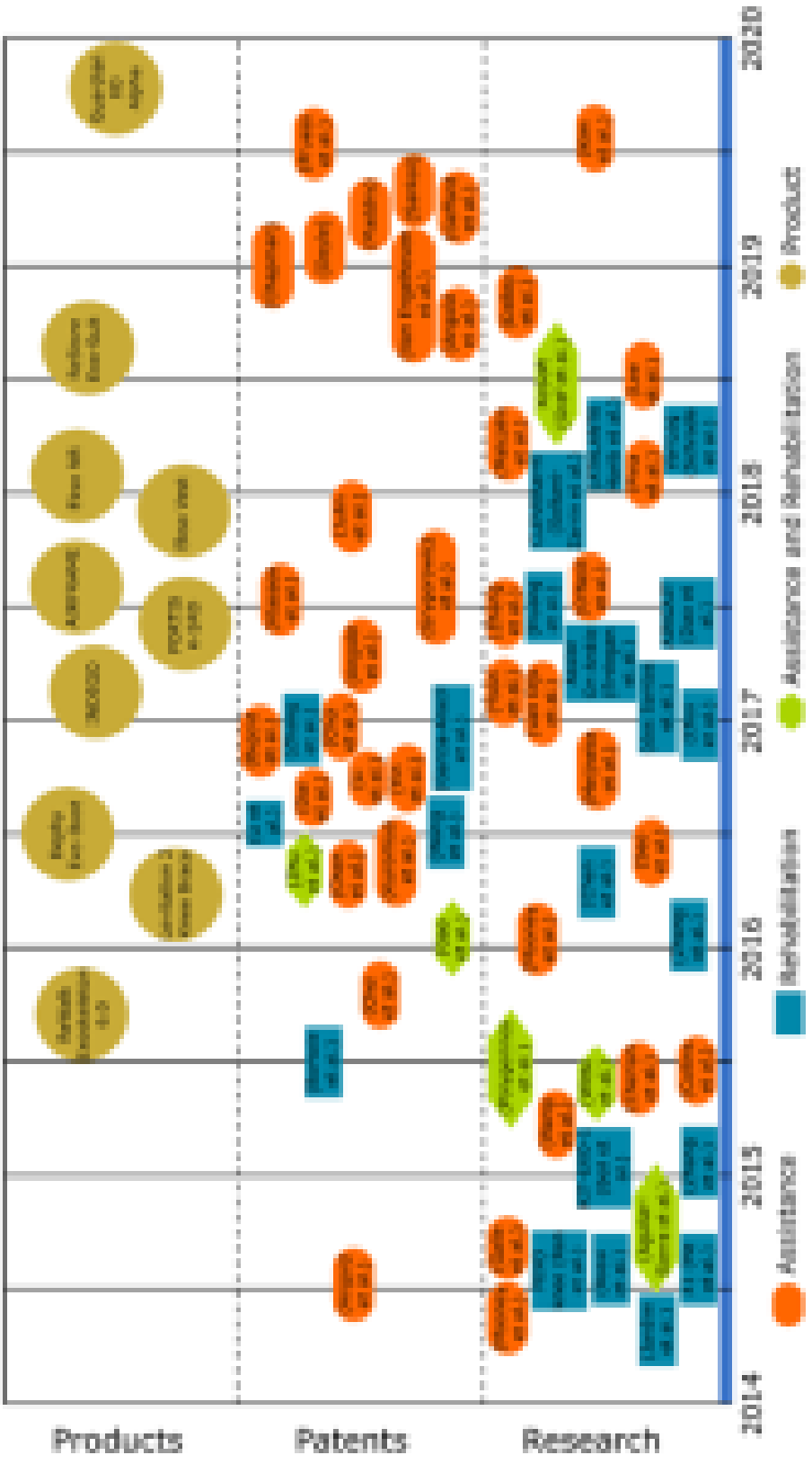
Figure 1-6: Historical Exoskeletons



Source: https://www.mdpi.com/applsci/applsci-11-00076/article_deploy/html/images/applsci-11-00076-g001.png
From: (de la Tejera, Bustamante-Bello, Ramirez-Mendoza, & Izquierdo-Reyes, 2020)
https://www.mdpi.com/2076-3417/11/1/76

More modern research and development of exoskeletons can be split into either rehabilitation (e.g., *Replacement*) or assistance (*Augmentation*) (de la Tejera, Bustamante-Bello, Ramirez-Mendoza, & Izquierdo-Reyes, 2020). The Military is a major source of research into this technology both to provide recovery to veterans wounded on the battlefield and to augment the abilities of soldiers enabling them to carry more, move faster and avoid fatigue. Some of the recent efforts can be seen in Figure 1-7. (Qui, Pei, & Wang, 2022)

Figure 1-7: Timeline of Exoskeletons 2014-2020



Source: https://www.mdpi.com/applsci/applsci-11-00076/article_deploy/html/images/

applsci-11-00076-g004.png
From (de la Tejera, Bustamante-Bello, Ramirez-Mendoza, & Izquierdo-Reyes, 2020) https://www.mdpi.com/2076-3417/11/1/76

While many of these exoskeletons are far beyond the reach of the average consumer, some of the research has resulted in products that are being targeted at people who wish to extend their travel and adventuring range. One such product is the Shift Robotics AI powered Moonwalker shoes which are designed to allow a person to walk 250% faster (Figure 1-8). (Shift Robotics, 2023). Another crowdfunded product is also an AI powered device – the Hypershell Exoskeleton which is designed to give a person 25KM or range offsetting 30KG of weight. (Figure 1-9) (Hypershell, 2023). In the mid-range offering is the suitX exoskeleton which both enables a paraplegic individual to walk (Ashley, 2017) and is targeted to industry to augment a person doing their daily tasks by reducing the muscle strain of heavy lifting and increasing the endurance of the individual using the suit. (Ottobock, 2021)

Figure 1-8: SHIFT MoonWalkers

Source: https://cdn.shopify.com/s/files/1/0652/6238/7422/products/1.jpg
From: https://shiftrobotics.io/products/moonwalkers

Figure 1-9: Hypershell

Source: https://c1.iggcdn.com/indiegogo-media-prod-cld/image/upload/c_limit,w_695/v1679988592/srxnwvrvzcj3bbhn03tv.png
From: https://www.indiegogo.com/projects/hypershell-exoskeleton-for-everyday-adventure--2

GIANT EXOSKELETONS

No discussion of exoskeletons can be had without looking at the giant robots that are created for recreational purposes. Although not technically an exoskeleton, the largest moving robot mech in the world is the 18 meter (59ft) tall "life-size" Gundam RX-78 (Figure 1-10) in Yokohama, Japan (Japan, 2020). For Transformers fans, The J-deite RIDE is a 4 meter (13 foot) tall transforming robot that converts from a drivable car to a walking robot (Figure 1-11). (BRAVE ROBOTICS Inc., 2018)

Figure 1-10: Gundam Factory Moving RX-78 Gundam

Source: https://gundam-factory.net/images/gallery/second/second_006.jpg
From: https://gundam-factory.net/gallery/2nd_anniv/

Figure 1-11: J-diete Ride Transforming Robot

Source: https://j-deite.jp/wp-content/uploads/2018/04/P1190431-2.jpg
https://j-deite.jp/wp-content/uploads/2018/04/j-deite-ride-5.jpg
From: https://j-deite.jp/en/portfolio_page/j-deite-ride/

When someone wants to push the limits of an exoskeleton, think no further than what was built to compete in a robot duel. At 13 feet tall, weighing in at 4 metric tons (12,000 pounds) Kuratas (Kuritas, 2023) (HT Tech, 2021) was built by the Japanese company Suidobashi Heavy Industry (Figure 1-12) . Kuritas participated in a match defeating Megabots Mark II and then tap out when Megabots Eagle One's chainsaw ripped into Kuritas's arm on October 17, 2017 (Carter, 2017). For a while they even offered the robot for sale on Amazon in Japan for the tidy sum of 120 million yen (US$1,008,000). (Baseel, 2015)

Figure 1-12: Kuratas

Source: https://images.hindustantimes.com/tech/img/2021/05/14/960×540/965492_Wallpaper2_1621008380272.jpg
From: https://tech.hindustantimes.com/photos/kuratas-japan-s-futuristic-robot-photo-62Ez674kIU0EyCkfrFGTUK.html

Another exoskeleton robot was built by Taguchi Industrial Co., Ltd – the Super Guzzilla (Figure 1-13) which features their Guzzilla series concrete crusher claws. (Taguchi Industrial, 2023). This robot stands four meters (13.1 feet) tall and weighs 15 metric tons (33,000 pounds). When members of the public were given an opportunity to sit inside Super Guzzilla, they were given a virtual experience through an Oculus Rift VR headset with the actual robot controls driving the virtual robot. (Baseel, 2015)

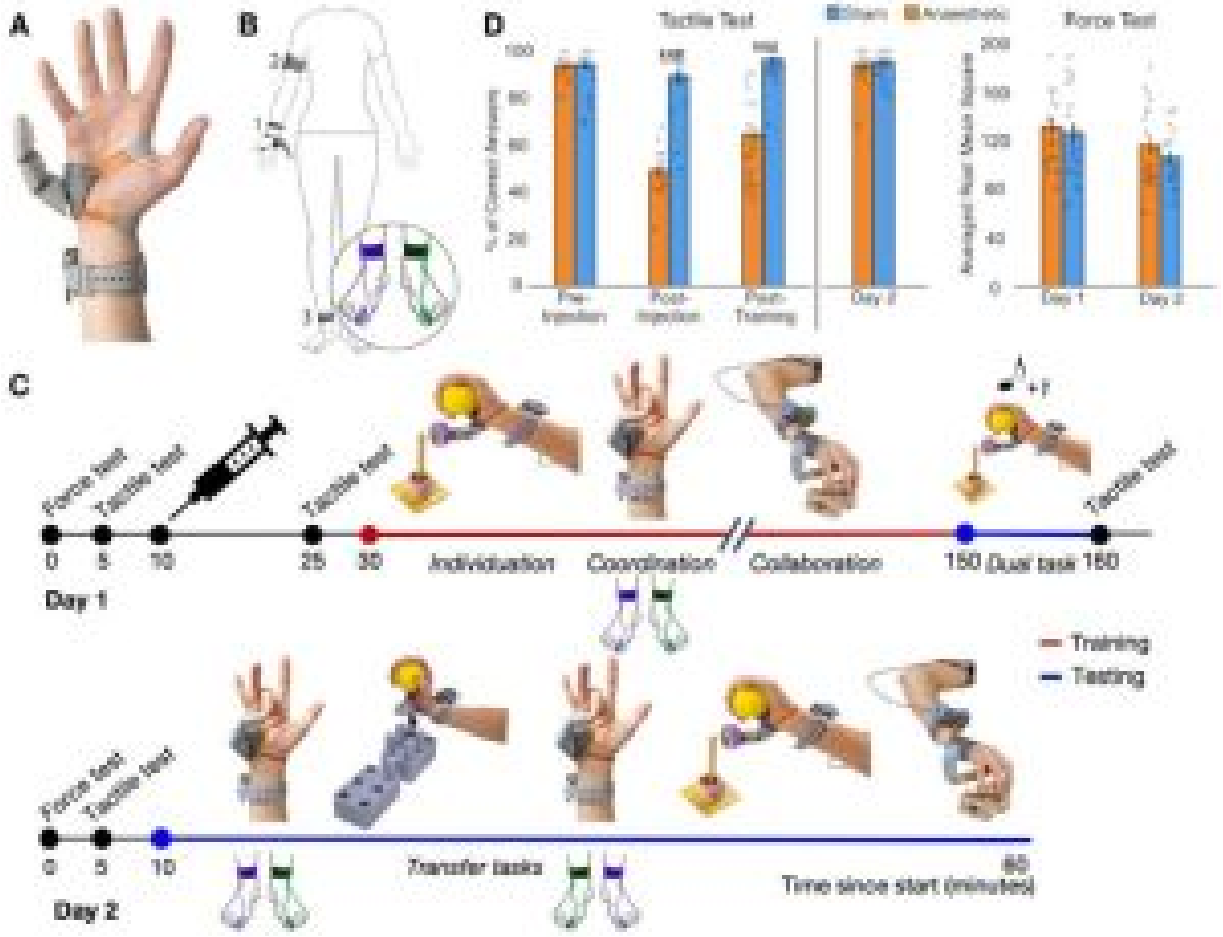
Figure 1-13: Super Guzzilla

Source: https://soranews24.com/wp-content/uploads/sites/3/2015/07/gr-3.jpg
From: https://soranews24.com/2015/07/19/you-can-take-this-33000-pound-robot-for-a-virtual-test-drive-watch-it-dance-to-j-pop-%E3%80%90video%E3%80%91/

EXTRA BODY PARTS

Where prosthetics get to be more interesting is when they are used to add an additional body part to assist in a function. Anyone who has soldered an electronic circuit has always wished for a third hand. For those wanting an extra thumb, Dani Clode at Cambridge University created a 3D-printed thumb that can be added to any hand. (Amoruso, et al., 2022) (Figure 1-14). Other uses envisioned are a surgeon who wants to hold a camera while doing shoulder surgery so that they can control where it points instead of having to rely on an assistant. (Davis, 2023)

Figure 1-14: Extra thumb – Photograph: Tom Stewart



Source: (Amoruso, et al., 2022)
via Creative Commons Attribution 4.0 International License

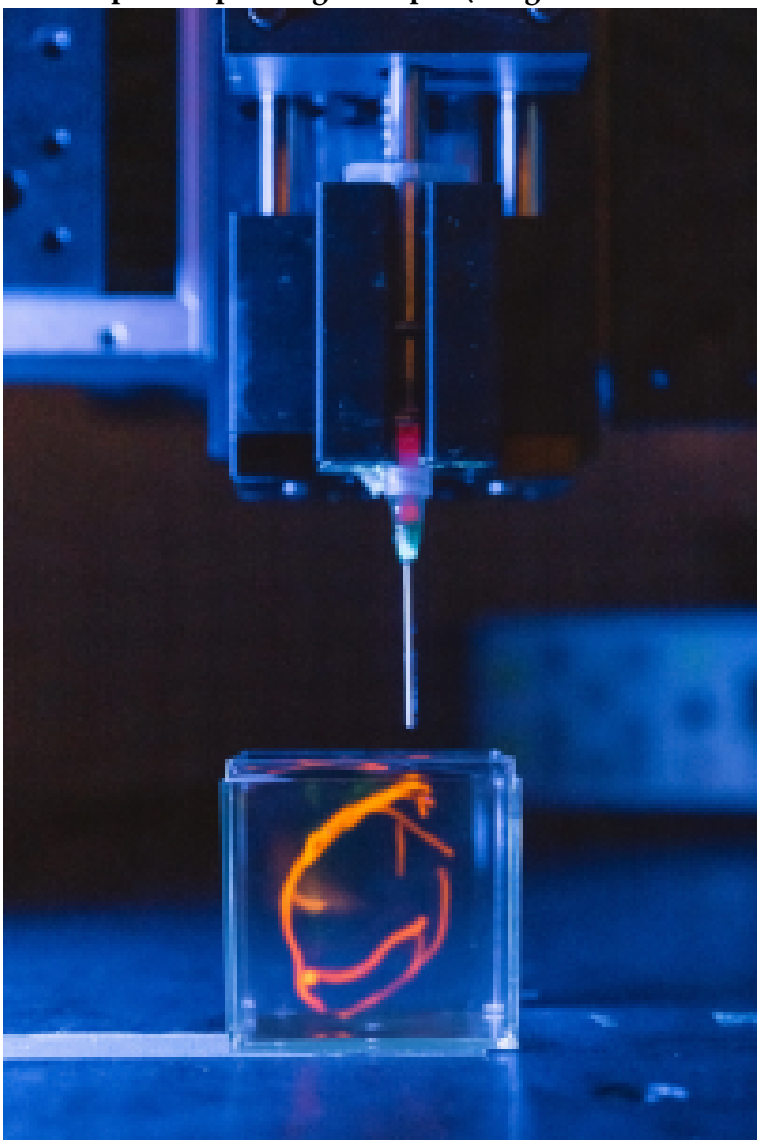
3D PRINTING BIO PARTS

While prosthetics and exoskeletons can help with a missing or non-functioning limb, internal organs require a completely different approach for replacement. Transplanting an organ from another human requires careful type matching and immunosuppression treatment in order to prevent rejection of that organ. Some inroads in a machine to replace an organ have been made for the heart as well as external organs such as the kidney with a dialysis machine. However, the advent of rapid prototyping and bio materials offers an opportunity to create replacement organs which can be created from the recipient's own cells. (Wang, 2019) (Wikipedia, 2023)

The bioengineers at Stanford University have been looking at how to approach building a human heart. (Levin, 2022) They start with modified stem cells processed through a centrifuge into a paste-like substance that is then printed into a gelatinous 3D structure (Figure 1-15). While the bio printers being used at the

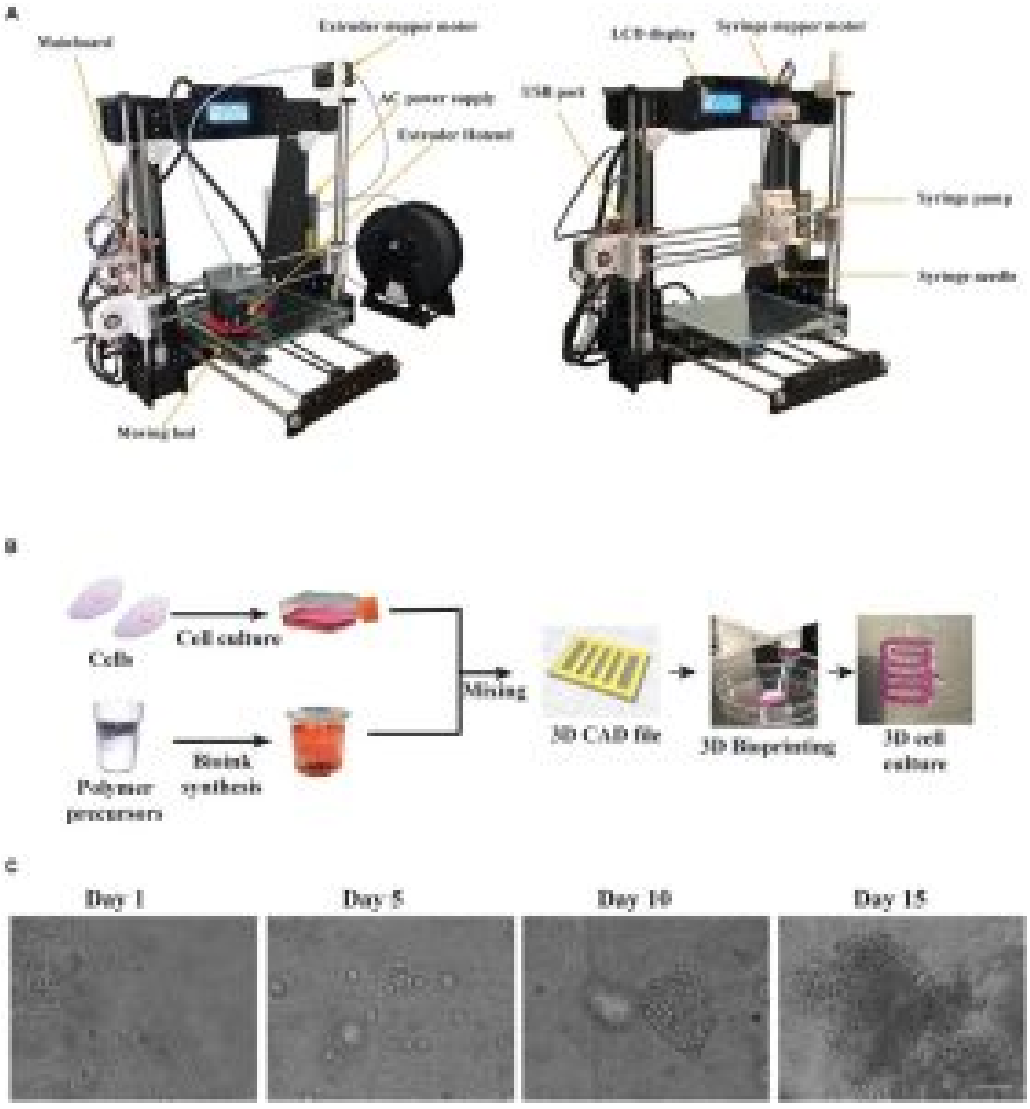
research level can be quite costly, a team of students from Ludwigs-Maximillians-Universität and the Technische Universität München won the 2016 Hackaday Prize when they repurposed a low-end Ultimaker 2+ 3D printer with a syringe to show how it can be used for 3D Bioprinting. (Hofmann, 2016). In 2012, students in the University of Patras, Greece collaborated in modifying an Anet A8 3D printer (Figure 1-16) to 3D print stem cells cultivated from wild mice. (Melanie, Markus, Phillipp, & Oliver, 2019)

Figure 1-15: 3D bioprinter printing a sample. (Image credit: Andrew Brodhead)



Source: https://news.stanford.edu/wp-content/uploads/2022/03/20220204_3D_Bioprinting_N6A8376.jpg
From: https://news.stanford.edu/2022/03/14/building-heart-one-layer-time/

Figure 1-16: 3D Printing mice stem cells on an Anet A8 printer



Source: https://www.frontiersin.org/files/Articles/580889/fbioe-08-580889-HTML-r2/image_m/fbioe-08-580889-g001.jpg
From: (Melanie, Markus, Phillipp, & Oliver, 2019)

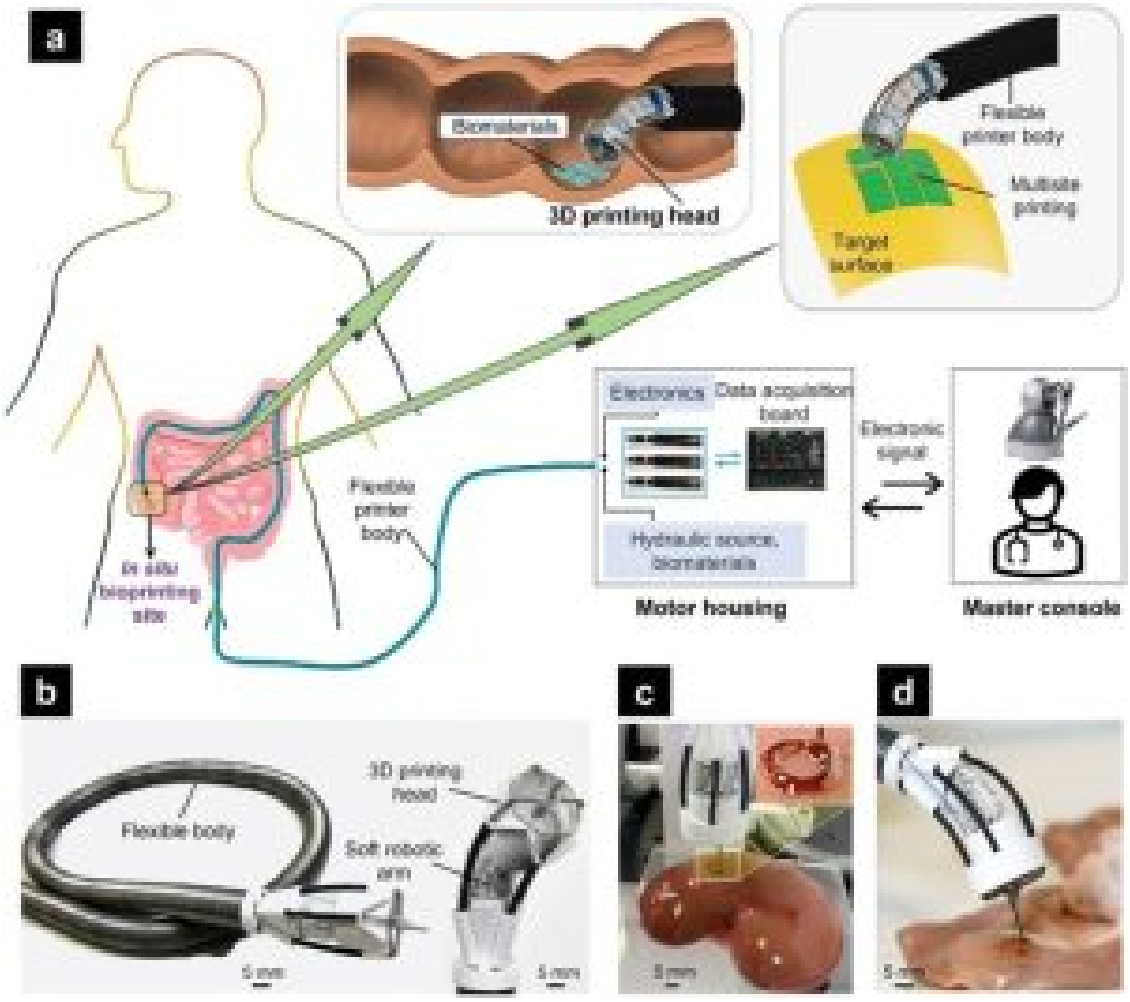
MODIFYING THE BODY FROM THE INSIDE

It is one thing to manufacture a part outside the body and insert it, but we want to think about how machines could inhabit our body and automatically repair it. One approach to repairing the body is the use of hydrogels that are injected into targeted areas to assist the natural body repair mechanisms or even replace diseased tissues. Researchers at MIT and Harvard university have been working on models for how these granular hydrogels

can be used both in 3D Bioprinting and injected into tissue. (Trafton, 2023) (Verheyen, Uzel, Kurum, Roche, & Lewis, 20223)

The next step is to have the 3D printer work inside the body to 3D print living cells directly on top of an organ. Researchers as UNSW Sydney Australia have developed 3D printer with a soft printer head (Figure 1-17) that can be inserted endoscopically and print directly inside the body. (Firtina, 2023)(Thai, et al., 2023)

Figure 1-17: 3D Printing inside the body



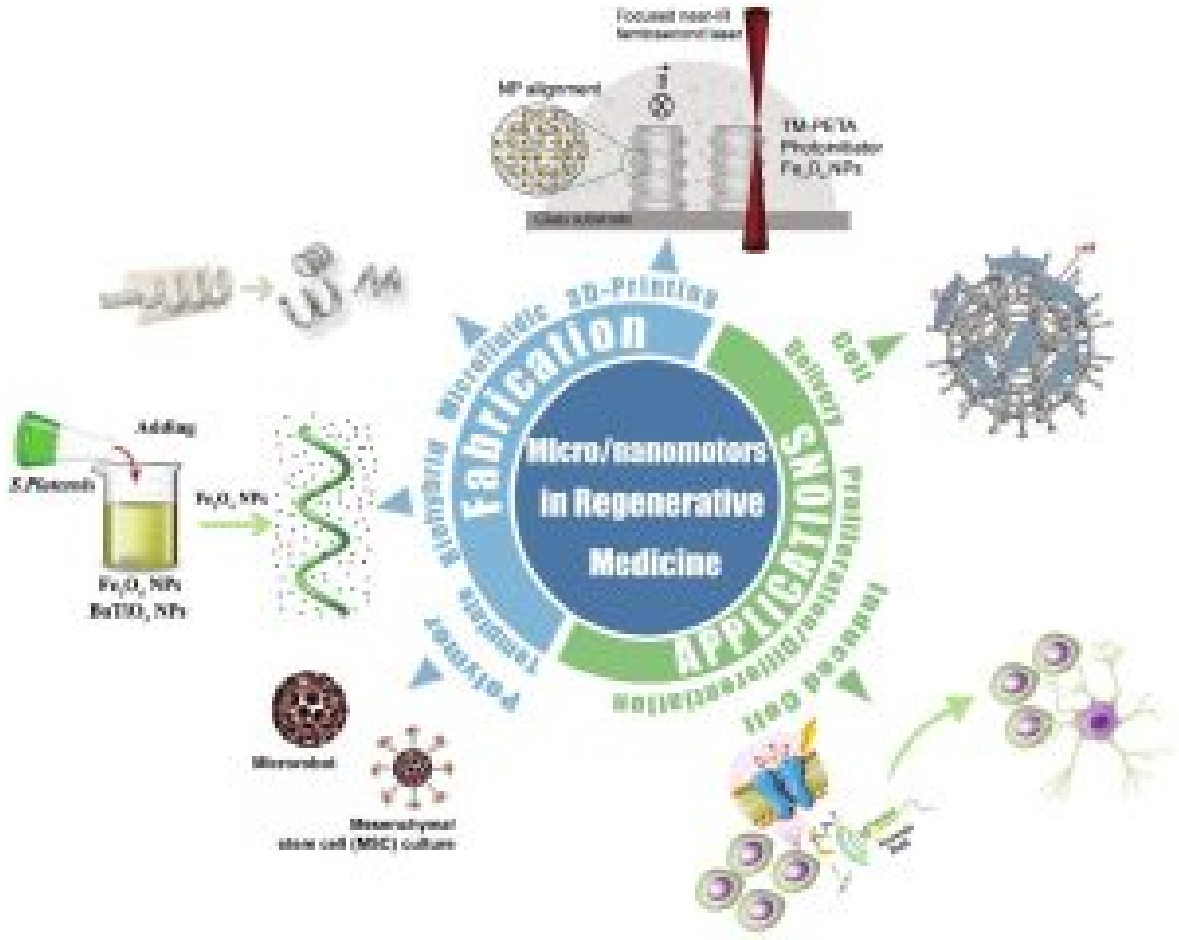
Source: https://onlinelibrary.wiley.com/cms/asset/9c5f5c50-5e03-4ef7-8ef6-d0f029f16ab4/advs5284-fig-0001-m.jpg
From: (Thai, et al., 2023)

The extreme version of this is a series of tiny machines that live in our body fixing whatever they find is wrong. This is the realm of Nanorobotics (Nanorobotics, 2023) and Nanomedicine (Nanomedicine, 2023) with active research driven by the National Nanotechnology Initiative (National Nanotechnology

Coordination Office, 2023). While a general purpose nanobot for the human body is not currently available, this targeted research includes using nanoparticles to deliver medication directly to cancer cells (Aggarwal & Kumar, 2022) and regeneration of bone and tissue. (National Nanotechnology Coordination Office, 2023)

In order to perform their functions, these nanoscale robotic devices need to be able to move effectively through the body. There are multiple strategies for creating these nanomotors including 3D Printing, microfluid spinning, integration of biological and synthetic materials and using a porous polymer template as a scaffold (Figure 1-18) (Liu, Gao, & Peng, 2022). In addition to being able to move through the body to target a particular cell or set of cells, nanoscale robots can also be used to help regulate the growth and differentiation of cells.

Figure 1-18: Micro/nanomotors in Regenerative Medicine

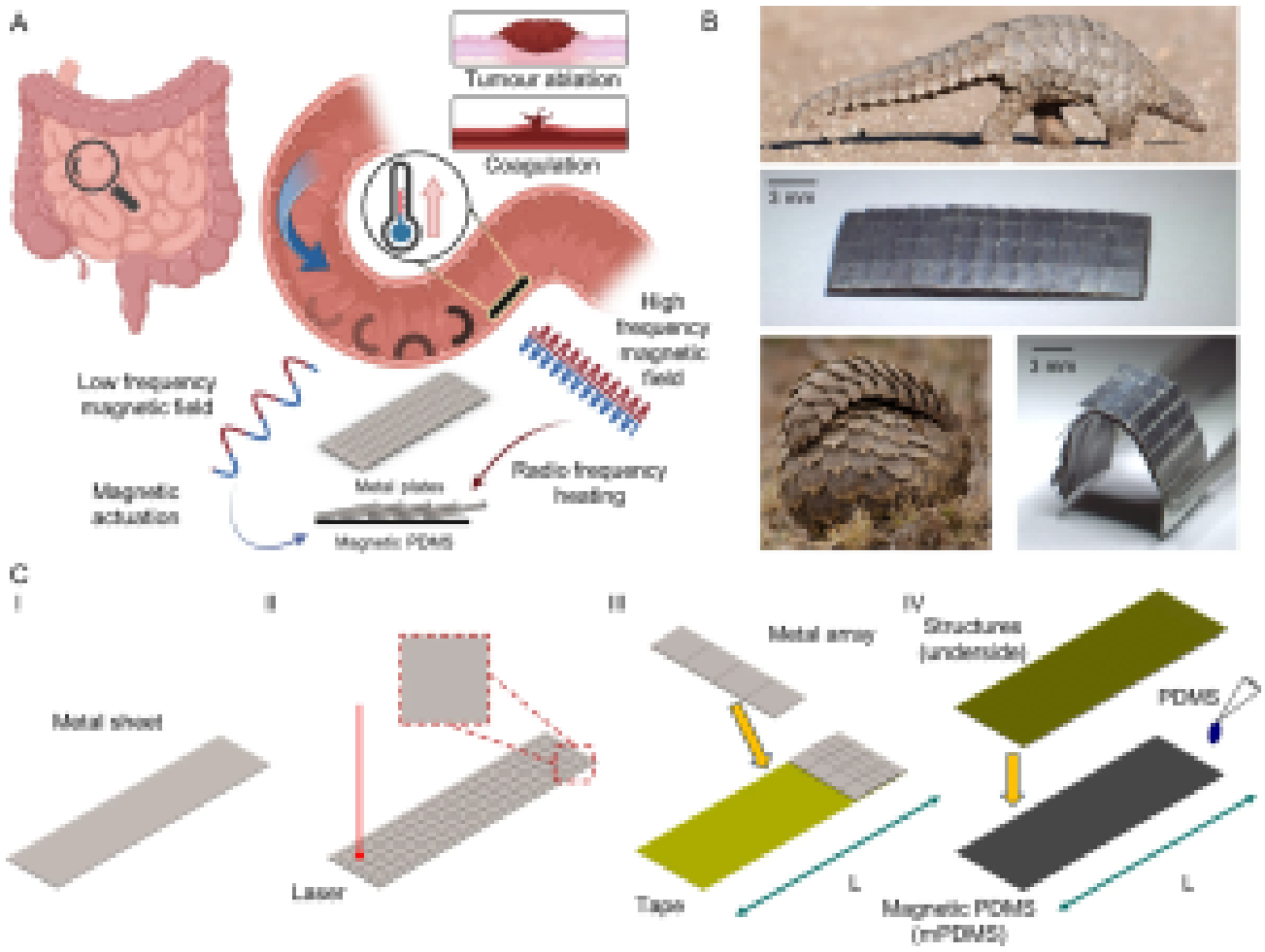


Source: https://ars.els-cdn.com/content/image/1-s2.0-S2590049822000777-gr1_lrg.jpg
From: https://www.sciencedirect.com/science/article/pii/S2590049822000777

Another approach for nanorobots in the body is to provide the power from outside the body in order to control where the treatment is to be applied. (Soon, et al., 2023). These untethered robots can be directed to

a specific location with one frequency of a magnetic field and then switch into a heating mode when a higher frequency is applied. (Figure 1-19)

Figure 1-19: Pangolin-inspired RF heating mechanism for untethered magnetic robots



Source: https://media.springernature.com/full/springer-static/image/art%3A10.1038%2Fs41467-023-38689-x/MediaObjects/41467_2023_38689_Fig1_HTML.png
From: https://www.nature.com/articles/s41467-023-38689-x

BIOHACKING

Instead of waiting for the mainstream to catch up, some individuals have chosen to modify their own body in a process known as biohacking which involves the process of infusing technological components into the body

or by introducing chemical components in order to modify DNA. What is key here is that these modifications are done using therapies and technology which has not gone through any governmental certification.

BIOHACKING – IMPLANTS

Implanting a device or magnet into an arm or hand is one of the simplest forms of biohacking. Steve Haworth is considered a pioneer in the field, implanting magnets into his body over 30 years ago and creating instruments for others to follow in his path. (Haworth, 2023) With a magnet, the individual can sense other magnetic objects and fields (including microwaves) and pick up small pieces of metal (Figure 1-20). A challenge with implanting magnets is that they can degrade over time reducing the function of the magnet and the sense that it brings. (Robertson, 2017).

Figure 1-20: Picking up a paper clip with an implanted magnet

By 1mrln – Own work, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=115315463

A similar problem comes when embedding an RFID tag or other Near Field technology. A Hackaday.io project from 2014 promises to turn you into a "bionic superhero" by implanting a small device into the arm to provide communication with the outside world. (txyz.info, 2014). It is also possible to purchase an NFC Implant for under the skin – a crowdfunded Indegogo campaign in 2013 resulted in the production

of the Dangerous Things xNT NFC chip implant that allows sharing data with NFC enabled smart phones (Dangerous Things, 2019). However, as the technology of the world continues to evolve, the implanted device is limited to accessing devices of the era when it was first implanted. For a person to be able to use their hand to pay for something in a contactless manner requires both a change in technology and agreements with the EMV contactless payment companies. (Graafstra, 2017)

Another problem to be aware of with any device under the skin is the potential for damage to the device or the body around it. After biohacker Lepht Anonym had a file sharing device with a WiFi antenna implanted in her arm, she accidentally damaged it when she hit her arm on the door of a taxi and had to have it removed because of the irritation to her skin. (Teresa, 2022).

Figure 1-21: Project Bionic Yourself (B10N1C) implant in arm

Source: https://cdn.hackaday.io/images/7176431409665975009.jpg
From: https://hackaday.io/project/2736-bionic-yourself-v20

When thinking about device obsolescence, in 2015 the World Economic Forum published a report expecting that implantable cell phones will be commercially available by 2023. (Global Agenda Councel on the Future of Software & Society, 2015). While that hasn't happened, Marty Cooper, who is credited with inventing the first phone in 1973, recently stated that one day we will have phone devices embedded under our skin. (Browne, 2023). We shall leave what happens when it is time to upgrade the device as an exercise for the reader.

BIOHACKING – DNA

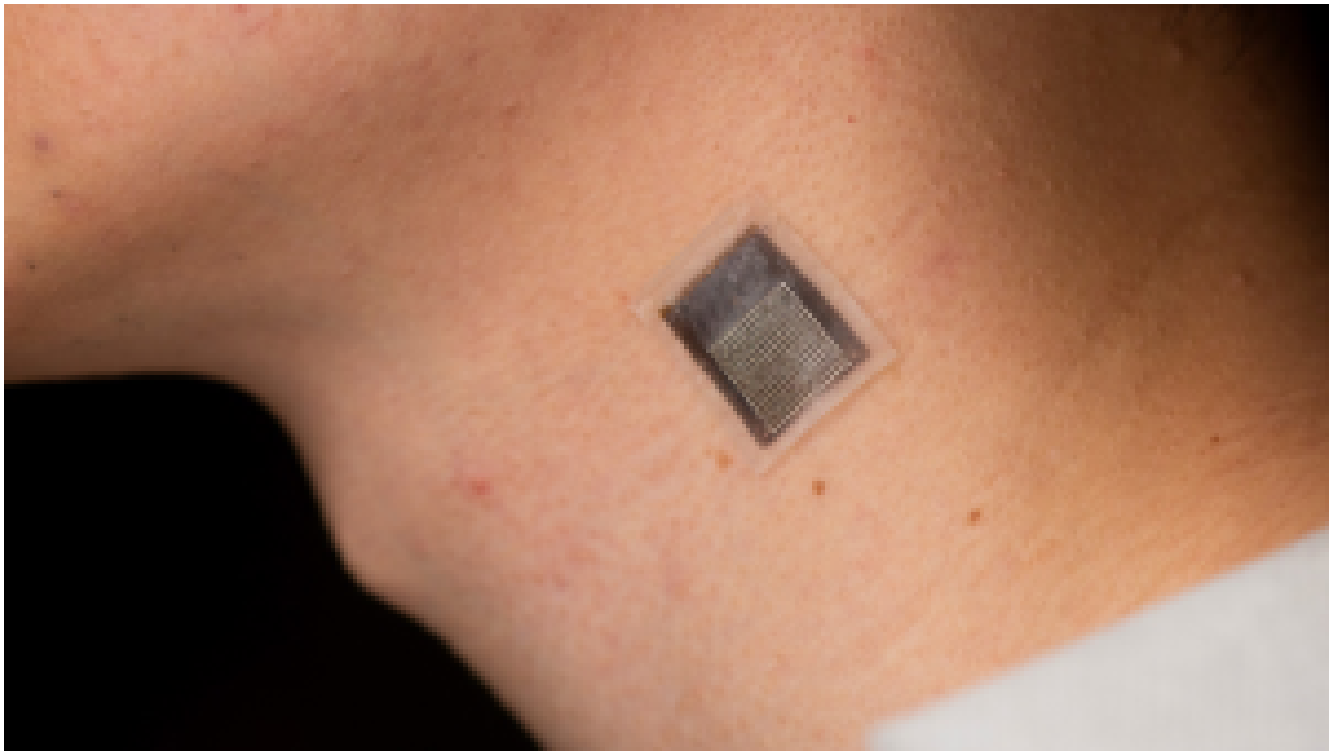
With implanted devices, there is always the option to remove the device. Another approach to biohacking is to target changing the body DNA. Despite all the peril of this form of DIY Gene Therapy, people continue to experiment with it, but often with disastrous results. (Schroeder, 2022) (Zhang, 2018). The use of CRISPR has made it easier for individuals to experiment with genetic engineering to the point that California has clamped down on the sale of kits for injection into individuals. To avoid such government oversight, a biotech startup called Minicircle that wants do to a clinical trial of gene therapy aimed at increasing longevity turned to using NFTs for access to trials in an experimental crypto city in Próspera, Honduras. (Clarke, 2023)

CONNECTING THE BODY

Not every connection to the machines around us requires implanting or modifying the body. Some technology can be done directly through the skin. Users of smart watches are already familiar with the ability to monitor body functions (heart rate, sleep tracking, blood oxygen and temperature). Another way to connect to the outside world is through a tattoo constructed of nanowires on top of a graphene aerogel conductive ink to allow for passive wireless communication to nearby devices without the need for an external power source similar to an RFID tag (Goth, 2023).

For detailed monitoring of muscle activity such as tracking a sports injury or the progress of a disease, researchers from six universities collaborated to create a soft wearable ultrasound sensor (Figure 1-22) that can monitor over an inch and a half deep into the skin. (Halfacree, 2023)

Figure 1-22: Wearable Ultrasonic Sensor

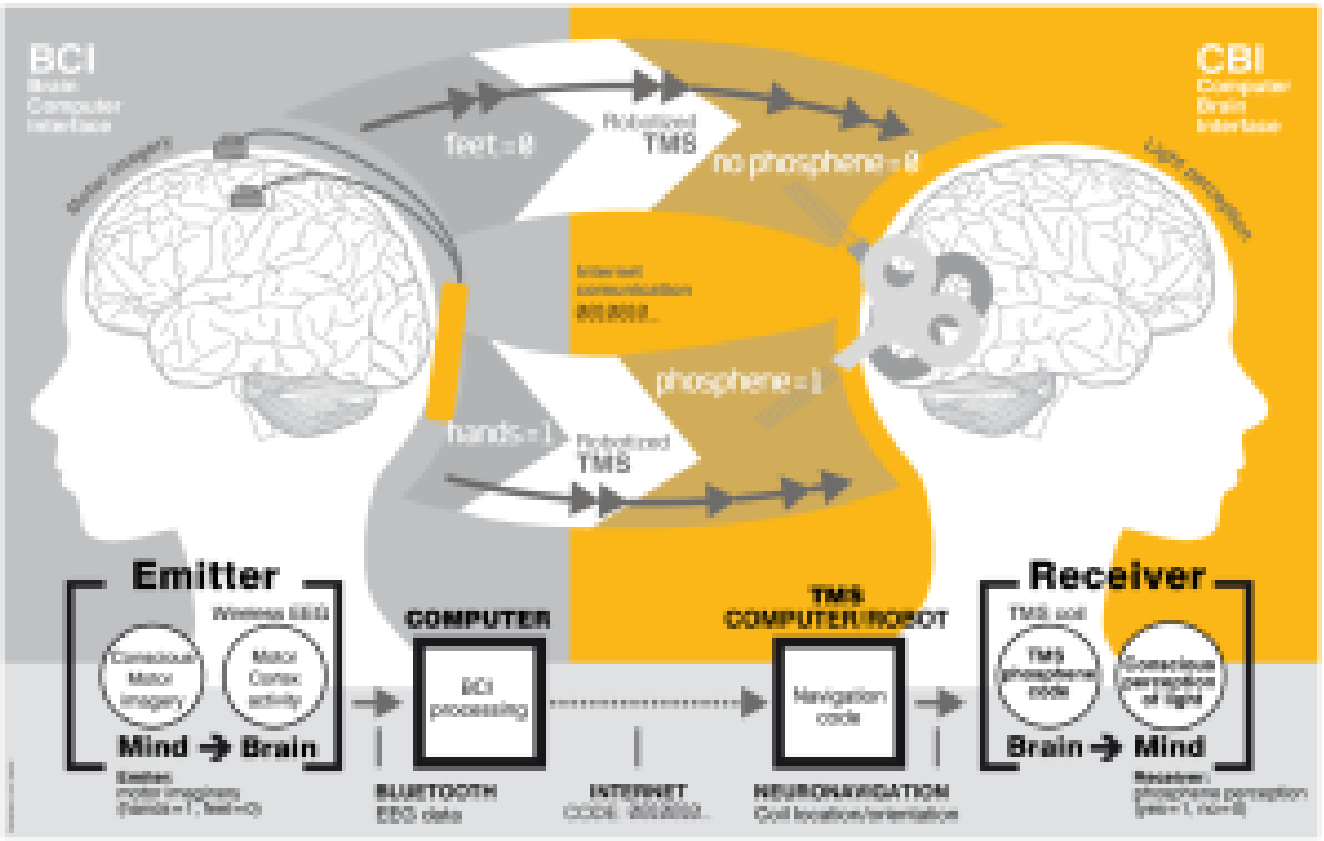


Source: https://hackster.imgix.net/uploads/attachments/1586951/image_WeqaxmgaNW.png
From: https://www.hackster.io/news/a-soft-wearable-ultrasound-sensor-peers-deep-under-your-skin-to-monitor-muscles-and-more-4e349a63eb16

READING THE BRAIN

The ultimate interface to the machines of the world is being able to control it with our thoughts. One of the most promising: Mary Lou Jepsen's OpenWater mind reader is a non-invasive technology that uses light to reconstruct the activity in the brain. (Fazekas, How does OpenWater's mind reader work?!, 2019). This allows for a form of telepathy such that thoughts of one individual can be transmitted to another. (Sánchez, 2023). An early experiment showing that this is possible was done in Barcelona in 2014 in which information read from one subject's brain was encoded as a Baconian cipher encoded information and transmitted to another subject over 7,000 kilometers away to be successfully received. (Figure 1-23) (Grau, et al., 2014)

Figure 1-23: 2014 Telepathy Experiment

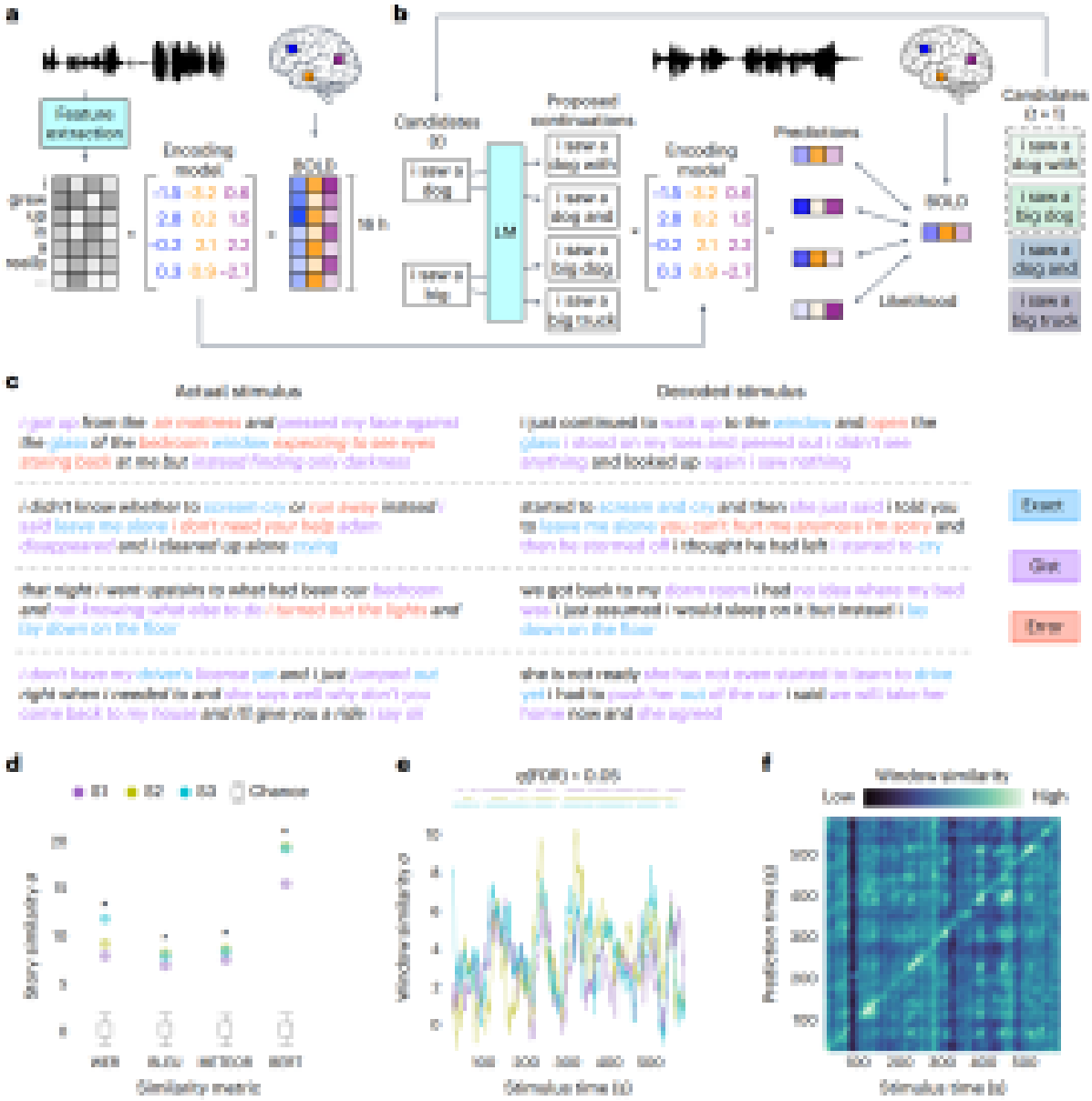


From: (Grau, et al., 2014)
https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0105225

Over 10 years ago, Researchers at the University of California, Berkeley have shown that using functional Magnetic Resonance Imaging (fMRI) combined with some specialized computational models, they were able to reconstruct movie clips of what the person is viewing. (Anwar, 2011). More recently, researchers at the Swiss Federal Institute of Technology Lausanne were able to use AI to predict (Schneider, Lee, & Mathis, 2023) the next frame in a video by monitoring the brains of mice watching the film. (Sharma, 2023)

More recently, the advances in A.I. Large language Models have enabled scientists to use non-invasive brain imaging to reveal the movies in our mind. By recording brain activity while a subject watches a movie the A.I. (based on GPT-1) can construct sentences which describe what the person is seeing. To be successful, it does require cooperation of the subject both during the training session and when determining what they are watching. (Whang, 2023)

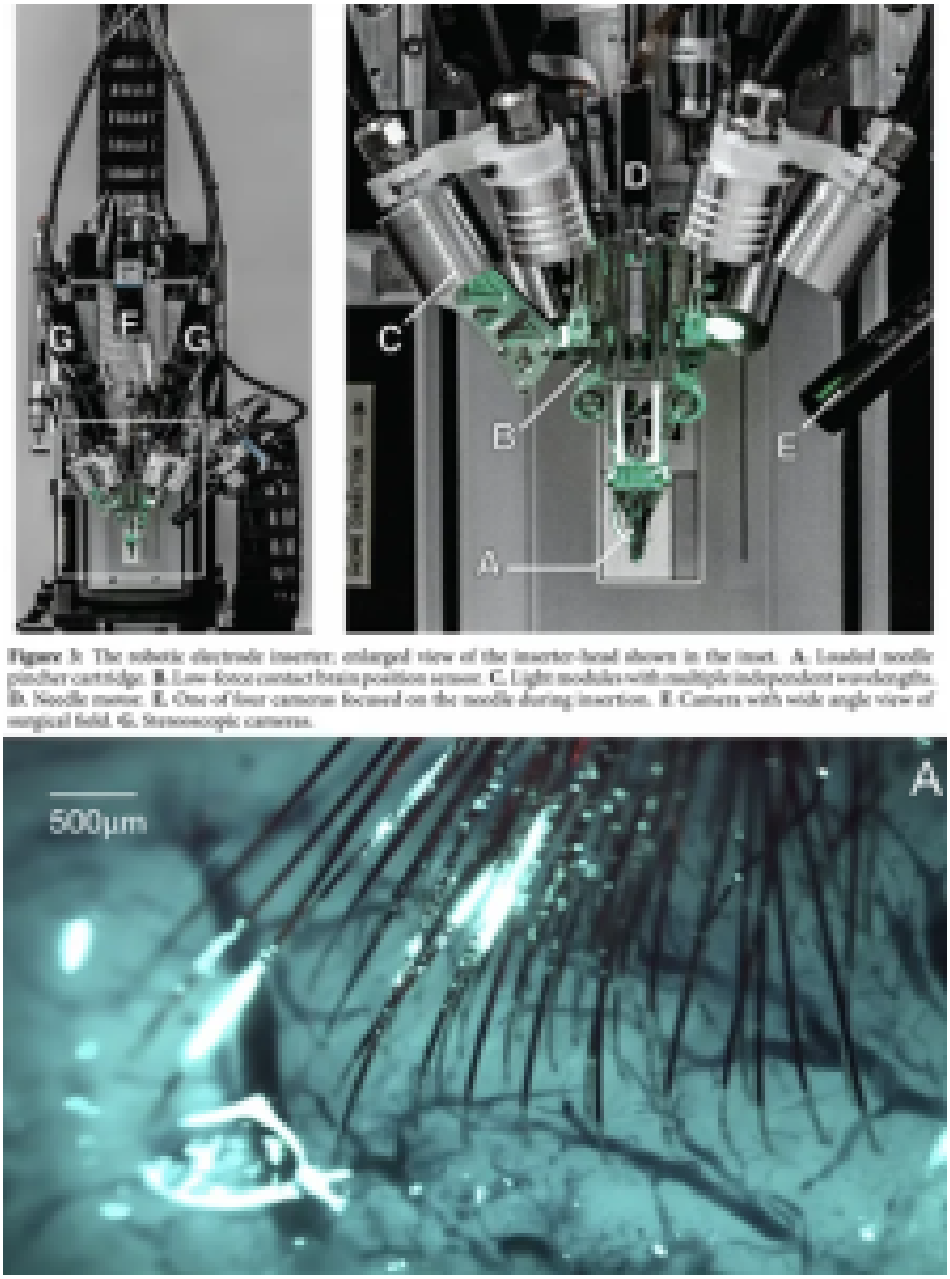
Figure 1-24: Language Decoder for LLM A.I.



Source: https://www.biorxiv.org/content/biorxiv/early/2022/09/29/2022.09.29.509744/F1.large.jpg (Tang, LeBel, Jain, & Huth, 2022)

Elon Musk has taken a more invasive approach to mind reading with the Neuralink device. It consists of a battery-operated device (rechargeable from outside the body) with 1024 electrodes that record neural activity. These electrodes are so fine that it requires a custom surgical robot to perform the implant operation. (Figure 1-25) (Fazekas, Neuralink, OpenWater, DARPA N3, aka how far is the full-immersive (MATRIX style) virtual reality?!, 2019). The FDA has approved the Neuralink for clinical studios (Levy, Taylor, & Sharma, 2023) but nobody has reported being implanted yet.

Figure 1-25: Neuralink insertion robot



Source: https://miro.medium.com/v2/1*h6tAKQO9DdQxC3KCd1wYDA.png

From: https://thebojda.medium.com/neuralink-openwater-darpa-n3-aka-how-far-is-the-full-immersive-matrix-style-virtual-reality-2f5576fa343c

Augmented Reality (AR) and Virtual Reality (VR) Vision

While the brain interface is still in development, Augmented/Virtual Reality hardware and applications are in active development. From a visual perspective with AR, the user gets to see virtual objects and information overlaid on top of the real-world environment. A key feature to make this work is processing power to track the eye and head movements to ensure that the overlaid information matches with the physical world. Switching to a VR mode involves cutting off the visible portions of the real world and replacing it with a completely synthetic world.

With an initial focus on gaming there are four major players in the AR/VR vision market today:

1. Microsoft HoloLens 2 – These goggles provide hand tracking, eye tracking and spatial mapping of the environment to allow the user to see and interact with virtual objects in the real environment. (Microsoft, 2023)
2. Magic Leap ML2 – Currently the lightest of the goggles, it also provides a dimming mode which allow highlighting the virtual objects in an AR mode.(Magic Leap 2, 2023)
3. Meta Quest Pro – Focused more heavily as a VR platform to allow users to collaborate in a Mixed Reality environment (Meta Quest Pro, 2023)
4. Apple Vision Pro – The newest platform which hasn't been released yet, it focuses on merging digital content into your physical space, offering multiple virtual monitors to interact with content (Apple Vision Pro, 2023)

The use of AR goggles isn't necessarily limited to what a user can see. Researchers at MIT have modified a Microsoft Hololens headset to provide the wearer with a form of X-Ray Vision to enable the retail and warehouse workers locate items much faster. (LANDYMORE, 2023)

Another specialized form of Virtual Reality is the Sol Reader which focuses solely on providing an environment simply to read a book blocking out everything else. (Kamp, 2023)

OTHER SENSES IN VR

While VR goggles can go a long way to immersing a person in an environment, the other senses need to perceive being there. Sound is the easiest through headphones giving spatial audio so that the user perceives the location of the object which makes the sound.

Motion in a VR world is one of the more challenging to pull off. To this end, there are multiple companies creating VR treadmills (Figure 1-26) which allow users to move around freely in a virtual environment while keeping them in the same safe location in the physical world. (Virtuix Omni One, 2023). These devices work by tethering the user on top of a platform which allows the user to walk, run, jump, and even swim by tracking the motion of the arms and legs.

Figure 1-26: Virtuix Omni One VR Treadmill

Source: https://omni.virtuix.com/images/virtuix_o1_crouched.jpg
From: https://omni.virtuix.com/

For touch, there are haptic gloves which not only track the hand motion but can provide tactile feedback so that the wearer can sense the objects that they are touching in the virtual world. (HaptX Gloves G1, 2023) (Figure 1-27). To fully experience the pressure and sounds of the environment, users can wear a haptic vest with speakers and motors and even electric shocks to provide feedback to other parts of the body, including a sensation of being attacked while playing a game. (Wöbbeking, 2023)

Figure 1-27: Haptx Force Feedback VR Gloves

Source: https://haptx.com/wp-content/uploads/Glove_Only-1200×1200.jpg
From: https://haptx.com/

The hardest sense to fool is smell. This concept of "smell-o-vision" is difficult to accomplish because of the wide range of chemicals which the human nose can distinguish. As such, most attempts to provide scent to VR involve a limited number of scents typically generated by heating a scented wax. (Donlevy, 2023) (Whit, 2023)

The last sense of course is taste. Unfortunately taste depends very heavily on the sense of smell in addition to the sensors in the tongue. A leading researcher Nimesha Ranasinghe at the University of Maine has been fooling the tongue through the use of electrodes stimulating specific parts of the tongue. (Using Electric Currents to Fool Ourselves Into Tasting Something We're Not, 2017).

AVATARS

These technologies combine to provide for the ultimate pairing of humans and machines – an avatar that

allows a human to be tele-present in a robot at a separate location. This is a VR environment for a person which is fed by sensors on the remote robot. This avatar is useful in environments where a human could not survive, such as deep under water, in the vacuum of space, or on a remote planet with a hostile environment.

Recognizing the need for the technology, the XPrize foundation held an Avatar competition with $10M in prize money (XPrize Avatar Competition, 2023). In November 2022, 17 teams from around the world competed with judges operating the telepresence robots in a simulated space station on an alien planet. The judge had to use the avatar to complete tasks including flipping switches, navigating an obstacle course, identifying a container by wright, operate a drill and even determine whether a rock is smooth or rough by touch. (Ackerman, 2023)

Figure 1-28: NimbRo XPRIZE Avatar Finals Operator Station

Source: http://nimbro.net/AVATAR/images/NimbRo_Avatar_2022_11_05_Finals_Day_2_Operator_Station.jpg
From: http://nimbro.net/AVATAR/

CONCLUSIONS

There are many ways in which we can integrate with the machines and computers of the world. Advancements in A.I and 3D Printing over the past decade have accelerated the rate at which we replace, augment, and connect our bodies to connect with the world.

QUESTIONS FOR STUDENTS

How do you draw the line for when a *Replacement* part becomes an *Augmentation*?
At what point in time does the ability an *Augmentation* provides become a concern for society?

REFERENCES

Ackerman, E. (2023, April 16). *Your Robotic Avatar Is Almost Ready*. Retrieved June 25, 2023 from IEEE Spectrum: https://spectrum.ieee.org/xprize-robot-avatar

Aggarwal, M., & Kumar, S. (2022, September). The Use of Nanorobotics in the Treatment Therapy of Cancer and Its Future Aspects: A Review. *Cureus, 14*(9), e29366.

Amoruso, E., Dowdall, L., Thomas Kollamkulam, M., Ukaegbu, O., Kieliba, P., Ng, T., . . . Makin, T. (2022, January). Intrinsic somatosensory feedback supports motor control and learning to operate artificial body parts. *Journal of Neural Engineering, 19*. doi:10.1088/1741-2552/ac47d9

Anwar, Y. (2011, September 22). *Berkeley News*. Retrieved June 25, 2023 from Scientists use brain imaging to reveal the movies in our mind: https://news.berkeley.edu/2011/09/22/brain-movies/

Apple Vision Pro. (2023, June 1). From Apple: https://www.apple.com/apple-vision-pro/

Ashley, S. (2017, February 21). *Robotic Exoskeletons Are Changing Lives in Surprising Ways*. Retrieved June 12, 2023 from NBC News: https://www.nbcnews.com/mach/innovation/robotic-exoskeletons-are-changing-lives-surprising-ways-n722676

Baseel, C. (2015, January 8). *Want to buy a giant, rideable robot? Amazon Japan will sell you one*. Retrieved June 16, 2023 from Sora News 24: https://soranews24.com/2015/01/08/want-to-buy-a-giant-rideable-robot-amazon-japan-will-sell-you-one/

Beck, O. N., Taboga, P., & Grabowski, A. M. (2022, January 5). Sprinting with prosthetic versus biological

legs: insight from experimental data. *Royal Society Open Science, 9*(1), 1-13. Retrieved Jun 9, 2023 from Sprinting with prosthetic versus biological legs: https://doi.org/10.1007/s42235-022-00289-8

Boyle, R. (2011, May 2). *Girl Scout Team Patents Prosthetic Hand Device, Helping a Toddler Write For the First Time.* Retrieved June 6, 2023 from Popular Science: https://www.popsci.com/technology/article/2011-05/girl-scout-team-patents-prosthetic-hand-device-helping-toddler-write-first-time/

BRAVE ROBOTICS Inc. (2018, April 10). *Project J-DEITE*. Retrieved June 12, 2023 from J-Diete: https://j-deite.jp/

Browne, R. (2023, March 1). *'Father of the cell phone' says one day we'll have devices embedded under our skin*. Retrieved June 25, 2023 from CNBC: https://www.cnbc.com/2023/03/01/mobile-phone-inventor-next-generation-will-have-devices-in-their-skin.html

Buchholz, K. (2021, August 24). *Chart: Where the Paralympics Beat the Olympics.* Retrieved June 9, 2023 from Statista: https://www.statista.com/chart/25606/paralympics-olympics-comparison/

Carter, J. ". (2017, October 19). *The Giant Robot Duel Was Underwhelming... And That's Okay*. Retrieved June 16, 2023 from GeekDad: https://geekdad.com/2017/10/giant-robot-duel/

Choi, C. Q. (2007, July 27). *World's First Prosthetic: Egyptian Mummy's Fake Toe.* Retrieved June 6, 2023 from Live Science: https://www.livescience.com/4555-world-prosthetic-egyptian-mummy-fake-toe.html

Chu, J. (2015, July 31). *A Low-Cost, High-Performance Prosthetic Knee | MIT Department of Mechanical Engineering.* Retrieved June 8, 2023 from MIT Department of Mechanical Engineering: https://meche.mit.edu/news-media/low-cost-high-performance-prosthetic-knee

Clarke, L. (2023, February 13). *This biohacking company is using a crypto city to test controversial gene therapies*. Retrieved June 25, 2023 from MIT Technology Review: https://www.technologyreview.com/2023/02/13/1068330/minicircle-prospera-honduras-biohacking-follistatin-gene-therapy/

Copy of Roman artificial leg, London, England, 1905-1915. (n.d.). Retrieved June 6, 2023 from Science Museum Group Collection: https://collection.sciencemuseumgroup.org.uk/objects/co84549/copy-of-roman-artificial-leg-london-england-1905-1915-artificial-leg

Daley, J. (2017, June 21). *This 3000-Year-Old Wooden Toe Shows Early Artistry of Prosthetics.* Retrieved June 6, 2023 from Smithsonian Magazine: https://www.smithsonianmag.com/smart-news/study-reveals-secrets-ancient-cairo-toe-180963783

Dangerous Things. (2019, June 24). *xNT NFC Chip*. Retrieved June 25, 2023 from Dangerous Things: https://dangerousthings.com/product/xnt/

Davis, N. (2023, March 2). *Human augmentation with robotic body parts is at hand, say scientists*. From The Guardian: https://www.theguardian.com/science/2023/mar/02/human-augmentation-with-robotic-body-parts-is-at-hand-say-scientists

de la Tejera, J. A., Bustamante-Bello, R., Ramirez-Mendoza, R. A., & Izquierdo-Reyes, J. (2020, December 24). *Systematic Review of Exoskeletons towards a General Categorization Model Proposal.* Retrieved June 9, 2023 from MDPI: https://www.mdpi.com/2076-3417/11/1/76

Dempsey, G. J., Murray, K., Greqell, M., Groat, Z., Pohlen, C., & Anderson, M. W. (2014, September 23). *United States of America Patent No. 8,840,157.*

Donlevy, K. (2023, May 10). *VR 'Smell-o-vision' may enable users to detect dozens of odors*. Retrieved June 25, 2023 from New York Post: https://nypost.com/2023/05/10/vr-smell-o-vision-may-enable-users-to-detect-dozens-of-odors/

Dvorsky, G. (2017, June 21). *This 3,000-Year-Old Prosthetic Wooden Toe is More Incredible Than We Thought.* Retrieved June 6, 2023 from Gizmodo: https://gizmodo.com/this-3-000-year-old-prosthetic-wooden-toe-is-more-incre-1796274259

Enabling The Future. (n.d.). Retrieved June 6, 2023 from Enabling The Future – A Global Network Of Passionate Volunteers Using 3D Printing To Give The World A "Helping Hand.": https://enablingthefuture.org/

Fazekas, L. (2019, May 19). *How does OpenWater's mind reader work?!* Retrieved June 25, 2023 from Medium: https://thebojda.medium.com/how-does-openwaters-mind-reader-work-750bea176aeb

Fazekas, L. (2019, July 28). *Neuralink, OpenWater, DARPA N3, aka how far is the full-immersive (MATRIX style) virtual reality?!* Retrieved June 25, 2023 from Medium: Neuralink, OpenWater, DARPA N3, aka how far is the full-immersive (MATRIX style) virtual reality?!

FIRST Robotics. (2021, January 4). *FIRST Robotics Competition Team Creates Prosthetic Hand*. Retrieved June 6, 2023 from community: https://community.firstinspires.org/first-robotics-competition-team-creates-prosthetic-hand

Firtina, N. (2023, February 28). *Watch: 3D printing living cells inside human body becomes a reality*. Retrieved June 16, 2023 from Interesting Engineering: https://interestingengineering.com/health/3d-printing-living-cells-human-reality

Global Agenda Councel on the Future of Software & Society. (2015, November 1). *Deep Shift 21 Ways Software Will Transform Global Society.* Retrieved June 25, 2023 from World Economic Forum: https://www3.weforum.org/docs/WEF_GAC15_Deep_Shift_Software_Transform_Society.pdf

Goth, G. (2023, June 12). *New Nanotattoos Don't Need Batteries or Wires*. Retrieved June 23, 2023 from IEEE Spectrumm: https://spectrum.ieee.org/nano-tattoo

Graafstra, A. (2017, May 1). *Making payments with an implant*. Retrieved June 25, 2023 from Dangerous Things: https://forum.dangerousthings.com/t/making-payments-with-an-implant/643

Grau, C., Ginhoux, R., Riera, A., Nguyen, T. L., Chauvat, H., Berg, M., . . . Ruffini, G. (2014, August). Conscious Brain-to-Brain Communication in Humans Using Non-Invasive Technologies. *PLOS ONE, 9*, e105225. doi:10.1371/journal.pone.0105225

Grunewald, S. J. (2016, February 19). *Three Year Old Gets His Own Iron Man e-NABLE Prosthetic Hand.* Retrieved June 6, 2023 from 3DPrint.com: https://3dprint.com/120465/iron-man-e-nable-hand/

Halfacree, G. (2023, April 5). *A Soft Wearable Ultrasound Sensor Peers Deep Under Your Skin to Monitor Muscles and More*. Retrieved June 25, 2023 from Hackster.io: https://www.hackster.io/news/a-soft-wearable-ultrasound-sensor-peers-deep-under-your-skin-to-monitor-muscles-and-more-4e349a63eb16

HaptX Gloves G1. (2023, June 1). Retrieved June 25, 2023 from haptx: https://g1.haptx.com/learnabout

Haworth, S. (2023). *About Steve Haworth Modified*. Retrieved June 25, 2023 from Steve Haworth Modified: http://stevehaworth.com/about/

Hofmann, J. (2016, September 14). *biotINK – the bioprinter of tomorrow*. Retrieved June 16, 2023 from Hackaday.io: https://hackaday.io/project/14501-biotink-the-bioprinter-of-tomorrow

HT Tech. (2021, May 14). *'Kuratas' Japan's futuristic robot*. Retrieved June 16, 2023 from HT Tech: https://tech.hindustantimes.com/photos/kuratas-japan-s-futuristic-robot-photo-62Ez674kIU0EyCkfrFGTUK-6.html

Hypershell. (2023). *Hypershell: Exoskeleton for Everyday Adventure*. Retrieved June 9, 2023 from Indiegogo: https://www.indiegogo.com/projects/hypershell-exoskeleton-for-everyday-adventure–2#/

Iowa Girl Scouts. (2011, April 20). *Iowa Girl Scouts Invent Prosthetic Hand for Three-Year-Old Girl and Win up to $20,000 to Patent it in Inaugural First® LEGO® League Global Innovation Award*. Retrieved June 6, 2023 from PR Newswire: https://www.prnewswire.com/news-releases/iowa-girl-scouts-invent-prosthetic-hand-for-three-year-old-girl-and-win-up-to-20000-to-patent-it-in-inaugural-first-lego-league-global-innovation-award-120294524.html

Japan, g. (2020, December 2). Retrieved June 12, 2023 from Japan Today: https://japantoday.com/category/entertainment/japan%E2%80%99s-new-life-size-moving-gundam-statue-unveiled-in-full-dramatic-glory

Kamp, H. J. (2023, June 9). *Sol Reader is a VR headset exclusively for reading books*. Retrieved June 25, 2023 from TechCrunch: https://techcrunch.com/2023/06/09/sol-reader/

Kelley, L. C. (1919, July 1). *US1308675A – Pedomotor*. Retrieved June 9, 2023 from Google Patents: https://patents.google.com/patent/US1308675A/en

Kuritas. (2023, June 9). Retrieved June 16, 2023 from Wikipedia: https://en.wikipedia.org/wiki/Kuratas

LANDYMORE, F. (2023, March 2). *HEADSET THAT CAN SEE INSIDE BOXES*. Retrieved June 25, 2023 from Futurism: https://futurism.com/the-byte/mit-headset-find-objects

Levin, D. (2022, March 14). *Stanford bioengineers aim to build a heart, one layer at a time*. Retrieved June 16, 2023 from Stanford News: https://news.stanford.edu/2022/03/14/building-heart-one-layer-time/

Levy, R., Taylor, M., & Sharma, A. (2023, May 26). *Elon Musk's Neuralink wins FDA approval for human study of brain implants*. Retrieved June 25, 2023 from Reuters: https://www.reuters.com/science/elon-musks-neuralink-gets-us-fda-approval-human-clinical-study-brain-implants-2023-05-25/

Liu, S., Gao, C., & Peng, F. (2022). Micro/nanomotors in regenerative medicine. *Materials Today Advances, 16*, 100281. doi:10.1016/j.mtadv.2022.100281

Magic Leap 2. (2023, June 1). From Magic Leap: https://www.magicleap.com/magic-leap-2

Melanie, K., Markus, G., Phillipp, H., & Oliver, F. (2019). Ultra-Low-Cost 3D Bioprinting: Modification and Application of an Off-the-Shelf Desktop 3D-Printer for Biofabrication. *Frontiers in Bioengineering and Biotechnology, 7*. doi:10.3389/fbioe.2019.00184

Meta Quest Pro. (2023, June 1). From Meta: https://www.meta.com/quest/quest-pro/

Microsoft. (2023). *HoloLens 2 Features*. From Microsoft: https://www.microsoft.com/en-us/hololens/hardware

MIT GEAR Lab. (n.d.). *Prosthetic Leg — MIT GEAR Lab.* Retrieved June 8, 2023 from MIT GEAR Lab: https://www.gear.mit.edu/prosthetic-knee

MIT Media Lab. (2019, December 2). *This MIT engineer built his own bionic leg — MIT Media Lab.* Retrieved June 8, 2023 from MIT Media Lab: https://www.media.mit.edu/articles/this-mit-engineer-built-his-own-bionic-leg/

MIT Media Lab. (n.d.). *Overview < Biomechatronics — MIT Media Lab.* Retrieved June 8, 2023 from MIT Media Lab: https://www.media.mit.edu/groups/biomechatronics/overview/

MIT Media Lab. (n.d.). *Transfemoral Powered Prostheses – Biomechatronics.* Retrieved June 8, 2023 from Biomechatronics – MIT Media Lab: https://biomech.media.mit.edu/portfolio_page/cseaknee/

MIT News. (2015, July 31). *A cheaper, high-performance prosthetic knee | MIT News | Massachusetts Institute of Technology.* Retrieved June 8, 2023 from MIT News: https://news.mit.edu/2015/cheaper-high-performance-prosthetic-knee-0731

Nanomedicine. (2023, February 6). From Wikipedia: https://en.wikipedia.org/wiki/Nanomedicine

Nanorobotics. (2023, December 5). From Wikipedia: https://en.wikipedia.org/wiki/Nanorobotics

National Nanotechnology Coordination Office. (2023). *About the NNI*. From National Nanotechnology Initiative: https://www.nano.gov/about-nni

National Nanotechnology Coordination Office. (2023). *Applications of Nanotechnology*. Retrieved June 25, 2023 from National Nanotechnology Initirative: https://www.nano.gov/about-nanotechnology/applications-nanotechnology

Otte, A., & Hazubski, S. (2019, March 3). *The Ancient Artificial Leg of Capua: First 3D Print after 2300 Years.* Retrieved June 6, 2023 from MDPI: https://www.mdpi.com/2673-1592/3/3/19

Ottobock. (2021, November 3). *suitX by Ottobock*. Retrieved June 12, 2023 from suitX: https://www.suitx.com/

Qui, S., Pei, Z., & Wang, C. (2022). *Systematic Review on Wearable Lower Extremity Robotic Exoskeletons for Assisted Locomotion.* J Bionic Eng. From https://doi.org/10.1007/s42235-022-00289-8

Robertson, A. (2017, July 21). *I hacked my body for a future that never came*. Retrieved June 25, 2023 from The Verge: https://www.theverge.com/2017/7/21/15999544/biohacking-finger-magnet-human-augmentation-loss

Sánchez, E. (2023, March 27). *Telepathy Experiments in Silicon Valley*. Retrieved June 25, 2023 from Exploring Your Mind: https://exploringyourmind.com/telepathy-experiments-in-silicon-valley/

Schneider, S., Lee, J. H., & Mathis, M. W. (2023). Learnable latent embeddings for joint behavioural and neural analysis. *Nature, 617*, 360–368. doi:10.1038/s41586-023-06031-6

Schroeder, K. (2022, March 29). *'Biohackers' and DIY Gene Therapy*. Retrieved June 25, 2023 from Front Line Genomics: https://frontlinegenomics.com/biohackers-and-diy-gene-therapy/

Sharma, S. (2023, May 4). *This new AI tool uses brain signals to predict what a mouse sees*. Retrieved June

25, 2023 from Interesting Engineering: https://interestingengineering.com/science/ai-tool-uses-brain-signals-to-predict-what-a-mouse-sees

Shift Robotics. (2023, 1 1). *Moonwalkers Deposit – Shift Robotics.* Retrieved June 9, 2023 from Shift Robotics: https://shiftrobotics.io/products/moonwalkers

Shirley Ryan AbilityLab. (n.d.). *Research | Shirley Ryan AbilityLab.* Retrieved June 8, 2023 from AbilityLab: https://www.sralab.org/research

Soon, R. H., Yin, Z., Dogan, M. A., Dogan, N. O., Tiryaki, M. E., Karacakol, A. C., . . . Sitti, M. (2023). Pangolin-inspired untethered magnetic robot for on-demand biomedical heating applications. *Nature Communications, 14*, 3320. doi:10.1038/s41467-023-38689-x

Stanford University. (n.d.). *Biomechatronics Laboratory.* Retrieved June 8, 2023 from Stanford Biomechatronics Laboratory: https://biomechatronics.stanford.edu/

Taguchi Industrial. (2023, June 16). *Guzzilla D Series Crusher*. From Taguchi Iindustrial: https://www.taguchi-industrial.com/en/product/guzzilla-crasher-d/

Tang, J., LeBel, A., Jain, S., & Huth, A. G. (2022). Semantic reconstruction of continuous language from non-invasive brain recordings. *bioRxiv*. doi:10.1101/2022.09.29.509744

Teresa, D. (2022, August 1). *A transhuman biohacker implanted over 50 chips and magnets in her body*. Retrieved June 25, 2023 from Interesting Engineering: https://interestingengineering.com/innovation/transhuman-biohacker-implanted-magnets

Thai, M. T., Phan, P. T., Tran, H. A., Nguyen, C. C., Hoang, T. T., Davies, J., . . . Do, T. N. (2023, February 19). Advanced Soft Robotic System for In Situ 3D Bioprinting and Endoscopic Surgery. *Advanced Science, 2023*(10), 2205656. doi:https://doi.org/10.1002/advs.202205656

Trafton, A. (2023, January 31). *How to make hyrdogels more injectable*. Retrieved June 16, 2023 from MIT News: https://news.mit.edu/2023/hydrogels-blocks-injectable-tissue-repair-0131

txyz.info. (2014, February 23). *Bionic Yourself V2.0*. Retrieved June 25, 2023 from Hackaday.io: https://hackaday.io/project/2736-bionic-yourself-v20

University of California at Berkeley. (n.d.). *Research Areas and Major Fields | UC Berkeley Mechanical Engineering.* Retrieved June 8, 2023 from UC Berkeley Mechanical Engineering: https://me.berkeley.edu/research-areas-and-major-fields/

University of Twente. (2020, December 9). Retrieved June 8, 2023 from Neurotechnology and Biomechatronics | Electrical Engineering: https://www.utwente.nl/en/education/master/programmes/electrical-engineering/specialisation/neurotechnology-biomechatronics/

Using Electric Currents to Fool Ourselves Into Tasting Something We're Not. (2017, August 15). Retrieved June 25, 2023 from Smithsonian Magazine: https://www.smithsonianmag.com/innovation/using-electric-currents-to-fool-ourselves-into-tasting-something-were-not-180970005/

Verheyen, C. A., Uzel, S. G., Kurum, A., Roche, E. T., & Lewis, J. A. (20223, March 1). Integrated data-driven modeling and experimental optimization of granular hydrogel matrices. *Matter, 6*(3), 1015-1036. doi:https://doi.org/10.1016/j.matt.2023.01.011

Virtuix Omni One. (2023, June 1). Retrieved June 25, 2023 from Virtuix: https://omni.virtuix.com/

Wang, X. (2019, Jan). Bioartificial Organ Manufacturing Technologies. *Cell Transplantation, 28(1)*, 5-17. doi:10.1177/0963689718809918

Whang, O. (2023, May 1). *A.I. Is Getting Better at Mind-Reading*. Retrieved June 23, 2923 from New York Times: https://www.nytimes.com/2023/05/01/science/ai-speech-language.html

Whit, C. (2023, May 10). *2 Odor Generator Formats Could Be the Solution To Incorporate Scents Into Virtual Reality*. Retrieved June 25, 2023 from The Science Times: https://www.sciencetimes.com/articles/43683/20230510/2-odor-generator-formats-solution-incorporate-scents-virtual-reality.htm

Wikipedia. (2023, April 30). *3D Bioprinting*. Retrieved June 16, 2023 from Wikipedia: https://en.wikipedia.org/wiki/3D_bioprinting

Wöbbeking, J. (2023, January 22). *Electric haptic vest makes for shocking VR experiences*. Retrieved June 25, 2023 from Mixed News VR Hardware: https://mixed-news.com/en/electric-haptic-vest-makes-for-shocking-vr-experiences/#:~:text=The%20Owo%20haptic%20vest%20provides,or%20stabbed%20in%20VR%20games.

XPrize Avatar Competition. (2023, April 16). Retrieved June 25, 2023 from XPrize: https://www.xprize.org/prizes/avatar

YAGN, N. (1890, November 18). *US440684A – Apparatus for facilitating walking.* Retrieved June 9, 2023 from Google Patents: https://patents.google.com/patent/US440684A/en

Zhang, S. (2018, February 20). *A Biohacker Regrets Publicly Injecting Himself With CRISPR*. Retrieved June 25, 2023 from The Atlantic: https://www.theatlantic.com/science/archive/2018/02/biohacking-stunts-crispr/553511/

2.

TECHNOLOGY, ETHICS, LAW AND HUMANITY [LONSTEIN]

STUDENT LEARNING OBJECTIVES

This chapter asks the student to dive deeply into a growing concern, have we become intoxicated, infatuated, and incapacitated by the abundance of technology in our lives? While most students have not enjoyed using a rotary phone, atlas, listening to AM or FM radio, using a Citizens Band Radio, or navigating without technology, they have grown up in a world of incredible innovation. Every aspect of our public and private lives is now touched by, if not run by, technology. So, the questions must be asked by everyone, how much is too much technology, and just because the technology exists to replace manual, human-run processes (Artificial Intelligence and Machine Learning Automation), does it mean it should?

INTRODUCTION

In 2018, ye author authored an article in Forbes entitled "Governments and Businesses Are Becoming Inebriated by Technology" as a warning to society that the rapid technological developments in the last ten years are causing a dangerous over-reliance upon it. I created a term meant to capsulize the challenge confronting an increasingly technology-dependent society: "Intechication." (Lonstein, 2018)

While overwhelmed by a myriad of new technologies such as Quantum Computing, Artificial Intelligence ("AI"), and Machine Learning ("ML"), to name a few, the blinding speed of advancements over the last five years should cause all of us to question not only dream of the possible benefits but also consider inherent risks of each as well as the consequence of combining technologies. For example, combining Social Media with the speed and scale of Quantum Computing and AL poses a formidable risk of widespread information warfare campaigns, which would be difficult, if not impossible, to contain. Where do we start? Is it too late? As Ian Malcolm (Portrayed by Jeff Goldblum), the lead in Michael Crichton's novel – turned blockbuster movie, Jurassic Park, put it, "Your scientists were so preoccupied with whether they could, they didn't stop to think if they should." (Speilberg, 1993)

In a world emerging from a pandemic that, according to the World Health Organization, has caused seven million deaths globally as of April 2023 (World Health Organization, 2023), the first glimpses of a new type of pandemic are already present, instant global disinformation and misinformation campaigns on social

media and elsewhere online. During the pandemic, numerous state-sponsored and private bot farms flooded social media and the broader internet with allegedly unsubstantiated claims, data, and theories, which caused widespread fear, doubt, protests, and even violence. (Himelein-Wachowiak, 2021)

Figure 2-1 Protests in Melbourne Australia

Sources: (Courtesy NY Times,) (Zhuang, 2021) (William, West Agence France-Presse — Getty Images, 2021)

The ability to automate and replicate content in social and online media may be an insurmountable problem, but what if the AI-fueled bots were using claiming content was disinformation – misinformation when it was legitimate dissent, opinion, or even factual?

NEW TECHNOLOGY – SAME OLD HUMANS: GUNS, EXPLOSIVES, BIOLOGICS, CHEMICALS, CONSUMER PRODUCTS AND CYBER

The introduction of groundbreaking new technologies is not something that is unique to the 20th and 21st centuries; in fact, some inventions were unintended by-products of research aimed to address entirely different issues. Gunpowder: one of the most important technological developments in history was a result of research designed to find a life-extending elixir by the Chinese somewhere between the eighth and ninth century A.D.

At the direction of the first Chinese Emperor Qin Shi Huang, researchers travelled far and wide to discover or create what was a tool for immortality. The researchers first discovered the element Potassium Nitrate (also known as saltpeter) combined with honey to create a healing smoke or Sulphur to create a healing salve. (Xinhua Net, 2017) (Ling, 1947)

After that, researchers discovered some other properties of Potassium nitrate leading to experiments that combined it with Charcoal and Sulphur, which created the first forms of what we now call gunpowder. (Shepherd, 2022) Over the centuries, gunpowder or its elements have been used to heal, kill, conquer, and create, depending on how the possessor used it. Similarly, the gun, a by-product of the discovery of gunpowder, has also been used to protect, purloin, conquer, defend, kill, hunt, feed, and or save lives. With further development, firearms became lighter, more powerful, affordable, and available. While the use of technology in service to the public or nation is one thing, the challenges of gun ownership and use by individuals are quite another. The use of guns in warfare made it clear that their use by individuals and the challenges it presented required governments to enact laws governing their use and ownership from as early as 1689. Century. (Satia, 2019)When placing military-grade, powerful technology in the hands of humans increases the risk of its misuse. Unlike nations and organizations where, in most instances, [1]some degree of debate, consultation, and risk assessment takes place among leadership, its use by an individual does not necessarily have the same type of braking mechanisms.

Figure 2-2 Las Vegas Mass Shooting

Police officers stand along the Las Vegas Strip outside the Mandalay Bay resort and casino during a deadly shooting near the casino, Sunday, Oct. 1, 2017, in Las Vegas. (AP Photo/John Locher) Florida Times-Union

Source: (Courtesy Florida Times Union/ AP) (Jacksonville.com, 2017)

Put another way, **"There is no legislation that will strip evil from an immoral man,"** by San Diego Gun Owners PAC Board member Warren Manfredi after the 2017-gun massacre at a concert in Las Vegas, Nevada.

The misuse of guns, explosives and other technological innovations in scale can lead to tragic and gut-wrenching results. Here are a few tragic examples:

GUNS

Las Vegas Shooting, 61 killed over 800 injured.

1. Pulse Orlando nightclub in Orlando, Fla. (June 12, 2016) – 49 killed, over 50 wounded.
2. Virginia Tech in Blacksburg, Va. (April 16, 2007) – 32 killed, over 17 injured
3. Sandy Hook Elementary School in Newtown, Conn. (Dec. 14, 2012), 26 killed (mostly children)
4. Luby's Cafeteria in Killeen, Texas (Oct. 16, 1991), 23 killed. (Peralta, 2016)

EXPLOSIVES

1. Oklahoma City Bombing, Federal Court House, Oklahoma City, Ok April 19, 1996
2. World Trade Center, February 26, 1993, New York, NY 6 killed, over 1000 killed
3. Boston Marathon Bombing, Boston, Ma April 15, 2013, 3 killed, over 100 injured.
4. Unabomber between 1978 and 1995 a series of bombings with 3 dead and 28 injured.
5. Haymarket Square, Chicago Il. May 4, 1886, 11 killed, over 100 killed.(National Academies of Sciences, Engineering, and Medicine, 2018)

BIOLOGICS AND CHEMICALS

Alphabet Bomber, Los Angeles, CA 1974, attempted attacks planned by a group including Muharem Kubergovic, who was arrested with 20 pounds of cyanide gas.

1. Followers of Bhagwan Shri Rashneesh placed homegrown salmonella bacteria on supermarket produce, salad bars, and other location in Oregon in 1984. Seven hundred fifty-one people fell ill from the attack, intended to affect a local election.
2. In 1994 and 1995, a test and follow-up attack occurred in Matsumoto (7 deaths and 500 injuries) and Tokyo Japan subway system (12 dead and thousands injured) using nerve gas. According to reports, the Aum Shinrikyo cult was also trying to develop or acquire Botulism and Ebola virus for use in weapons. (Smart, 1997)

CONSUMER AND COMMERCIAL TECHNOLOGY WEAPONIZATION

1. The September 11th, 2001, attacks using a box cutter to hijack and crash commercial airliners into the World Trade Center in New York City, NY, The Pentagon in Arlington, VA., and a crashed plane in Shanksville, PA. Almost 3,000 died on the attack date, thousands more died from 9/11 cleanup exposure diseases, and thousands more were injured.
2. In May 2021, consumer drones were sued for supplying drugs, guns, phones, and cash to a Lee County, South Carolina prison. (Robinson, 2022)
3. Explosive attack using drones on an Ecuadorian prison orchestrated by drug cartels in September 2021. (Crumley, 2021)

INTERNET & SOCIAL MEDIA

1. The September 11, 2001, attacks: According to the United States Department of Justice, "Evidence strongly suggests that terrorists used the Internet to plan their operations and attacks on the United States on September 11, 2001. " (Thomas, 2003)
2. Colonial Pipeline Attack, In May 2021, hackers using connectivity commenced a ransomware attack Colonial Pipeline was the target of a ransomware assault exploiting an insecure VPN, which shut it down for several days in 2021. The attack resulted in a significant nationwide fuel supply disruption and caused considerable price increases and long lines at gas stations. (United States Senate Committee on Homeland Security & Governmental Affairs, 2021)Figure 2-3 (Courtesy Jim Lo Scalzo, EPA) (EPA, J. Lo Scalzo, 2021)
3. Arab Spring., December 2020 "The internet and social media were vital tools for mobilizing Arab Spring protesters and documenting some government injustices." (Robinson K., 2020)
4. In a case of alleged cryptocurrency financing of terrorist groups in Syria, Victoria Jacobs, a/k/a Bakhrom Talipov, was indicted in February 2023; Jacobs allegedly laundered $10,661 on behalf of Malhama Tactical by receiving cryptocurrency and Western Union and MoneyGram wires from supporters around the globe and sending the funds to Bitcoin wallets controlled by Malhama Tactical. In addition to sending cryptocurrency, she also purchased Google Play gift cards for the organization, according to the indictment." (Katersky, 2023)

CAN TECHNOLOGY BE INHERENTLY EVIL?

In May 1927, Charles Lindbergh became a national hero and international celebrity. He was the first to fly across the Atlantic, from Long Island, New York, to Paris, France, non-stop and by himself. (National Air and Space Museum, 2023) With the heroic accomplishment came celebrity and, sadly, tragedy. In 1932 his firstborn child Charles, Jr., was kidnapped on March 1, 1932, and found murdered on May 12, 1932, a few

miles away from the Lindbergh home. (Federal Bureau of Investigation, 2023) Seeking to remove themselves from the spotlight and media frenzy, the Lindbergh's moved to France.

Still connected with flight, the U.S. Military asked Lindbergh to travel to Germany to assess the German air assets. He made at least three trips to Germany between 1936 and 1939. Lindbergh, of German descent, was awarded a medal known as the Commander Cross of the Order of the German Eagle on behalf of Adolph Hitler by Hermann Göring. Understandably, there was outrage in the United States and elsewhere when the story was published. Lindbergh discovered that his love of airplanes and the importance they introduced could not attenuate the risks associated with their misuse. In his book Brave Companions, author David Mc McCullough explained Lindbergh's epiphany this way; "The evil of technology was not in the technology itself, Lindbergh came to see after the war, not in airplanes or the myriad contrivances of modern technical ingenuity, but in the extent to which they can distance us from our better moral nature, our sense of personal accountability." (Mc Cullough, 1992)

Figure 2-3 Lindbergh accepts medal presented by Hermann Goering on behalf of Adolph Hitler

Source: (Courtesy Minneapolis Star Tribune/ Acme) (Duchshchere, 2022)

In early 1945 President Harry Truman asked Secretary of War Henry Stimson to create and convene a Blue-Ribbon committee to establish a set of recommendations for the use of atomic weapons during the late stages of WWII as well as a policy for post-war use and security of this nascent and potent new technology. Of great concern was the fear that the United States could not "maintain its monopoly" on the technology for long; some members of the committee believed the way to prevent a post-war (Unites States Department of Energy, 2023)

The constant friction between the tremendous power of nuclear weapons and the fear of misuse starts with the Manhattan Project itself. The United States and its allies created the Manhattan Project in response to information provided by intelligence and refugee scientists from Europe who informed the allies that Germany was working on and close to perfecting a weapon of mass destruction that harnessed and used the immense power of nuclear energy. (National WW II Museum, 2023) One particular friction associated with nuclear technology in warfare was scientist Joseph Rotblat. Born in Poland, Rotblat studied science in the United Kingdom and was part of a team that split the atom, which led to the ability to create a nuclear bomb. In light of the widely held belief that Germany was working work to create a nuclear bomb, the race was on. Part of a British team collaborating with the Americans, he eventually went to Los Alamos, New Mexico.

While Rotblat was at Los Alamos, he discovered how enormous the project would be to make a nuclear bomb. From this information, he became convinced that given the limitations of Germany in terms of talent, money, and manpower, it would be impossible for Germany to create a nuclear bomb.

Rotblat was interviewed as part of the History of the Atomic Heritage Foundation's "Voices of the Manhattan Project" series in 1989.

"I was becoming more and more unhappy about my participation in the project, even without Niels Bohr, for the simple reason that I had begun to realize when I came to Los Alamos the enormity of the project, how much it requires, the enormous manpower required, and the technological resources, to see how much money went into there. Ignoring what was going on in Oak Ridge, Hanford, and Berkeley. There is this enormous effort for the Americans to make the bomb."

"I could see that the war was coming to an end in Europe, and still it did not look like the bomb would be finished. We still had to grapple with basic issues like the implosion technique. But it became clear to me that [it was] very unlikely the Germans would make the bomb. I did not believe that the Germans could really produce something at less cost in this time, considering their involvement in the war [inaudible] was going on.

It became clearer gradually that the Germans are not going to make the bomb. The only reason really why I worked on the bomb was because of the fear of the Germans. This is the only reason. I would never have worked on this otherwise. This is quite simple, and not to be swayed, [inaudible] my motivation for work on the bomb was becoming invalid. But it was fortified by two events—well, not events. One was an event. This is the remark made by General Groves, which I described.

At that time, it was March of 1944, I was living with the Chadwick's, and Groves prepared to make a visit

to Los Alamos. The notification was he would come to Chadwick's, because he had become very friendly with Chadwick and would have dinner. Therefore, I was being a resident in the house, therefore I was also there.

This struck in my mind, the shock of it. We had been talking of a general sort over dinner on sort of things. It came down to the project. All of a sudden**, he said, "You realize, of course, that one purpose of this project is to subdue the Russians."** To me it came as a terrible shock, because to me the whole premise of the project was quite different." (Rotblat, Voices of the Manhattan Project, the Joseph Rotblat's Interview, 1989)

In 1995 Rotblat, the Pugwash organization, was awarded the Nobel Peace Prize "for their efforts to diminish the part played by nuclear arms in international politics and, in the longer run, to eliminate such arms."

In his acceptance speech at 88, he challenged those who invent, research, work on or use new powerful technologies. Is it a challenge that confronts all of us today and, most notably, today's students who will face these existential considerations in the coming years?

"But there are other areas of scientific research that may directly or indirectly lead to harm to society. This calls for constant vigilance. The purpose of some government or industrial research is sometimes concealed, and misleading information is presented to the public. It should be the duty of scientists to expose such malfeasance. "Whistleblowing" should become part of the scientist's ethos. This may bring reprisals; a price to be paid for one's convictions. The price may be very heavy, as illustrated by the disproportionately severe punishment of Mordechai Vanunu. I believe he has suffered enough.

The time has come to formulate guidelines for the ethical conduct of scientist, in the form of a voluntary Hippocratic Oath. This would be particularly valuable for young scientists when they embark on a scientific career. The US Student Pugwash Group has taken up this idea – and that is very heartening.

At a time when science plays such a powerful role in the life of society, when the destiny of the whole of mankind may hinge on the results of scientific research, it is incumbent on all scientists to be fully conscious of that role and conduct themselves accordingly. I appeal to my fellow scientists to remember their responsibility to humanity." (Nobel Prize Outreach, 2023)

Figure 2-4 Leaving Los Alamos

Leaving the bomb project

A nuclear physicist responsible for helping design the atomic bomb tells for the first time why he decided to leave Los Alamos in 1944.

Source: (Courtesy Tom Herzberg, Joseph Rotblat and Bulletin of Atomic Scientists, 1985)

In December 1946, Dr. Karl T. Compton authored an article in the Atlantic Magazine entitled "If the Atomic Bomb Had Not Been Used, Was Japan already beaten before the August 1945 Bombings?" As part of the article, he wrote about his interrogation of a senior Japanese Military Official who survived the bombings of Hiroshima and Nagasaki had not occurred; what would Japan have done? He answered:

"You would probably have tried to invade our homeland with a landing operation on Kyushu about November 1. I think the attack would have been made on such and such beaches.... It would have been a very desperate fight, but I do not think we could have stopped you..... We would have kept on fighting until all Japanese were killed, but we would not have been defeated," by which he meant that they would not have been disgraced by surrender." (Compton, 1946)

Dr. Sidney J. Stein was this author's Great Uncle. As a child, I would hear stories about this project he worked on for the government, which was crucial in ending World War II. During my High School and College years, we talked about the challenge of creating technology that can be used to kill massive numbers of humans. His response was always one of pride and introspection. Like all the scientists who worked on

the Manhattan Project, he knew the war had to end. Although none of us will ever know with certainty, there is no dispute that an invasion Japanese mainland would exact a heavy toll upon Japan & the Japanese people. Most scholars, military experts, and historians believe that the United States and its allies would have also suffered enormous casualties and deaths. Estimates range from fifty thousand deaths in the initial ground invasion alone (Compton, 1946) to tens of millions. (Jenkins, 2016)According to his Obituary written by his son Michael, "Sid remembered hearing that the bombs had been dropped and that the Japanese had surrendered. "We were thrilled knowing we had shortened the war and saved lives." Stein was decorated for his work. As fate would have it, the company he founded in 1962, Electro Science Laboratories, maintained its Asian headquarters in Tokyo, Japan, for decades, employing many Japanese citizens. (Stein, 2015)

Figure 2-5 Sidney J. Stein Grave, Frazer, Pa.

Source: (Courtesy Stein Family) (Stein, 2015)

ITS 2023 AND THE CONCERNS OF HUMAN MISUSE OF TECHNOLOGY GROWS

From Artificial Intelligence ("AI"), Machine Learning ("ML"), and Quantum Computing to Genomics, Robotics, 3D Printing, and Virtual Reality, the world is seeing breakthroughs in technology at a breathtaking pace.

In 1950 Alan Turing, a mathematician and one of the first computer scientists, authored a paper entitled "Computing and Intelligence." In the article, he sought to discuss and answer the question, can machines think?

Part of his hypothesis required a method to determine if the output of the machine or produced by a human. To prove his hypothesis, he called for a human interrogator to examine the answers to questions asked of humans and machines and determine whether a human or machine created the response. Turing was particularly keen on an "infinite capacity computer." He envisioned what we might call today, Quantum Computing, adding storage and processing capacity as needed depending on the amount of data ingested and the processing capacity required for more complex information sets. He is widely considered one of the progenitors of Artificial Intelligence and Machine Learning. (Turing, 1950)

Dr. Turning alluded to the infinite capacity and storage that would eventually become Moore's Law. Gordon Moore, Co-Founder of what is today known as the Intel Corporation, postulated that the transistor capacity of a chip doubles every two years, so does processing power. Simultaneously, as the number of transistors increases, the cost per transistor falls, thereby reducing cost while allowing the processing power of computer chips to grow exponentially. (Moore, 1965)

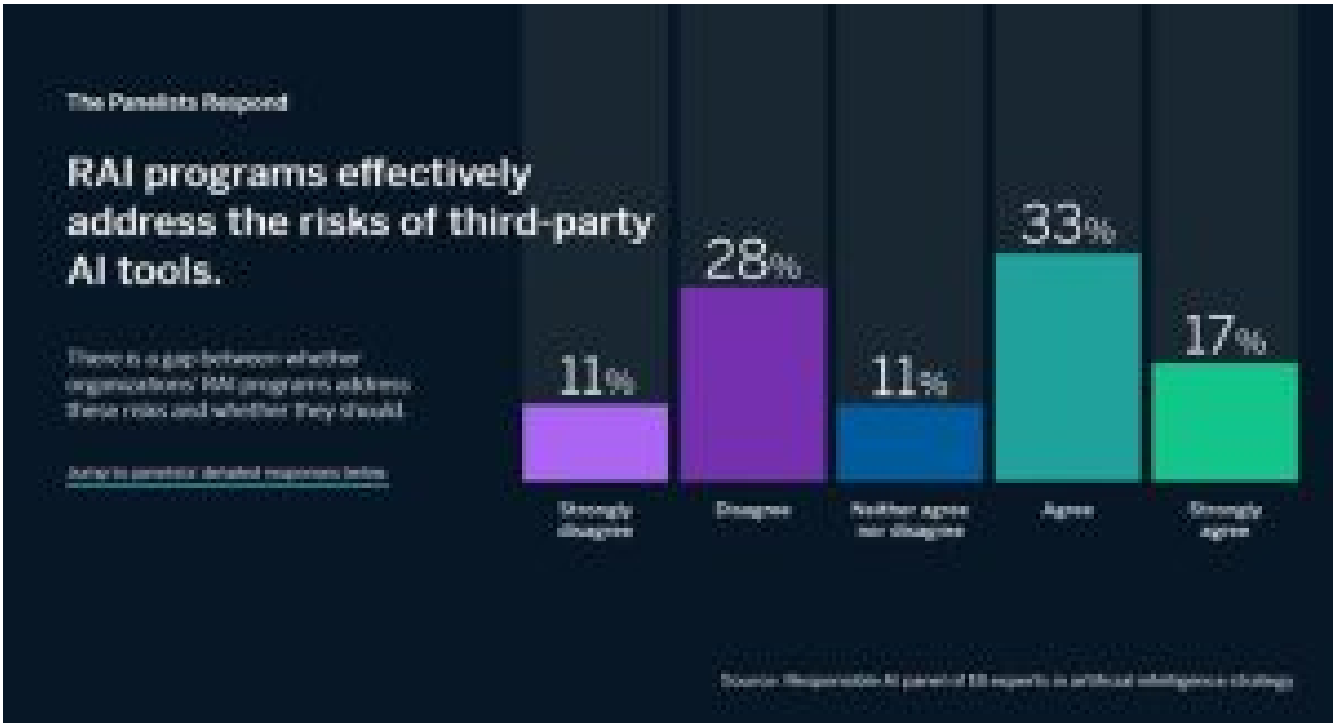
AI and Quantum Computing gave rise to the fission-like explosive growth of automation, AI, and ML. With this rapid development comes the challenge of misuse or mishap in scale. Although Robotics, Automation, AI, and ML have already demonstrated the ability to improve our lives while presenting the same existential threats as nuclear energy, electromagnetic pulse technology, lasers, and biological and chemical agents, you name a few.

One glance at any news source will undoubtedly contain reports of the many benefits of AI, ML, etc., and other stories about the threats these technologies may pose. Students and technology professionals will be required to decide whether to use technology, how to use technology, limitations on the international, national, commercial, and personal use of these new technologies, counter technologies, or other measures to deal with the misuse, unintended. Whatever is written on these pages today will undoubtedly be outdated months after publication. There is precious little we can accurately predict about ten or twenty years in the future, much less twenty minutes from now. Therefore, this chapter intentionally does not focus on currently perceived or known threats from technology; instead, our focus has been on what history has shown us and what precautions, legislation, countermeasures, or detection methods can be implemented to prevent the risks we know exist from becoming a reality. In no particular order, here are some examples of potential defenses.

JUST BECAUSE WE CAN DOES NOT MEAN WE SHOULD

As discussed throughout this chapter, Risk/Benefit analysis is essential before introducing such new technologies into public, private, commercial, or defense environments. Since most AI technology available today is Third Party ("TPAI") created, a significant analysis must be performed to assess the risks associated with its use which has been referred to as Responsible Artificial Intelligence ("RAI"). To that end, the MIT Sloan Management Review and Boston Consulting Group surveyed 18 panelists involved in considering or actually implementing TPAI
into their organizations.

Figure 2-6 RAI Survey April 2023



Source:(Courtesy MIT Sloan Management Review) (Renieris, 2023)

As the small but instructive survey reveals, there needs to be more agreement or confidence in using RAI to analyze the risks and benefits of TPAI. The people deciding whether TPAI is a sound, safe, and responsible decision for their organization need to be more confident in their analytical tools or processes; how can they implement the technology ethically?

WHAT ARE THE ETHICAL AND LEGAL CONSIDERATIONS?

Given the nascent state of the use of AI, ML, and other new technology, and the rapid rate of their development and implementation, the concepts of law, ethics, and morality of specific use cases and scenarios are taking a back seat. However, this is not to say that no guiding principles exist making creating, using, or restricting the use of AI, ML, or their progeny. Isaac Asimov was a Russian Immigrant to America who eventually served as a biochemistry professor at Boston University. In addition, he was a prolific writer who became enamored with science fiction as a child by reading small "pulp" magazines on this subject in his family's candy store. Later on

Asimov wrote a series of short stories and novels between 1940 and 1945, eventually including them in his 1950 compilation entitled I, Robot. One story, written in 1941, was entitled "Runaround." In Runaround, Asimov introduced the "Three Laws of Robotics," also known as Asimov's Law.

FIRST LAW: A ROBOT MAY NOT INJURE A HUMAN BEING OR, THROUGH INACTION, ALLOW A HUMAN BEING TO COME TO HARM.

SECOND LAW: A ROBOT MUST OBEY THE ORDERS GIVEN TO IT BY HUMAN BEINGS EXCEPT WHERE SUCH ORDERS WOULD CONFLICT WITH THE FIRST LAW.

THIRD LAW: A ROBOT MUST PROTECT ITS OWN EXISTENCE AS LONG AS SUCH PROTECTION DOES NOT CONFLICT WITH THE FIRST OR SECOND LAWS. (ASIMOV, 1942)

The fact that Asimov created his laws for robots' points to a more critical issue, whether technology or human, which needs regulation. Suppose technology could self-determine how its use; it could be engineered to have internal self-limitations to prevent misuse. A case in point is firearms. For as long as they have existed, guns have been used in war, law enforcement, and self-defense. The Second Amendment to United States Constitution. (United States of America, 1791) establishes the right to own (bear") arms. For the same period, firearms have been misused or accidentally used in a way society finds unacceptable. According to the Judicial Learning Center: "Laws are rules that bind all people living in a community. Laws protect our general safety and ensure our rights as citizens against abuses by other people, by organizations, and by the government itself. We have laws to help provide for our general safety." (Judicial Learning Center, 2019)

What happens when these laws and regulations are broken or violated, and a person has been proven guilty of the offense? [2] Does a punishment regime exist? Why is there punishment? The four primary philosophical reasons for punishment in a system of laws are:

RETRIBUTION: PUNISHMENT SERVES THE PURPOSE OF RETRIBUTION WHEN IT SIMPLY RETALIATES (OR GETS EVEN) BY INFLICTING PAIN OR DISCOMFORT PROPORTIONATE TO THE OFFENSE.

INCAPACITATION: PUNISHMENT SERVES THE PURPOSE OF INCAPACITATION WHEN IT PREVENTS OFFENDERS FROM BEING ABLE TO REPEAT AN OFFENSE. THE MOST

POPULAR FORM OF INCAPACITATION TODAY IS INCARCERATION.

DETERRENCE: PUNISHMENT SERVES THE PURPOSE OF DETERRENCE WHEN IT CAUSES OFFENDERS TO REFRAIN FROM COMMITTING OFFENSES AGAIN (INDIVIDUAL DETERRENCE) OR WHEN IT SERVES AS AN EXAMPLE THAT KEEPS OTHERS FROM COMMITTING CRIMINAL ACTS (GENERAL DETERRENCE).

REHABILITATION: THE PURPOSE OF REHABILITATION IS TO CHANGE OFFENDERS THROUGH PROPER TREATMENT. (CHERRINGTON, 2007)

The greatest challenge in regulating AI, ML, and similar technologies is the new reality of scale and speed. As of this writing, AI through consumer products such as ChatGPT is already increasing and will require more work to regulate effectively. Students will undoubtedly be confronted with the challenge of resolving these and many more ethical and legal challenges presented by AI, ML, and other self-developing autonomous technology. The most vexing challenge may not be whether humans will obey the laws created to regulate technology but whether and how long it will take them to decide to abide by them.

Figure 2-7 War Games Movie Nuclear War Machine Learning Scene

Source: (Courtesy United Artists 1983) (Badham, 1983)

COUNTER -AI

The final and most important part of our discussion deals with the reality that when, not if AI, ML, or similar technology goes awry or becomes a hacker itself? No less than the esteemed Cryptography expert Bruce Schneier distilled the problem this way:

"There are really two different but related problems here. The first is that an AI might be instructed to hack a system. Someone might feed an AI the world's tax codes or the world's financial regulations, with the intent of having it create a slew of profitable hacks. The other is that an AI might naturally, albeit inadvertently, hack a system. Both are dangerous, but the second is more dangerous because we might never know it happened." (Schneier, 2021)

The risk of conflict increases with the world's nations all racing to become the leader in AI technology. Governments and non-state actors are experimenting with its capabilities. The experiments may cause unexpected results or even work cause unintended harm. Much like crowded airspace in a war zone, the risk of conflict is already significant, and the risk of accidental events causing conflict may be even greater. Even the intended results of the testing and implementing various AI technology by one nation might be deemed an existential threat by another, which, in turn, could create a scenario where virtual technology leads to kinetic engagement. The risk of an AI failure, attack, or unexpected result exists from pipelines to power plants and air travel to atomic energy. As more and more AI systems develop, the risk of unintended consequences grows. Prudence dictates that the creation of Counter AI technology and protocols happens rapidly. Professor M. A. Thomas of the United States Army Scholl of Advanced Military Studies described the urgent challenge to develop Counter AI systems this way:

"The singular strategic focus on gaining and maintaining leadership

And the metaphor of an "arms race" is unhelpful, however.

Races are unidimensional, and the winner takes all.

Previous arms races in long-range naval artillery or nuclear weapons were

predicated on the idea that advanced tech would create standoff, nullifying the effects of the adversary's weapons and deterring attack. But AI is not unidimensional; it is a diverse collection of applications, from AI-supported logistics and personnel systems to AI-enabled drones and autonomous vehicles. Nor does broadly better tech necessarily create standoff, as the US military learned from improvised explosive devices in Afghanistan. This means that in addition to improving its own capabilities, the United States must be able to respond effectively to the capabilities of others. In addition to its artificial intelligence strategy, the United States needs a counter-AI strategy." (Thomas M. A., 2020)

CONCLUSIONS

We are living through the beginning of an unprecedented development period of new technology of power and speed never before seen. Indeed, the introduction of atomic weapons was earth-shattering at the time.

However, its development took many years and thousands of people to perfect. With AI and automation technology, the need for thousands of humans, many, if not all, endeavors of discovery or invention may decrease to only a few or none. It is the hope of this author and the members of the Wildcat Team that students and those professionals who read it use it as a call to action. The promise and danger of this new technology are both unlike anything the world has previously witnessed. With that tremendous power comes challenge, and like it or not, the burden of finding answers to the questions raised in this chapter and in this book will fall upon its reader. Here is wishing Godspeed to all those who take on the challenge, and may their efforts result in a safer and more peaceful world.

REFERENCES

Asimov, I. (1942). *runaround.* New York: Street & Smith .

Badham, J. (Director). (1983). *War Games* [Motion Picture].

Cambridge Dictionary. (2023, April 27). *Transhumanism*. Retrieved from Cambridge Dictionary: https://dictionary.cambridge.org/us/dictionary/english/transhumanism

Cherrington, D. J. (2007, April 1). *Crime and Punishment: Does Punishment Work?* . Retrieved from Brigham Young Scholars Archive: https://scholarsarchive.byu.edu/cgi/viewcontent.cgi?article=1953&context=facpub

Compton, D. K. (1946, December). If the Atomic Bomb Had Not Been Used, Was Japan already beaten before the August 1945 bombings? *The Atlantic*, pp. 54, 55.

Crumley, B. (2021, September 14). *Drones drop explosives in Ecuador prison attack by suspected drug cartels*. Retrieved from Drone DJ: https://dronedj.com/2021/09/14/drones-drop-explosives-in-ecuador-prison-attack-by-suspected-drug-cartels/

Daily Mail. (2021, November 22). *Blow-by blow account of how Christmas parade pandemonium unfolded as SUV driver barreled through crowd and killed at least five.* Retrieved from Daily Mail Online: https://www.dailymail.co.uk/news/article-10230313/Waukesha-Christmas-parade-horror-Timeline-carnage-unfolded.html

Director of National Intelligence. (2018, March 30). *Planning and Preparedness Can Promote an Effective Response to a Terrorist.* Retrieved from Director of National Intelligence: https://www.dni.gov/files/NCTC/documents/jcat/firstresponderstoolbox/First-Responders-Toolbox—Planning-Promotes-Effective-Response-to-Open-Access-Events.pdf

Duchshchere, K. (2022, June 3). *Was Charles Lindbergh a Nazi sympathizer?* Retrieved from Star Tribune: https://www.startribune.com/charles-lindbergh-little-falls-world-war-2-nazi-germany/600178871/

Environmental Protection Agency, James Lo Scalzo. (2021, May 19). *Colonial Pipeline confirms it paid $4.4m ransom to hacker gang after attack.* Retrieved from The Guardian : https://www.theguardian.com/technology/2021/may/19/colonial-pipeline-cyber-attack-ransom

Federal Bureau of Investigation. (2023, April 6). *Lindbergh Kidnapping*. Retrieved from FBI: https://www.fbi.gov/history/famous-cases/lindbergh-kidnapping

Folger Shakespeare Library. (2015, July 10). *Now Thrive the Armorers: Arms and Armor in Shakespeare*. Retrieved from Folgerpedia: https://folgerpedia.folger.edu/Now_Thrive_the_Armorers:_Arms_and_Armor_in_Shakespeare

Hayles, K. N. (1999). *How we became posthuman : virtual bodies in cybernetics, literature, and informatics.* Chicago, Il.: University of Chicago Press.

Himelein-Wachowiak, M. e. (2021, May 20). *Bots and Misinformation Spread on Social Media: Implications for COVID-19.* Retrieved from Journal of Medical Internet Research: https://www.ncbi.nlm.nih.gov/pmc/issues/380959/

Jacksonville.com, F. T. (2017, October 2). *Las Vegas attack is deadliest shooting in modern US history*. Retrieved from Florida Times Union: https://www.jacksonville.com/story/news/nation-world/2017/10/02/las-vegas-attack-deadliest-shooting-modern-us-history/15775260007/

Jenkins, P. (2016, May 18). *Back to Hiroshima: Why Dropping the Bomb Saved Ten Million Lives*. Retrieved from ABC Religion & Ethics: https://www.abc.net.au/religion/back-to-hiroshima-why-dropping-the-bomb-saved-ten-million-lives/10096982

Judicial Learning Center. (2019). *What is a Law?* Retrieved from Judicial Learning Center: https://judiciallearningcenter.org/law-and-the-rule-of-law/#:~:text=Laws%20protect%20our%20general%20safety,provide%20for%20our%20general%20safety.

Katersky, A. (2023, February 1). *New York City woman charged with financing terrorist groups in Syria through cryptocurrency*. Retrieved from ABC News: https://abcnews.go.com/US/new-york-city-woman-charged-financing-terrorist-groups/story?id=96818461

Library of Congress. (2023, April 15). *Military Technology in World War I.* Retrieved from Library of Congress: https://www.loc.gov/collections/world-war-i-rotogravures/articles-and-essays/military-technology-in-world-war-i/

Ling, W. (1947). On the Invention and Use of Gunpowder and Firearms in China. *Isis, Vol 37*, 167.

Lonstein, W. (2018, April 12). *Governments and Businesses Are Becoming Inebriated by Technology*. Retrieved from Forbes: https://www.forbes.com/sites/forbestechcouncil/2018/04/12/governments-and-businesses-are-becoming-inebriated-by-technology/?sh=4d52c7c148df

Mc Cullough, D. (1992). *Brave Companions, Portraits in History.* New York, NY: Simon & Schuster.

Moore, G. E. (1965, April 19). Cramming more components onto integrated circuits. *Electronics, Volume 38, Number* .

National Academies of Sciences, Engineering, and Medicine. (2018). *Reducing the Threat of Improvised Explosive Device Attacks by Restricting Access to Explosive Precursor Chemicals.* Washington DC: The National Academies Press.

National Air and Space Museum. (2023, April 20). *The First Solo, Nonstop Transatlantic Flight*. Retrieved from National Air and Space Museum: National Air and Space Museum

National Institute of Drug Abuse. (2019). *Research Report – How is methamphetamine misused?* Baltimore, MD: National Institute of Drug Abuse.

National WW II Museum. (2023, April 5). *The Manhattan Project*. Retrieved from National WW II Museum: https://www.nationalww2museum.org/war/topics/manhattan-project

Nobel Prize Outreach. (2023, April 1). *Joseph Rotblat Facts and Lecture*. Retrieved from The Nobel Prize: https://www.nobelprize.org/prizes/peace/1995/rotblat/lecture/

Peralta, E. (2016, June 12). *A List Of The Deadliest Mass Shootings In Modern U.S. History*. Retrieved from NPR: https://www.npr.org/sections/thetwo-way/2016/06/12/481768384/a-list-of-the-deadliest-mass-shootings-in-u-s-history

Renieris, E. M. (2023, April 20). *Responsible AI at Risk: Understanding and Overcoming the Risks of Third-Party AI*. Retrieved from MIT Sloan Management Review: https://sloanreview.mit.edu/article/responsible-ai-at-risk-understanding-and-overcoming-the-risks-of-third-party-ai/

Robinson, H. (2022, February 3). *20 people arrested in connection to drone attacks at Midlands prison*. Retrieved from WIS TV: https://www.wistv.com/2022/02/03/20-people-arrested-connection-drone-attacks-midlands-prison/

Robinson, K. (2020, December 3). *The Arab Spring at Ten Years: What's the Legacy of the Uprisings?* Retrieved from Council on Foreign Relations: https://www.cfr.org/article/arab-spring-ten-years-whats-legacy-uprisings

Rotblat, J. (1985). Leaving the bomb project. *Bulletin of the Atomic Scientists Volume 41, Issue 7*, 16-19.

Rotblat, J. (1989, October 12,). Voices of the Manhattan Project, the Joseph Rotblat's Interview. (M. J. Sherwin, Interviewer)

San Diego County Gun Owners. (2017, October 1). *A message on the tragedy in Las Vegas*. Retrieved from San Diego County Gun Owners: https://sandiegocountygunowners.com/project/message-tragedy-las-vegas/

Satia, P. (2019). What guns meant in eighteenth-century Britain. *Palgrave Commun 5*, 105.

Schneier, B. (2021, April). *The Coming AI Hackers.* Retrieved from The Harvard Kennedy School Belfer Center: https://www.belfercenter.org/publication/coming-ai-hackers

Shepherd, A. D. (2022). From Spark and Flame: a Study of the Origins of Gunpowder. *Tenor of Our Times, Vol. 11, Article 12*, 2. Retrieved from Tenor of Our Times.

Smart, J. K. (1997). *History of Chemical and Biological Warfare: An American Perspective.* Aberdeen Proving Ground, MD: U.S. Army.

Speilberg, S. (Director). (1993). *Jurassic Park* [Motion Picture].

Stein, M. (2015, August 15). *A Portrait of Sid Stein*. Retrieved from Find A Grave: https://www.findagrave.com/memorial/193235542/sidney-j-stein

The 9/11 Commission . (2004). *The 9/11 Commission Report.* Washington, DC: United States of America .

The Economic Times. (2022, November 17). *Christmas parade killer Darrell Brooks gets 1,067 years of sentence, judge breaks down in tears, says 'heart-wrenching'*. Retrieved from The Economic Times:

https://economictimes.indiatimes.com/news/international/uk/christmas-parade-killer-gets-1067-years-of-sentence-judge-breaks-down-in-tears-says-heart-wrenching/articleshow/95582665.cms

Thomas, M. A. (2020, Spring). Time for a Counter-AI Strategy. *Strategic Studies Quarterly*, p. 3.

Thomas, T. L. (2003). *Al Qaeda and the Internet: The Danger of "Cyberplanning".* Washington, D.C. : United States Department of Justice Office of Justice Programs.

Turing, a. m. (1950). Computing Machinery and Intelligence. *Mind 49*, 433-460.

United States of America. (1791, December 15). Second Amendment to the United States Constitution. *United States Constitution* . Washington, DC: United States.

United States Senate Committee on Homeland Security & Governmental Affairs. (2021). Testimony of Joseph Blount, CEO Colonial Pipeline . *United States Senate Transcript* (p. 4). Washington DC: United States Congress.

Unites States Department of Energy. (2023, April 5). *The Manhattan Project, an ?Interactive History*. Retrieved from U.S. Department of Energy – Office of History and Heritage Resources: https://www.osti.gov/opennet/manhattan-project-history/Events/1945/debate.htm

William, West Agence France-Presse — Getty Images. (2021, August 21). *Protests in Melbourne.* Retrieved from New York Times: https://static01.nyt.com/images/2021/08/21/world/21virus-briefing-oz-protests/merlin_193494093_43aeb0fb-7671-4f97-858d-47ab6368be91-superJumbo.jpg?quality=75&auto=webp

World Health Organization . (2023, April 16). *World Health Organization*. Retrieved from https://covid19.who.int/: https://covid19.who.int/

Xinhua Net. (2017, December 24). *Across China: Wooden slips reveal China's first emperor's overt pursuit of immortality*. Retrieved from Xinhua Net: http://www.xinhuanet.com/english/2017-12/24/c_136848720.htm

Zhuang, Y. (2021, August 21). *In Melbourne, Australia, a protest against Covid restrictions turned violent.* Retrieved from New York Times: https://www.nytimes.com/2021/08/21/world/australia/melbourne-protests-covid-restrictions.html

Zoli, C. (2017, October 2). *Is There Any Defense Against Low-Tech Terror?* Retrieved from Foreign Policy: https://foreignpolicy.com/2017/10/02/terror-has-gone-low-tech/

ENDNOTES

[1] It is not lost on the author that many nations and groups have used and abused in ways that most humanities found offensive, improper, and inhumane. Hitler, Pol Pot, and Stalin misused powerful technologies most brutally and horrifically, leading to the deaths of millions of innocents. Tyranny, mental illness, and cults are examples where group oversight, consideration, and debate failed... (San Diego County Gun Owners, 2017)

[2] This presumes a system of laws and punishments provides a method of adjudication with the presumption of innocence, the right of the accused to have a defense, confront the accuser, and have guilt or innocence determined by a neutral judge or jury of peers.

3.

ARTIFICIAL BRAINS AND BODY [MUMM]

STUDENT LEARNING OBJECTIVES

The student will gain knowledge of the concepts and framework related to the current and future uses of human systems as related to the artificial brain and body (form factor), along with an assessment of how these autonomous systems are integrated into the world around us.

WHY ARE AUTONOMOUS SYSTEMS/ROBOTS IN THE FORM FACTOR OF HUMANS?

What is a body, and what is its purpose? Why do humans feel it is necessary to make all things conform to their relatively limited functional world? The fact that humans have opposable thumbs and can manipulate items in their environment better than a dog or a dolphin does not mean that our human environment is the most effective or efficient for getting work done or even for human happiness.

Figure 3-1: Humanoid robot in runner's starting stance

Source: (Bandakkanavar, 2021)

A limitation of the form factor for robots can become an obstacle to forward progression, as humans must unlearn their environment and learn through the lens of a robot's point of view. Unfortunately, most of our world is set up to work within human limitations as humans must adapt to dull, dirty, or dangerous activities, yet robots thrive in these spaces.

The definition of the body when we are referring to a human is "the organized physical substance of an animal or plant either living or dead, the material part or nature of a human being" (Merriam-Webster., 2023). Yet when we examine the human counterpart in a humanoid autonomous system, the definition is "A humanoid is a robot with a human-like appearance that allows interaction with tools or environments made for humans" (Khillar, 2020). Figure 3-2 provides a quick comparison of characteristics between humanoids and robots.

Figure 3-2: Comparison Chart of Humanoid vs. Robot

Humanoid Characteristics	Robot Characteristics
A humanoid is a robot with a human-like appearance that allows interaction with tools or environments made for humans.	A robot is a machine capable of executing a co tasks automatically with utmost speed and pre
The defining characteristics of a humanoid are to perform a complex series of physical tasks and to operate tools and manipulate objects designed for humans.	The essential characteristics of a robot include movement, power, and intelligence. A robot c of shapes and sizes.
The world's first humanoid robot to be able to communicate with humans was WABOT-1.	The first programmable robot was an industri Unimate.

Source: (Khillar, 2020)

"Robots have become humanoid robots with a human-like shape. The drive to create smart and intelligent human-like artificial machines has led to the development of humanoids" (Khillar, 2020).

The purpose and capabilities of humanoid robots vary greatly; however, they can "adapt to its surroundings and continue with its direction or command. Depending upon the size and weight, these robots have the capability of self-maintenance and an advanced feature of autonomous learning; thus, they avoid harmful situations to people, property, and themselves" (Bandakkanavar, 2021).

The challenge of choosing whether to adapt the robot or humanoid to human surroundings or allow the robot to learn and adapt its shape, form, and function to the human environment is still in debate. The issue of how to give the robot proper feedback in any given environment or situation is still in the infant stages and collecting information for feedback mechanisms is essential. How much information, what types of data, and the amount of personal privacy of an individual balance against an autonomous robot's safe and optimal operation is still being determined.

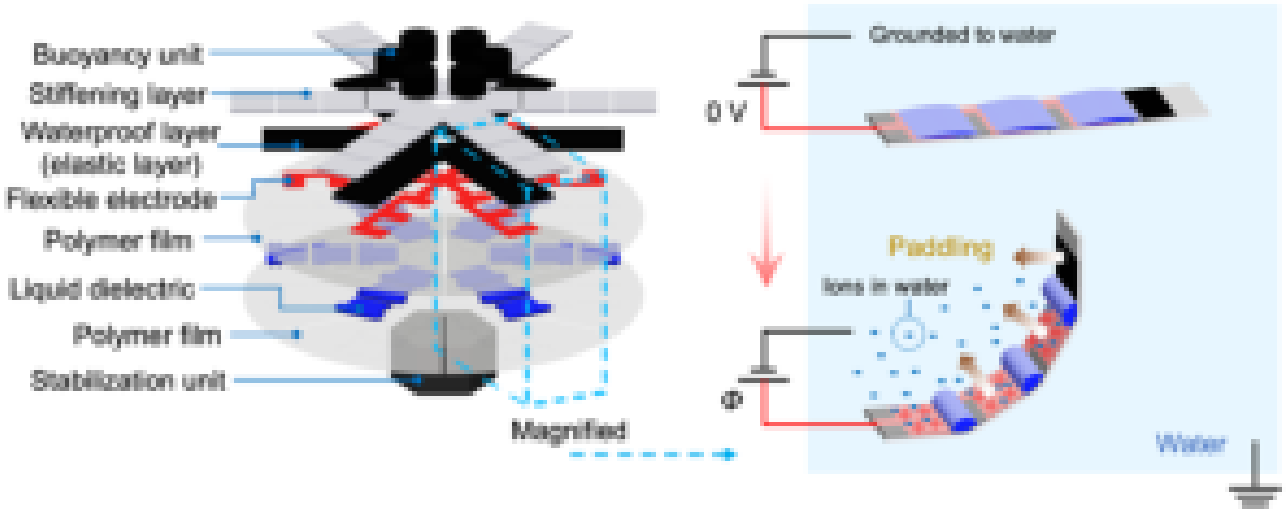
THE SUM OF ITS PARTS, THE BODY-WHAT IS THE OPTIMUM FORM FACTOR?

Retrieving garbage from the sea can be a difficult and expensive task; typically undertaken with large machines that grab, scoop, or attempt to capture debris in similar ways to humans' hands. However, the human form may not be the best to emulate in delicate situations, and nature might offer a better shape to mimic. So enters the robotic jellyfish. See Figures 3-3 and 3-4 for the advantages of robotic jellyfish and how they have been designed.

Figure 3-3: Jellyfish might clean the ocean one day

Source: (Jellyfish-like robots could one day clean up the world's oceans., 2023)

Figure 3-4: Jellyfish might clean the ocean one day



Source: (Jellyfish-like robots could one day clean up the world's oceans., 2023)

An undertaking by the Max Planck Institute for Intelligent Systems has "discovered that the flapping propulsion system of a robotic jellyfish is not only good for movement, but it can also draw small bits of debris up from the ocean floor without any contact" (Franco, Robotic jellyfish can suck up ocean debris without touching it. , 2023b)**.** This non-invasive movement could be leveraged to clean unique, fragile surfaces such as those found in coral reefs. (Franco, Robotic jellyfish can suck up ocean debris without touching it. , 2023b)**.** With an eye towards nature combined with robotics, processes that date back hundreds of years are now being updated, changed, made more efficient, and sometimes even simplified.

Brewing beer is one example of a natural chemical process that is being revised. "In order to speed up and simplify the process, scientists have developed tiny BeerBots" (Coxworth, 2023)**.**

Figure 3-5: **Beerbots help fermentation**

Source: (Coxworth, 2023)

These Beer Bots "release carbon dioxide gas into the air, before sinking back down again. They repeat this up-and-down process until all the sugars in the wort have been fermented" (Coxworth, 2023). Figure 3-5 illustrates BeerBots in action. BeerBots can be reused for up to three more fermentation cycles before being discarded. Professor Martin Pumera, the creator of BeerBots, admits that it would be "difficult to scale up to industrial use in its present form, so it may end up being utilized mainly by small-scale craft beer producers" (Coxworth, 2023).

Humans have had to learn to adapt to an animal-dominated world. It is "sometimes difficult to imagine how the planet we call home, with its megalopolis cities and serene farmlands, was once dominated by dinosaurs as big as buses and five-story buildings" (Reynolds, 2023).

Nature evolves as it learns to survive and thrive in its surroundings. An example is the inside of an elephant skull where there are large air sacs that allow the animal to move its massive head and heavy tusks without straining the neck muscles. The human head must be able to move similarly to the elephant, yet the human brain tends to be more delicate, and so it is protected by two layers of hard, compact bone (inner and outer tables) ...known as the diploe" (Reynolds, 2023). How did animals and humans evolve in similar ways, yet be so dissimilar to each other? This is due to something known as "convergent evolution in which animals are faced repeatedly with the same problem, evolving similar – but not always identical – solutions each time" (Reynolds, 2023).

Animals evolved with vegetation, water, and different types of terrain. Then the animals had to develop with humans and additional species of animals, all fighting for the same resources. Now humans, animals, vegetation, waterways, and robots will be fighting for a balance in a resource-limited world. Robots and

humans must now work through convergent evolutionary issues together, with little historical precedent to fall back on. The unknowns of true AI, quantum, hybrid networks, hybrid humans, hybrid robots, and integrated autonomous systems can harmonize humanity or result in chaos. Consider that this integration and adaptation between humans, nature, and now robots will be made with little understanding of the long-term outcomes or consequences. In an ever-changing world, convergent evolution could allow all involved to flourish or fail during some or all of these adaptations.

While considering the complexity of evolution, let us not forget that the next phase of human evolution will be in space. Recently, Rolls Royce received a £2.9-million (US$3.5-million) contract from the United Kingdom Space Agency. This contract was to develop a nuclear reactor prototype that would be part of a future lunar outpost. The energy from the reactor must be sufficient to support everything necessary within the outpost, including life support systems, communications systems, and any scientific fieldwork. The contract stipulates that the prototype must be completed by 2029 (Szondy,2023). There is no doubt that this prototype will include robotic assistance to monitor the power quality and numerous ancillary systems. The promise of a lunar outpost means that humans and robots will need to adapt to a new environment that neither are necessarily equipped to understand, work in, or be optimized for efficient harmonization.

WHY ARE AUTONOMOUS SYSTEMS/ROBOTS IN THE FORM FACTOR OF HUMANS?

When people hear the word robot, they conjure images of the AI robot Sofia or the robot Sonny from the movie iRobot. However, these human form factors are some of the least desirable as they force a machine to be subservient to a human's world instead of allowing the machine to become the solution and the path of efficiency for humankind. Our current world is set up for humans to do the work, make the decisions, and interact with the infrastructure. However, where we need to be is just the opposite as autonomous systems begin to interact with our environments and other autonomous systems.

A hybrid of a robot and a human might be the bridge between only humans working within our human-optimized environments and when humans build more autonomous systems optimized environments, thus ending the human-driven or human-assisted work era. As noted by Wired Magazine on March 23, 2023, "For Smarter Robots, Just Add Humans autonomous machines are still too clumsy for delicate tasks. But humans can operate mechanical arms from afar, turning physical labor into remote work" (Knight, 2023). Sanctuary AI describes it as "Leveraging a blend of symbolic and neural reasoning, our autonomous control system utilizes the best of both approaches to AI while mitigating the weaknesses of each. Put another way, it is AI like it has never been done before" (Sanctuary AI-Creating human-like intelligence. , 2023). Figure 3-6 illustrates the connection between robots and human intelligence, form, and senses.

Figure 3-6: Creating the future


HUMAN-LIKE INTELLIGENCE
Under AI or Teleoperation
HUMAN-LIKE SENSES
See, Hear, Feel
HUMAN-LIKE FORM
Hands and Body

Source: (Sanctuary AI-Creating human-like intelligence. , 2023)

Sanctuary AI believes that an essential job of the future will be created in the area of remotely operating or teleoperating a physical robot Sanctuary AI "believes that this might provide a way to train robots how to perform tasks that are currently well out of their (mechanical) reach, and imbue machines with a physical sense of the world some argue is needed to unlock human-level artificial intelligence" (Knight, 2023).

The next robotic evolution for Sanctuary AI is a sixth-generation, general-purpose robot (GPR) named Phoenix™. The company aims to "shoot for the world's first human-like intelligence in general purpose robots. Phoenix builds on some very impressive earlier work and a neat "piloted" approach to training" (Blain, 2023). Figure 3-7 provides an image and features of the Phoenix GPR.

Figure 3-7: Phoenix

Source: (Blain, 2023)

Phoenix takes on a human form, although Sanctuary AI admits that the humanoid form "certainly isn't the most efficient shape for a useful robot – but it's an excellent shape for a robot that's designed to take over as many human tasks as possible" (Blain, 2023). This is an example of evolving robots into a human environment instead of adapting the environment to accommodate the most efficient robotic design. The humanoid design allows the robot to work immediately in the infrastructure that is seen today as the "modern world is constructed mainly for bipedal creatures around a certain height, with five-fingered hands and opposable thumbs" (Blain, 2023).

The challenge of how to allow robots to operate more efficiently and effectively can sometimes be found in nature, as with the "Prehistoric sea creature-like robot can navigate, surf, crawl up onto the beach. The recently developed C-Ray uses fins to cross water, land, and ice" (Woolfolk, 2023).

Figure 3-8: Velox Robot

Source: (Aouf, 2019)

Taking a page from nature and allowing the robot to operate in many different environments allows the "amphibious Velox robot to use its undulating fins to swim and crawl and Velox's versatility is due to its undulating soft fins, which sit on either side of Velox and move in a hyperbolic pattern reminiscent of a stingray or a millipede" (Aouf, 2019). See Figure 3-8 for a picture of the Velox robot.

THE ROBOTIC "EVOLUTION"

The robotics "evolution" is on pace to overtake the expectations of most investors and consumers. Consider Renuka Apte, a former Dropbox and Nvidia employee turned entrepreneur. Apte founded Clockwork, a robotics company that offers robot manicures through self-service kiosks (Clockwork Manicures in Minutes., 2023). It is reported that Clockwork has contracts with Target and XpressSpa in dozens of airports and other locations and plans to have stand-alone stores. Figure 3-9 shows a picture of the robotic manicure station.

Figure 3-9: Robotic Manicure Station

Source: (Clockwork Manicures in Minutes., 2023)

This gives Clockwork access to tens of thousands of customers daily. The company claims that "At just 10 minutes and $10, it's self-care that's fast and affordable" (Clockwork Manicures in Minutes., 2023).

Clockwork creates robots that offer people the ability not to be responsible for everyday tasks. Clockwork indicates they exist to "free people through smart automation— changing how they work, spend their time, and where they find peace of mind. We're utopian dreamers from around the world who believe there is no time to waste on the mundane" (Clockwork Manicures in Minutes., 2023).

AI-THE TRAINABLE BRAIN

The human brain is still a mystery in many ways. Yet AI and other autonomous system programming profiles

attempt to use the human brain patterns to create machines that can learn, think, goal-seek, and work out complex problems using critical thinking skills.

Scientists are starting from the bottom and believing they are now closer to understanding consciousness in completing the world's "first complete, high-resolution brain map of the baby fruit fly. It's the most complex and intricate connectome of any animal's brain ever constructed and paves the way for a revolutionary new frontier of artificial intelligence and neuroscience developments" (Thompson, 2023).

Mapping the brain of the Drosophila Melanogaster, a type of fruit fly, took twelve years to complete. The fruit fly shares a similar biology to that of humans. This tiny insect has 3,016 neurons with 548,000 connections..." (Thompson, 2023). Researchers have been correlating the study of insect brains to humans into an actual trainable AI brain. It is easy to see that although AI is data-rich and offers the beginning of complex problem-solving; it will take a significant effort in funding, research, and development to demonstrate actual progress.

Most people think of killer robots or the adverse actions that these machines can take based on their trainable brains when discussing the concept of AI, machine learning, advanced robotics, or quantum computing in the context of autonomous systems. However, advanced robots are no different from any other technology; they can be used for good or evil or flip-flop from good and bad deeds based on the programmed missions of their human owner.

The healthcare industry benefits as robotics can assist the healthcare worker shortages and advance medicine beyond the current norm. Robots would not replace all humans; they would supplement healthcare workers as robots "could take on basic healthcare tasks to support the work of doctors and nurses may be the way of the future" (Sensing robot healthcare helpers. , 2021).

Woo Soo Kim, associate professor in the School of Mechatronic Systems Engineering, states, "The recent pandemic demonstrates the need to minimize human-to-human interaction between healthcare workers and patients... There's an opportunity for sensing robots to measure essential healthcare information on behalf of care providers in the future" (Sensing robot healthcare helpers. , 2021).

The development of human and machine interfaces can take many forms, such as Elon Musk's Nuerolink (Gilbert, 2019) or in "The development of a cutting-edge graphene sensor has led to the creation of an interface that is able to accurately control a robot using thought alone. The development has positive implications not only for healthcare but for a range of other industries" (McClure, 2023). See Figure 3-10 for a person using a graphene sensory device.

Figure 3-10: Male human wearing an augmented reality visor with graphene sensors attached to the back of the scalp

Source: (McClure, 2023)

The augmented reality visor, as shown in Figure 3-10, serves as a brain-machine interface. "Brain-machine interfaces (BMIs) allow a person to operate a device using their brainwaves. As hands-free and voice-free interfaces, BMIs hold great potential for use in robotics, bionic prosthetics, and self-driving cars" (McClure, 2023).

Nanobots target a brain cancer known as glioblastoma as it builds on previous research at the University of Toronto Robotics Institute. The Hospital for Sick Children (SickKids) research team using Midjourney took a novel approach to a possible answer to glioblastoma. They used nanorobotic scalpel swarms to shred the mitochondria of the cancer cells from the inside. The scalpel swarms were energized by using a magnetic field surrounding the malignant cells "...the tubes were made to spin, wreaking havoc to the internal structure of the cells – particularly to their mitochondria, which fundamentally provides cellular energy. The tubes acted like thousands of mini scalpels that sliced up the cancer cells from the inside (Franco, Nano-robotic scalpel swarm shreds brain cancer cells from the inside, 2023a).

Figure 3-11: Brain image highlighting the surgical area

Source: (Franco, Nano-robotic scalpel swarm shreds brain cancer cells from the inside, 2023a)

Although this technique is specific to help fight glioblastoma, "the new nanobot technique could also be adjusted to work on other types of tumors...Theoretically, by changing the antibody coating and redirecting nanotubes to the desired tumor site, we could potentially have a means to precisely destroy tumor cells in other cancers" (Franco, Nano-robotic scalpel swarm shreds brain cancer cells from the inside, 2023a).

SECURING THE INSTRUCTIONS/QUANTUM REVOLUTION

In a 2023 article titled "An AI Was Trained to Detect Parkinson's Years Before Symptoms Appeared," David Nield discusses how the AI "Using trained layers of nodes modeled on the human brain, the tool hunts for specific chemical compounds (metabolites) in the blood, figuring out the patterns that can potentially predict the presence of disease or protect against it" (Nield, 2023).

Disease prevention is an excellent use of AI; however, what if the AI was trained to attack healthy cells or, on command, kill the host?

Most, if not all, robots/humanoids/autonomous systems are connected via a link to the internet, an intranet, each other, or other systems. These autonomous systems are an extension of the Internet of Things (IoT) as they perform a function with a base set of instructions. Sadly, as the world is discovering, IoT devices are not being designed or built with the proper level of cyber security.

The first open-market humanoid robot was from the Chinese tech firm Xiaomi, named CyberOne, in August 2022. The robot has a starting cost of more than $100,000. The robot claims human-like properties including walking and recognizing dozens of emotions "as it interacts with humans that it encounters" (Stokel-

Walker, 2022). The humanoid robot is 5'9" tall and designed to be at eye level with its human counterpart. In addition, CyberOne can "identify 85 environmental sounds, alongside the 45 human emotions that it can discover, using its AI interaction algorithm that perceives where it is in the world in three dimensions...which allows it to fully simulate human movements" (Stokel-Walker, 2022).

Tesla is not far behind in launching the sale of its robot. Elon Musk, Tesla's Chief Executive Officer, has written that the goal was "for humanoid robots to go beyond industrial work in factories and instead to make themselves at home in the home, helping out with household tasks in a way that would be meaningful" (Stokel-Walker, 2022). Musk continued with his vision. "It is foreseeable that with the power of robots, we will create an era of extreme abundance of goods and services, where everyone can live a life of abundance," Musk wrote. "Perhaps the only scarcity that will exist in the future is for us to create ourselves as humans" (Stokel-Walker, 2022).

All of this is exciting news. However, there does not appear to be any mention of the security protocols on board or how the AI and IoT instructions are being secured, verified, altered, or monitored. The size, shape, and uses of autonomous systems continue to evolve, and so must the security levels in these systems. Consider that "Autonomous mining trucks are a $1.6 billion market and currently account for approximately 2% percent of all mining trucks, but there is a tremendous opportunity with revenue expected to increase to $12.6 billion by 2031" (Reynolds, 2023).

Figure 3-12: A Caterpillar 550 autonomous mining truck

Source: (Reynolds, 2023)

Figure 3-12 depicts a Caterpillar 794AC mining truck equipped with CAT MineStar Command for Hauling. More than 550 CAT autonomous mining trucks are in operation.

The intended or unintended damage of an autonomous system of this size being hacked and given nefarious instructions could be devastating. Mining operations around the world are expanding their use of autonomously operated systems. An "Australian mining firm Roy Hill recently announced the expansion of its AHS by converting its fleet of 96 conventional haul trucks to driverless operation and creating the world's largest autonomous mine" (Reynolds, 2023).

Governments and industries are working together to ensure safety. However, enterprises and governments are not moving as quickly as one would think, as there is currently "no single agency in charge of this issue nor a clear path to creating a support mechanism for future needs. Nor is there a single sensor type, defense posture, or reliable countermeasure currently in place to stop these evolving threats" (Bishop, 2023).

Once considered only science fiction, the shift in the world's workforce to autonomous systems is now a reality.

In its many forms, quantum is an example of forward progress, without adequately recognizing the need for security before marketing a product. The "emergence of potential quantum supremacy has been predicted by 2035. This prediction has caused excitement and an inflection point for the quantum information science ecosystem. Quantum supremacy will require a strategic shift in the workforce to meet this new cross-domain capability" (Bishop, 2023).

Currently, the Institute of Electrical and Electronics Engineers (IEEE) is investigating self-healing systems through a committee known as Cyber Security for Next Generation Connectivity Systems, including developing a standard for fault-tolerant systems to the point of self-healing.

This concept is further discussed in a 2023 article in the Quantum Literacy magazine "Self-Healing Systems is a field of study that finds methods and ways on how a system, service, or product can adjust and self-heal based on various types of triggers or criteria" (Bishop et al., 2023).

This discussion is critical as "building self-healing systems will require the ability to continuously measure systems, services, or products at a sub-component level, all the while adjusting the security configurations based on observed triggers or criteria" (Bishop et al., 2023).

This line of inquiry has a goal to "explore how a system, service, or product could be dynamically protected (in a self-healing manner) based on those observed criteria" (Bishop et al., 2023).

Two researchers have shown how a Tesla — and other cars — can be hacked remotely without user interaction. A drone conducted the attack on the Tesla car (Kovacs, 2021).

The attack, dubbed TBONE, exploits "two vulnerabilities affecting ConnMan, an internet connection manager for embedded devices. A hacker who exploits the vulnerabilities can perform any task that a regular user could from the infotainment system...opening doors, changing seat positions, playing music, controlling the air conditioning, and modifying steering and acceleration modes" (Kovacs, 2021).

To secure the data in advanced computing systems that are required to allow autonomous systems to

operate, manufacturers must start by linking quantum security with the ability "to explore emerging concepts of cyber and supply chain trust models while creating hybrid computing security controls models will enable a digital forensic investigation (DFI) of an alleged supply chain cybersecurity breach to be documented and properly investigated" (Bishop et al., 2023).

CONCLUSIONS

There are many different form factors for robots and autonomous systems. Robots built to operate in the human world give little thought as to how to optimize the world around the robot to allow it to perform its mission more efficiently. Robots are being built to look like humans, take on human emotions, and learn and interact in a world that has been optimized for human beings and even animals, although not autonomous systems.

The critical thinking, learning, and decision engines that are being built into autonomous systems are made by humans; thus, they will have flaws, unintended uses, and consequences. The systems' brains will remain binary all the way. Yet, humans still struggle to understand how a human brain functions, learns best, retains, and retrieves data. This data movement is influenced by emotions driving the body and mind, not in a binary energy exchange. The security required to allow autonomous systems to flourish with minimal risk of hacking and harm to the human and environment around the designs is not in place and, at present, does not appear to be a priority to manufacturers, governing bodies, or governments. The lack of security controls should raise alarms to those conducting research and development, integrators, and the end user.

QUESTIONS

1. Do you think the robotic evolution will see a day when humans no longer work a full-time job or have multiple careers in their lifetime?

2. List three disruptive technologies that have altered the form factor of human systems.

3. How would you design the form factor of a robotic system to make a peanut butter and jelly sandwich? Consider you might need to change the entire supply chain to take advantage of robotic efficiencies.

4. Can a shape-shifting robot be used for good and evil purposes? Please give two examples.

5. In the current cyber security arena, do you think an AI or quantum-driven humanoid can be secured to only run/operate on its given instructions and simplistic critical thinking skills? What level of cyber security do you think is acceptable?
6.

REFERENCES

Aouf, R. S. (2019). *Amphibious Velox robot uses undulating fins to swim and crawl.* . Retrieved from dezeen.com/: https://www.dezeen.com/2019/02/07/amphibious-velox-robot-technology/

Bandakkanavar, R. (2021). *The truth about Humanoid Robots.* Retrieved from krazytech.com/technologies/humanoid-robots: https://krazytech.com/technologies/humanoid-robots

Bishop, J. A. (2023). *Quantum Supply Chain – Cybersecurity Logistics. Quantum Literacy Magazine.* . Retrieved from quantumliteracy.org/: https://quantumliteracy.org/national-quantum-literacy-magazine/

Blain, L. (2023). *Sanctuary rolls out Phoenix, a Carbon-based humanoid AI labor robot.* . Retrieved from newatlas.com: https://newatlas.com/robotics/sanctuary-ai-phoenix-humanoid-robot/?utm_source=New+Atlas+Subscribers&utm_campaign=9372c1c223-EMAIL_CAMPAIGN_2023_05_19_02_

Clockwork Manicures in Minutes. (2023). Retrieved from likeclockwork.com/: https://likeclockwork.com/

Coxworth, B. (2023). *Bubbling "BeerBots" could boost the brewing of beer.* . Retrieved from newatlas.com/science/: https://newatlas.com/science/beerbots-beer-brewing/?utm_source=New+Atlas+Subscribers&utm_campaign=49a77ebaec-EMAIL_CAMPAIGN_2023_04_26_01_35&utm_medium=email&utm_term

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

Franco, M. (2023a). *Nano-robotic scalpel swarm shreds brain cancer cells from the inside.* Retrieved from newatlas.com/medical/nano-robotic-scalpel-brain-cancer/?utm_source=New+Atlas+Subscribers&utm_campaign=10e825078c-EMAIL_CAMPAIGN_2023_04_28_01_: https://newatlas.com/medical/nano-robotic-scalpel-brain-cancer/?utm_source=New+Atlas+Subscribers&utm_campaign=10e825078c-EMAIL_CAMPAIGN_2023_04_28_01_

Franco, M. (2023b). *Robotic jellyfish can suck up ocean debris without touching it.* . Retrieved from newatlas.com/marine/robotic-jellyfish-ocean-debris/?utm_source=New+Atlas+Subscribers&utm_campaign=49a77ebaec-EMAIL_CAMPAIGN_2023_04_26_01_35&utm_med: https://newatlas.com/marine/robotic-jellyfish-ocean-debris/?utm_source=New+Atlas+Subscribers&utm_campaign=49a77ebaec-EMAIL_CAMPAIGN_2023_04_26_01_35&utm_med

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/

Gilbert, B. (2019). *Elon Musk finally took the wraps off his new brain microchip company that plans to*

connect people's brains to the internet by next year. . Retrieved from www.businessinsider.com/: https://www.businessinsider.com/what-is-elon-musk-brain-chip-comp

Green, L. C. (1998). *The Law of War in historical Perspective.* Providence, RI: U.S. Naval War College.

Hallevy, G. (2015). *Liability for Crimes Involving Artificial Intelligence Systems.* Switzerland: Springer.

Hoynes, C. W. (1916). *Preparedness for War and National Defense.* Washington, DC: Government Printing Office.

International Committee of the Red Cross. (2022, March 19). *The Geneva Conventions of 1949 and their Additional Protocols.* Retrieved from The International Committee of the Red Cross: https://www.icrc.org/en/doc/war-and-law/treaties-customary-law/geneva-conventions/overview-geneva-conventions.htm

Jellyfish-like robots could one day clean up the world's oceans. (2023). Retrieved from is.mpg.de/news/quallenahnliche-roboter-konnten-eines-tages-die-weltmeere-saubern: https://is.mpg.de/news/quallenahnliche-roboter-konnten-eines-tages-die-weltmeere-saubern

Khillar, S. (2020). *Difference Between Humanoid and Robot.* . Retrieved from www.differencebetween.net/technology/difference-between-humanoid-and-robot/: http://www.differencebetween.net/technology/difference-between-humanoid-and-robot/

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.

Knight, W. (2023, March 23). *For Smarter Robots, Just Add Humans.* . Retrieved from www.wired.com/story: https://www.wired.com/story/fast-forward-for-smarter-robots-just-add-humans/

Kovacs, E. (2021). *Tesla Car Hacked Remotely From Drone via Zero-Click Exploit.* . Retrieved from www.securityweek.com/: https://www.securityweek.com/tesla-car-hacked-remotely-drone-zero-click-exploit/

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/

McClure, P. (2023). *New graphene sensors make for better brain-machine interface.* . Retrieved from newatlas.com/technology/: https://newatlas.com/technology/graphene-sensor-interface-thought-controlled-robot/?utm_source=New+Atlas+Subscribers&utm_campaign=19ef55bc25-EMAIL_

Merriam-Webster. (2023). *Definition of Body.* (Vols. 2023). Merriam-Webster.

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/

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

Nield, D. (2023). *An AI Was Trained to Detect Parkinson's Years Before Symptoms Appeared. Science Alert.* Retrieved from www.sciencealert.com/: https://www.sciencealert.com/an-ai-was-trained-to-detect-parkinsons-years-before-symptoms-appeared?utm_source=ScienceAlert+-+Daily+Emai

Reynolds, S. (2023, May 9). *This Adaptation Allowed Dinosaurs to Not Only Survive But to Dominate The Planet.* . Retrieved from www.sciencealert.com/: https://www.sciencealert.com/this-adaptation-allowed-dinosaurs-to-not-only-survive-but-to-dominate-the-planet

Sanctuary AI-Creating human-like intelligence. . (2023). Retrieved from www.sanctuary.ai/: https://www.sanctuary.ai/

Selbst, A. D. (2020). NEGLIGENCE AND AI'S HUMAN USERS . *Boston University Law Review*, 1323.

Sensing robot healthcare helpers. . (2021). Retrieved from www.sciencedaily.com/: https://www.sciencedaily.com/releases/2021/02/210227083259.htm

Stokel-Walker, C. (2022). *Science fiction as reality: Tesla joins Xiaomi in releasing first humanoid robots.* . Retrieved from cybernews.com/editorial/: https://cybernews.com/editorial/tesla-and-xiaomi-humanoid-robots/

Thompson, B. (2023). *Insect Brain Map a Landmark First Step in Unlocking Human Consciousness.* . Retrieved from //newatlas.com/: https://newatlas.com/science/insect-brain-map-first-step-human-consciousness/?utm_source=New+Atlas+Subscribers&utm_campaign=3b13f5d3e5-EMAIL_CAMPA

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

Woolfolk, D. (2023). *Prehistoric sea creature-like robot can navigate surf, crawl up onto the beach.* Retrieved from www.militarytimes.com: https://www.militarytimes.com/video/2023/04/10/prehistoric-sea-creature-like-robot-can-navigate-surf-crawl-up-onto-the-beac

4.

AI / ML AND AGRICULTURE AND FOOD INDUSTRIES [NICHOLS, HOOD, SINCAVAGE]

LEARNING OUTCOMES

AI in the Agricultural (Ag) and food industries comprise a number of technologies, from robotics to machine learning. By "AI" we are simply referring to machinery and technologies used to conduct complex tasks that previously required human thought to complete. Our purposes:

- To explore artificial intelligence (AI) and Machine Learning (ML) in the world of agriculture, food production and global food supply.
- To investigate AI related technologies from space operations to earth manufacturing with the goal of feeding the world population more efficiently.
- To recognize the US will continue to be vulnerable to deliberate introductions of exotic plant and animal diseases by terrorist groups and to identify effects.

INTRODUCTION

In 2023, Artificial Intelligence (AI) is the subject of thousands of articles and books. Artificial intelligence is defined as: "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." (Definition of Artificial Intelligence , 2023). Chapter 4 is devoted / limited to continuing our humanitarian goal of using technologies to improve the lives of the global population. In our previous textbook, *Space Systems: Emerging Technologies and Operations*(Nichols R. K., et al., 2022), Section III included three chapters on the subject. Chapter 10 covered Drones and Precision Agricultural Mapping. (Mumm, 2022) Chapter 11 covered Civilian use of Space for Environmental, Wildlife Tracking, & Fire Risk Zone ID. (Ryan, 2022) Chapter 12 addressed the Humanitarian Use of Space Technologies to Improve Global Food Supply & Cattle Management. (Larson, 2022)

"SECTION 3 is our Hope for Humanity and Positive Global Change. Just think if the technologies we

discuss, when put into responsible hands, could increase food production by 1-2%. How many more millions of families could have food on their tables?" (Nichols R. K., et al., 2022)[1]

ARTIFICIAL INTELLIGENCE AND AGRICULTURE: HOW INTELLIGENT TECHNOLOGIES CAN HELP FEED THE WORLD

AI has significant potential to improve the agricultural industry and help feed the worlds growing population. Through applications like precision agriculture, livestock monitoring, supply chain optimization, and labor optimization, AI can provide farmers with essential information and insights to make better decisions about productivity. (Zheng, 2023)

However, there are challenges that must be addressed in the adoption of AI (and ML) in Agriculture (Ag) such as: data availability and quality, integration with legacy systems, and cost. Ethical considerations of transparency, accountability, fairness, and privacy must be integrated into the AI systems implemented.

There is also the threat of using AI to implement Bioweapons in the Ag sphere and necessity of risk assessments to reduce vulnerabilities from these threats and to apply appropriate countermeasures. (Nichols & Carter, 2022) (Nichols R. K., et al., 2022)

TYPES OF ARTIFICIAL INTELLIGENCE

AI dates back to the 1950's with rule-based systems. In recent years, sophisticated AI algorithms capable of complex decision-making and problem-solving tasks have been built. AI takes many forms:

Rule-based AI: aka expert systems, uses pre-programmed data and rules and relies on "if-then" statements and logical rules to make decisions.

ML: a form of AI that involves developing algorithms that can learn from data and improve performance over time.

Deep Learning: ML subset that focuses on neural networks with many layers of processing. They are used to analyze "big data," or large amounts of data, image recognition, speech recognition, and natural language processing.

Reinforcement Learning: see definition below.

Natural Language Processing (NLP): is a type of AI involving analyzing and generating human language. NLP is used in chatbots, voice assistants, and language translations.

Reactive Machines: Only respond to specific stimuli and do not learn or predict outcomes

Limited Memory: Limited to specific data sets are able to learn to improve performance

Self-Aware: Theoretical and would possess human-like consciousness and emotions.[2] (Zheng, 2023)

Similarly, there are growth in the machine learning (ML) techniques:

Supervised Learning: Training an AI system with labeled data sets and allowing it to make predictions,

Unsupervised Learning: Training an AI system on unlabeled data sets and enabling them to identify patterns and relationships without guidance,

Reinforcement Learning: Training an AI system through trial and error, rewarding it for correct decisions and punishing it for incorrect ones. (Zheng, 2023)

AG LANDSCAPE

The global landscape of agriculture is diverse and complex with different regions and countries facing unique challenges and opportunities. (Zheng, 2023) identifies key global trends in the Ag and food production.

Growing population and food demand: Global population is projected to reach 9.7 billion by 2050, leading to a significant increase in global food demand. (Zheng, 2023)

Climate change and environmental pressures: Climate change and environmental pressures pose significant challenges for agricultural production. More frequent and severe weather events such as droughts and floods can affect crop yields and increase production costs. "The agriculture industry needs to adopt sustainable practices to minimize its environmental footprint." (Zheng, 2023)[3] See (Wrightstone, 2017) and (R. K. Nichols, 2021)also for different perspectives.

Technical advancements in Ag: we have come a long way from simple tools and plows to advanced machinery like tractors and combines. Now AI offers the next generational step to improve efficiency, productivity, and sustainability in Ag. (Zheng, 2023)

Changes in Crops and Livestock production: Resources, cultural practices, cultivation readiness affect the high-value crops such as rice, wheat, fruits, and vegetables all may change with the AI use. Similarly, livestock production including dairy, meat, and poultry will be directly affected by AI. (Zheng, 2023) Land ownership will change, and this has an indirect affect on the introduction if AI technologies. [4]

Supply chain and distribution: Ag supply chains comprise a network of producers, processors, distributors, wholesalers, and retailers who collectively ensure that food reaches consumers. Logistics and distribution play a critical role in maintaining the quality and safety of food products during transportation. (Zheng, 2023)

Policy and Regulation: policies, regulations, environmental practices, food safety inspections, labor standards can vary significantly from country to country and may have significant implications for the industry's sustainability and profitability. (Zheng, 2023)

SURVEYING THE POTENTIAL OF AI IN AGRICULTURE

A good place to start is a review of Louis Columbus' Forbes article on the 10 Ways AI Has The Potential To

Improve Agriculture In 2021. [5] (Columbus, 2021) We follow this review with a report on Dr. MingHai Zheng's 2023 book entitled *Artificial Intelligence and Agriculture: How Intelligent Technologies Can Help Feed the World*. Dr. Zheng explores the current state-of-the-art intersection of AI and agriculture, focusing on how intelligent technologies can be used to improve farming practices and increase productivity. Dr Zheng's goal is to identify opportunities for future research and development. Along with Hope comes Evil. Our survey will include selected directions from our own research chaired by international SME Dr. Suzanne M. Sincavage in her *Chapter 8. Bio-threats to Agriculture-Solutions from Space*. (S. Sincavage, 2022)

AI POTENTIAL TO IMPROVE AGRICULTURE

The driving force is money. According to BI Intelligence Research, global spending on smart, connected agricultural technologies and systems, including AI and machine learning (ML) is projected to triple in revenue by 2025 to $15.3 billion. (Top 5 2023 Agriculture Trends to Watch, 2023). (Columbus, 2021) Spending on AI solutions for agriculture is predicted to grow at a whopping CAGR[6] of 25.5% to $4 billion in 2026. (Columbus, 2021) 87% of U.S. agricultural businesses use AI. (87-of-us-agriculture-businesses-are-currently-using-ai, 2021) According to Allied Market Research, IoT enabled agricultural (IoTAg) monitoring is the fastest connected growing technology segment projected to reach $84.5 billion by 2031 growing at CAGR of 12.6%. (Allied Market Research, 2023) How valid these estimates are only time will tell, however, we conclude there is considerable financial interest in AI/ ML and real-time sensor data to apply to agricultural applications, such as precision farming, livestock monitoring, [7] smart greenhouses, and fish farm monitoring.

AI, machine learning (ML) and the IoT sensors that provide real-time data for algorithms increase agricultural efficiencies, improve crop yields, and reduce food production costs. (Columbus, 2021)Of special interest is IoT- enabled sensors and devices that allow farmers to remotely monitor soil moisture, temperature, and other conditions to optimize crop yields and reduce water usage. (Allied Market Research, 2023)

Linking farms through a single platform and sharing intelligence gained is another method to improving productivity and reducing waste. Allied Market Research, 2023)

IoT boosts agricultural output. Real time field data collection, storage, analysis, and control platforms improve operational efficiency and increase crop yields. Excellent data portends the success of crop cycles. (Columbus, 2021) Think of the many processes that farmers must track weather, seasonal sunlight, migratory patterns of animals, birds, insects, deer,[8] use of specialized fertilizers, insecticides by crop, planting cycles and irrigation cycles all affect yield. These are perfect for AI and ML solutions. Data-centric approaches work. (Columbus, 2021)

SURVEILLANCE

Using AI and ML- based surveillance systems to monitor every crop field's real-time video feeds identifies

animal or human breaches, sending an alarm or alert immediately can be remarkably effective, *annoying* [9] and provide evidence, if necessary, in a police call. On the positive side, AI / ML reduce domestic and wild animals potential to accidentally destroy crops or experience a break-in or burglary at a remote farm location. Farm perimeter security can be augmented. AI /ML solutions are scalable. (Columbus, 2021)

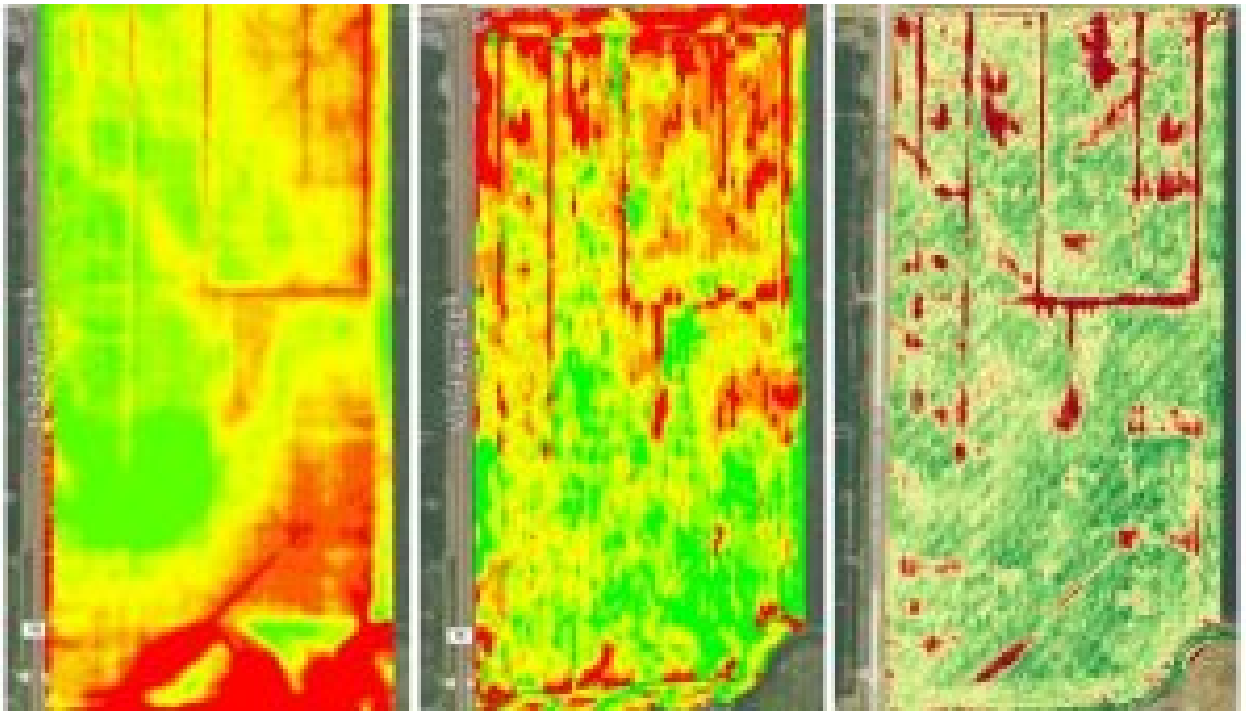
CROP YIELD PREDICTION

Crop yield predictions are improved through real-time AI/ML sensor data and visual analytics data from drones. (Larson, 2022) Drones provide real-time streaming on large acreage via "Earth Traces." These make it possible to combine in-ground sensor data on moisture, fertilizer, and natural nutrient levels plus *water / irrigation availability* to analyze growth patterns of each crop over time. (Nichols R. K., et al., 2022) (Columbus, 2021) Understanding yield rates and quality levels of crops help agricultural firms, co-ops and farmers better negotiate for the best possible price for their harvests. (Columbus, 2021)

YIELD MAPPING

"Yield mapping is an agricultural technique that relies on supervised machine learning algorithms to find patterns in large-scale data sets and understand the orthogonality of them in real-time – all of which is invaluable for crop planning." (Columbus, 2021) Potential yield rates of a given crop field can be estimated before a vegetation cycle is started. Some of the techniques deployed are ML, 3-Dmapping, social condition data from IoT sensors and drone-based data on soil-color. (Ryan, 2022) (Columbus, 2021) (See Figure 4-1 example Integration.)

Figure 4-1 Integrate UAV Technology with Yield Maps

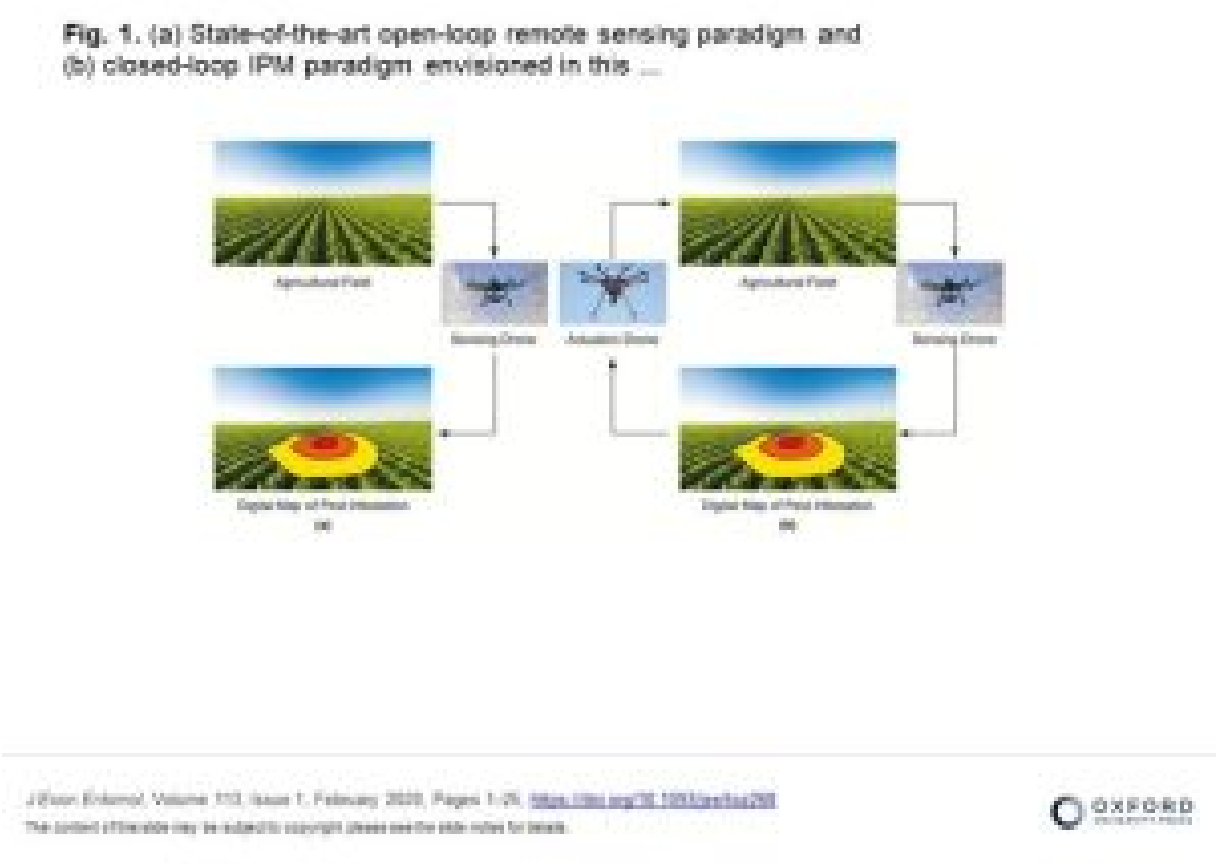


Source: (Integrate UAV Technology with Yield Maps, 2023)

DRONES AND PESTS

The UN, international agencies, and large-scale agricultural operations (and Kansas State University)[10] are pioneering drone data combined with in-ground sensors (and weather stations) [11]to improve pest management. (Mumm, 2022) Drones using IR camera data combined with sensors on fields and weather data, which monitor plants' health, permit prediction and identification of pest infestations. (Mumm, 2022) (Columbus, 2021) (Figure 4-2)

Figure 4-2 (a) State-of-the-art open-loop remote sensing paradigm and (b) closed-loop IPM paradigm envisioned in this article. Sensing drones could be used for detection of pest hotspots, while actuation drones could be used for precision distribution of solutions.



Source: Adapted from (Teske A. L., 2019)

Both (Mumm, 2022) and (Columbus, 2021) point out that AI/ML optimization biodegradable pesticides to only the field areas that need treatment, reduces costs, and increases yields. By using intelligent sensors combined with visual data streams from drones, agricultural AI applications can now detect a planting area's most infected areas. Using supervised machine learning algorithms, they can then define the optimal mix of pesticides to reduce pests' threat spreading further and infecting healthy crops.

FARM EMPLOYEE TROUBLE? AI TO RESCUE

In 2023, there's a shortage of agricultural workers, making AI and machine learning-based smart tractors, agribots and robotics a viable option for many remote agricultural operations. Large farming operations turn to robotics for hundreds of acres of crops while also providing an element of security around the perimeter of remote locations. Programming self-propelled robotics machinery to distribute fertilizer on each row of crops helps keep operating costs down and improve field yields. (Columbus, 2021)

TRACK AND TRACEABILITY (T&T)

Improving the track-and-traceability of agricultural supply chains by removing roadblocks to get fresher, safer crops to market is a must-have Tin 2023. A well-managed T&T system helps reduce inventory shrinkage by providing greater visibility and control across supply chains. A state-of-the-art T&T system can differentiate between inbound shipments' batch, lot, and container level assignments of materials. T&T systems rely on advanced sensors to gain greater knowledge of each shipment's condition. RFID and IoT sensors are now becoming more commonplace across manufacturing. (Columbus, 2021)

WATER

AI/ML optimizing irrigation systems and measuring how effective frequent crop irrigation improves yield rates are all areas AI contributes to improving farming efficiencies. Water is the scarcest resource in many parts of North America, especially in communities that rely most on agriculture as their core business. Being efficient in using it can mean the difference between a farm or agricultural operation staying profitable or not. (Columbus, 2021) (Larson, 2022) (Mumm, 2022) (Ryan, 2022)

LIVESTOCK

(Larson, 2022) discusses monitoring cattle health and food intake. Dr Larson validates (Columbus, 2021) conclusions about livestock in his Forbes article. **"**Monitoring livestock's health, including vital signs, daily activity levels and food intake, ensures their health is one of the fastest-growing aspects of AI and machine learning in agriculture. Understanding how every type of livestock reacts to diet and boarding conditions is invaluable in understanding how they can be best treated for the long term. Using AI and machine learning to understand what keeps daily cows content and happy, producing more milk is essential. For many farms who rely on cows and livestock, this area opens up entirely new insights into how farms can be more profitable." (Columbus, 2021)

ROBOTS AND AI

According to research by the University of Sydney, Ag-robots have the potential to mitigate food security issues.[12] (University of Sydney, 2022) Ending global hunger has long been a critical goal for the global community. When the United Nations' Sustainable Development Goals were released in 2014, ending hunger, food insecurity and all forms of malnutrition formed SDG2. (University of Sydney, 2022)

"Though there has been some progress in the fight against hunger – ongoing conflicts, economic downturns and the COVID-19 pandemic have been major barriers to achieving SDG2. As of 2020, according to the UN,

720 and 811 million people globally faced hunger, and current estimates suggest that 660 million people may still face hunger in 2030." (University of Sydney, 2022)

Professor Salah Sukkarieh, a robotics engineer at the University of Sydney's Australian Centre for Field Robotics, and his team have developed *Digital Farmhand*, a small, autonomous, electric tractor-like vehicle can assist smallholder farmers to improve their productivity and yields.

"Our Digital Farmhand robot is designed to assist smallholder farmers to improve their productivity and yields and provide a more reliable income amidst changing markets and climates. In its simplest form the Digital Farmhand is a small, autonomous electric tractor-like vehicle that can tow a variety of implements such as seeders, weeders, and bed preparation tools, and can undertake precision automation of many labor-intensive farm tasks, like weeding, spraying, and seeding." (University of Sydney, 2017)

"Digital Farmhand can also use accessible smartphone technologies along with AI to provide crop analytics such as yield estimation or pest and disease identification." (University of Sydney, 2022) Professor Sukkarieh's team is developing open-source artificial intelligence packages for smartphones which can be easily accessed in the APAC. (University of Sydney, 2017) [13]

Figure 4-3 Digital Farmland

Source: http://confluence.acfr.usyd.edu.au/display/AGPub/Our+Robots ((University of Sydney, 2017)9

5 WAYS AI IMPROVES FOOD MANUFACTURING

Aptean is a large food service technology organization. Aptean presents 5 ways that they predict that AI will change food manufacturing for the better.

1. Developing New Recipes Guided By Consumer Trends

According to Aptean's VP John Payne, "all food manufacturers know that they must constantly be on the lookout for new ways to refresh their product lines in order to stay relevant and tap into new sources of revenue. Whereas this has traditionally taken the form of surveys and adapting to emerging trends, AI offers companies the opportunity to predict their customers' preferences.

By analyzing huge amounts of data around sales patterns and flavor preferences for each demographic group, manufacturers are now able to model future trends and develop new products to capitalize on them quicker. AI is also being used to allow consumers a greater degree of personalization in the products they buy. This breakthrough doesn't just identify what the most popular flavor combinations are likely to be, it makes the product development process shorter and less expensive, helping companies get their new products to market faster and with less trial and error." (Payne, 2021)

2. Supply Chain Management

Being able to manage supply chains effectively is one of the top priorities for food manufacturers. Companies at the cutting edge are now utilizing algorithms based on artificial neural networks to monitor shipments at every stage of the supply chain, improving food safety standards and enabling full transparency. AI in the food industry is also capable of creating accurate forecasts to manage inventory and pricing. This kind of predictive analysis helps keep food businesses one step ahead, enabling them to avoid wastage and unnecessary costs, said Mr. Payne. (Payne, 2021)

3. A More Efficient Cleaning Process

All equipment and machinery involved in food production needs to be cleaned to the most rigorous standards. This isn't just to avoid contamination of food with pathogens, but to prevent allergen cross-contamination. Unfortunately, this comes at a cost—in terms of both time and money. Innovative AI technology is beginning to change this. Developed by the University of Nottingham, a Self-Optimizing-Clean-In-Place (SOCIP) system uses optical fluorescence imaging and ultrasonic sensing to scan the food remains left in machinery after use. (University of Nottingham SOCIP, 2016) [See Figure 4-4] This allows for a more optimized cleaning process, where the amount of water needed is cut by 20-40% and the cleaning time is reduced by 50%, because equipment no longer needs to be disassembled. (Payne, 2021)

4. More Hygienic Production Lines

Food safety breaches can be unbelievably costly for food manufacturers. Both in terms of fines and the reputational damage associated with poor health and safety. AI in food manufacturing is reducing the risk of such breaches in a number of ways. The more parts of the food production process that can be dealt with by robots, the less likely products are to become contaminated with pathogens. Robots can be made completely sterile. AI can be used to increase the cleanliness of a manufacturer's human workforce. Facial and object-recognition technologies are being used to track whether hygiene protocols are being followed. (Payne, 2021)

5. Food Sorting

Food sorting is a laborious and time-consuming process that slows the production line and requires the employment of many staff members. This is especially true when it comes to the sorting of fresh produce items—with human sorters responsible for removing all units that aren't at the standard required for sale. The amount of time and the number of people required to complete this crucial activity can be reduced with the assistance of AI. Cameras and lasers are used to assess the shape, color, and structural integrity of every item, automatically identifying ones which need to be filtered out. (Payne, 2021)

Figure 4-4 SOCIP

Source: (University of Nottingham SOCIP, 2016)

WIZATA

WIZATA in Luxembourg adds a key element to Payne's list. Along with Sorting Food, Improving Cleaning Processing, Supply Chain Management and Growing Better Food, they add emphasis to Food Safety Compliance. (WIZATA, 2023) Safety is the top priority for all food processing businesses. All employees and workers who come in direct touch with food have to wear a proper costume and comply with safety standards. Tracking hundreds of employees and making sure that everyone follows the rules is easier said than done. AI-enabled cameras can monitor all workers and notify managers in case a rule is broken. The AI can quickly identify safety issues such as not wearing proper food protection gear or not complying with the rules. The AI can monitor production in real-time and send warnings directly to workers or their managers. (WIZATA, 2023)

AI AND RESTURANTS

Escoffier.edu teaches courses in restaurant management. Part of their culinary, pastry and courses for restaurant discipline presents students with a seminar in how AI is changing restaurants. Here are the 9 ways that AI is improving restaurant efficiency:

1. Personalized menu recommendations for guests
2. Permitting management to make predictive analytics for smarter forecasting
3. Chatbots to answer questions, take orders, and set reservations
4. Improved cost tracking and menu pricing
5. AI-integrated inventory & purchasing to save time
6. Robotic food delivery
7. More efficient food production
8. Developing a stronger and safer supply chain
9. Predicting Consumer Response to new products. (escoffier.edu, 2023)

INDIA AND ETHIOPIA

In an extensive Indian and Ethiopian joint university research project lead by Dr. Indrajeet Kumar, AI and ML were reviewed in *Opportunities of Artificial Intelligence and Machine Learning in the Food Industry. (Kumar, Rawat, Mohd, & Husain, 2021)*[14]***[15]***

Their findings for AI and ML in the food industry are consistent with all the OSI addressed factors identified/discussed elsewhere in this chapter. See Figures 4-5, 4-6, 4-7, 4-8, and 4-9 for image summaries of Dr. Kumar's team findings.

Figure 4-5 shows the roles that AI plays in the food industry:

Food Security management

- Image processing and recognition technologies
- Fertilizer management
- Food inspection and grading
- Robots for warehouse functions
- Food security through information sharing

Food Quality management

- Food quality
- Modeling
- ML for increased productivity
- Pesticide management

Figure 4-6 shows AI / ML important applications taken from food processing and handling industry:

- Products sorting and packaging
- Personal health sanitation
- Customer interactions and decisions
- Equipment cleaning and maintenance
- New products
- Demand-supply chain management

Figure 4-7 shows how AI is used for data analysis in the food industry:

- Introducing new recipes
- Food delivery
- Customer satisfaction

Figure 4-8 shows ML applications in the restaurant business:

- Food vending terminals
- Customer feedback
- Food delivery
- Revenue prediction
- Online restaurant search engine
- Voice assistants
- Self-ordering kiosk system
- Robotics

Figure 4-9 shows two key AI uses in food safety:

- NGS and electric noses [16]
- Food waste management

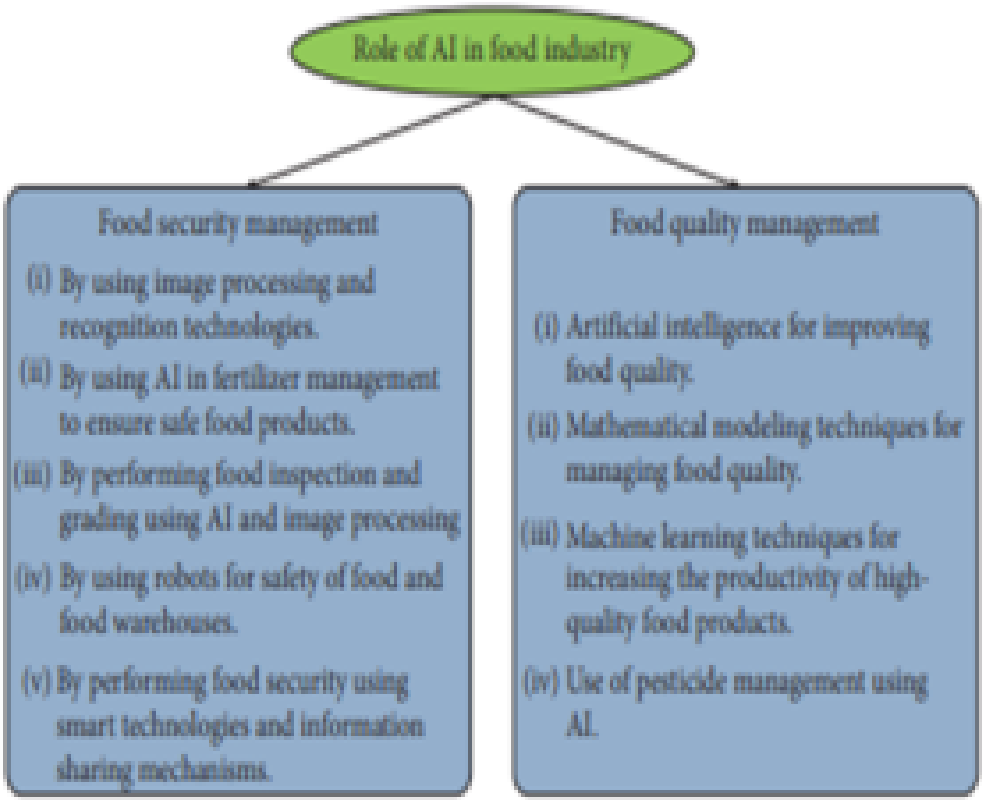
NEXT-GENERATION SEQUENCING AND ELECTRIC NOSES

The two most promising inventions in the food industry are next-generation sequencing (NGS) and electric noses (ENs). NGS is replacing the DNA approach in the food security region very quickly. The introduction of AI-based automated systems and workflows helped formulate data acquisition and laboratory trials much quicker and more accurately. NGS can find hazardous inclination very quickly and efficiently. It can also prevent the infection epidemics before the impairment of an ample amount of people. ENs are the surrogate for a person muzzle in fabrication surroundings. Some sensors are placed that can precisely identify a diversity of smells. These sensors just sense the smell around the surroundings, and sensed data are transferred to a data center where ML algorithms access these data (Fedorova, Darbasov, & Okhlopkov, 2020) (Yu, Lin, & Wu, 2020). According to the decision made by the ML-based system, an alarm signal is transferred to the

manufacturing units. EN can be the upcoming future of food products safety. (Kumar, Rawat, Mohd, & Husain, 2021) However, they did present clarifications of interest on smart farming (SF) technologies.

AI in SF has some important applications such as soil monitoring, robot cropping, and predictive analysis.

Figure 4-5 Role of AI in the Food Industry

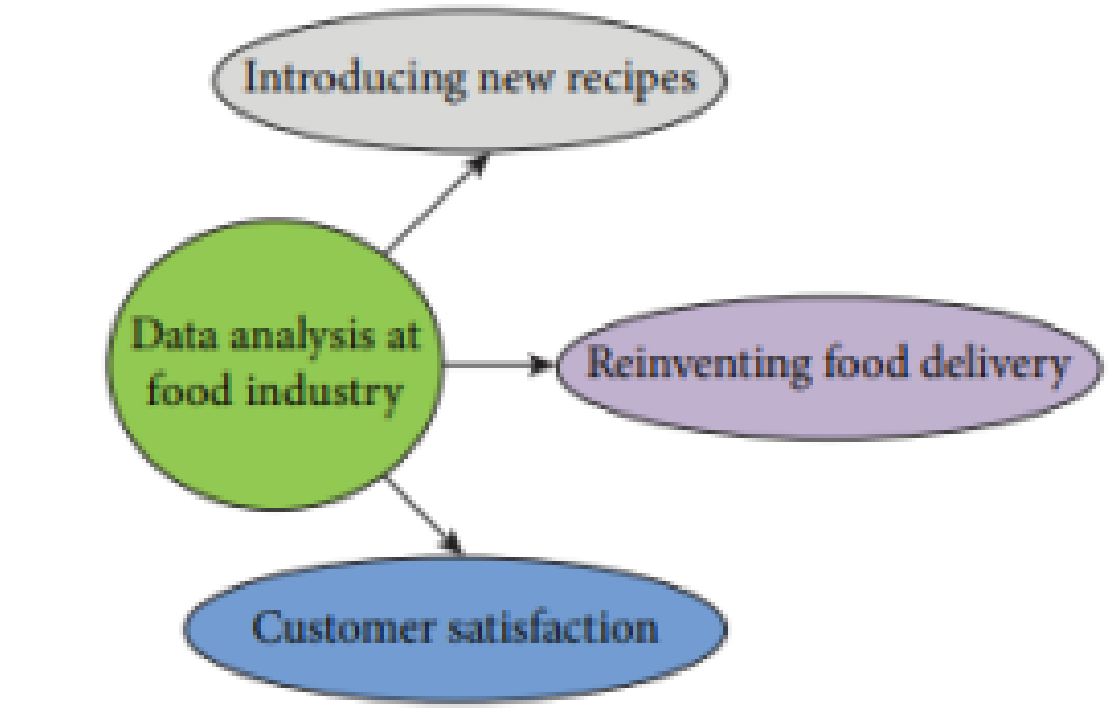


Source: Adapted from Figure 1, p2 in (Kumar, Rawat, Mohd, & Husain, 2021)

Figure 4-6 Important Applications Taken From Food Processing And Handling Industry

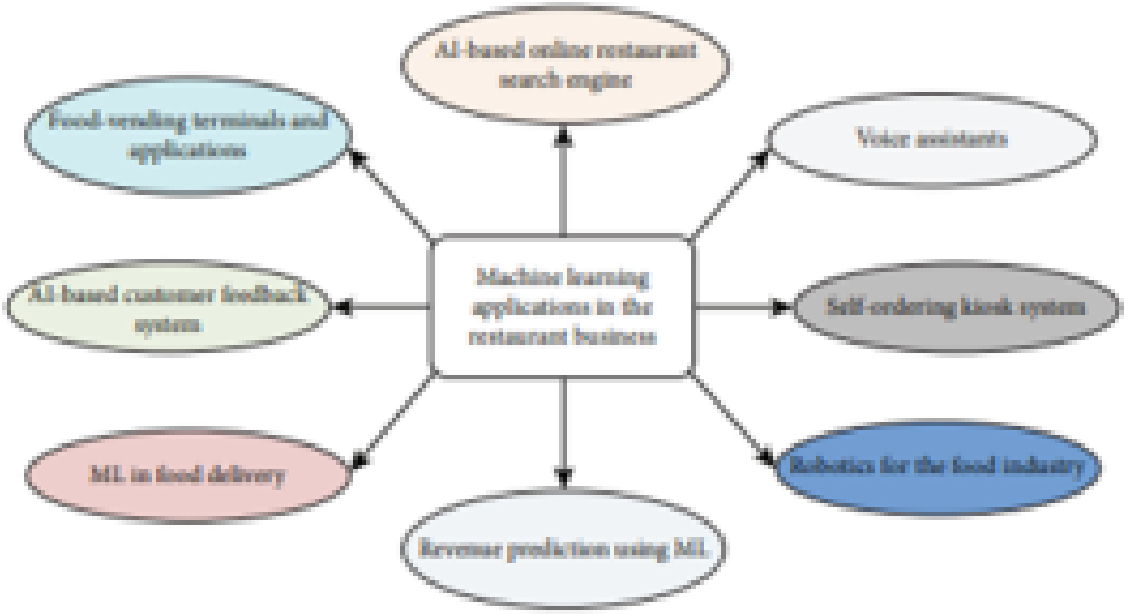
Source: Adapted from Figure 4, p4 in (Kumar, Rawat, Mohd, & Husain, 2021)

Figure 4-7 Data Analysis in the Food Industry



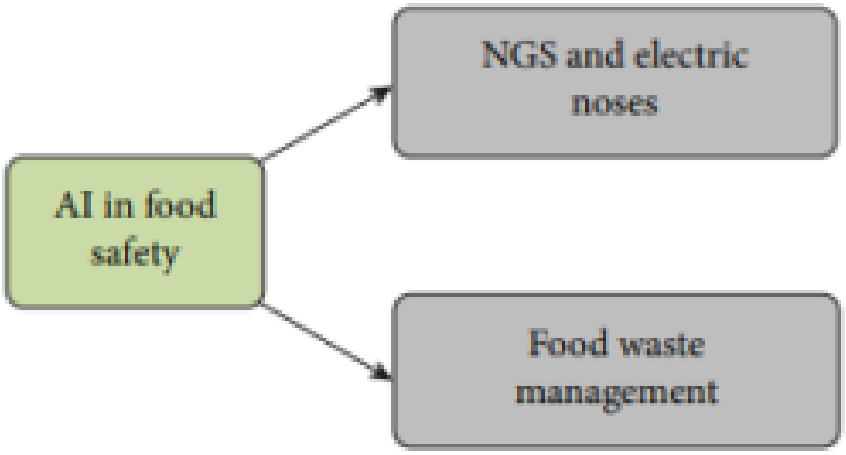
Source: Adapted from Figure 5, p6 in (Kumar, Rawat, Mohd, & Husain, 2021)

Figure 4-8 ML Application In The Restaurant Business



Source: Adapted from Figure 6, p6 in (Kumar, Rawat, Mohd, & Husain, 2021)

Figure 4-9 AI in Food Safety



Source: Adapted from Figure 7, p8 in (Kumar, Rawat, Mohd, & Husain, 2021)

SOIL MONITORING (SM)

Under the AI-based system, computer vision and deep-learning algorithm is particularly important and used to investigate the sequence of information or data received by the AI-based agents to trace the progress of crop and soil health. Computerized systems are used to make available clients with a sagacity[17] of their soil's strengths and weaknesses. The prime objective behind the building of the developed system is to identify defective crops and identify the probable approach for healthy crop development. (Kumar, Rawat, Mohd, & Husain, 2021)

Companies are taking advantage of agriculture AI and aerial technology (Drones / UAS) to keep an eye on crop health. The company's primary reason is to decrease the costs and improve crop growth. Users preprogram the drone's route and then integrate with the device. After that, the computer vision will record some pictures that will be used for examination purposes. (Kumar, Rawat, Mohd, & Husain, 2021)

IoT plays an important role in decision on crop and soil monitoring (Raut, Varma, Mulla, & Pawar, 2018). SM with IoT is the application of AI that supports farmers and food industries to capitalize on their economy,

diminish the chances of ailment, and optimize uses of available assets. In these, sensors are deployed to sense the temperature of the soil, amount of nitrogen, phosphorus, and potassium (NPK) in soil, moisture level, the content of water, potential in soil, amount of photosynthetic radiation, and oxygen level in soil (Bhattacharyya, Sarkar, Sarkar, Sinha, & Chanda, 2020). Collected data from the various sensors [Table 4-1]are forwarded to the cloud for action. The outcome of the analysis, visualization of received data, is helpful in resource use. The identification of the behavior of the system requires identifying the trends of soil and making the decisions to maximum crop yield and excellent products. (Raut, Varma, Mulla, & Pawar, 2018) (Bhattacharyya, Sarkar, Sarkar, Sinha, & Chanda, 2020). Agriculture based IoT is called *smart agriculture*. IoT-based food industry is called the *smart food industry. (Kumar, Rawat, Mohd, & Husain, 2021)*

ROBOCROP

Robocrop is an AI-based robotic system that advances the yielding process by maximizing usefulness and uniformity. It conducts line up crop tools accurately and at a high rate. The food industry product shrubbery forward of the system is monitored by a high-resolution and precise system. The captured image is processed by a high-performing workstation to attend the maximum attentiveness of green band pixels relating to the crop line. Due to the outsized region captured by the input devices and the numerous processing line, an outstanding typical crop Center-line tracking is accomplished (Machleb, Peteinatos, Kollenda, And′ujar, & Gerhards, 2020). It evaluates the resultant image to a ground truth gridiron pattern with the crop line area. The obtained information is then employed to align the instruments in the row via a hydraulic-based shift. The pattern-based attribute builds the system healthy besides backdrop pick over infestations. It improves the performance and production rate just because of multicameras and multiple sensors. (Kumar, Rawat, Mohd, & Husain, 2021) See example in Figure 4-10.

Dr. Kumar describes several advanced Robocrop systems, including dual arm systems for fruit harvesting; robotic weeding systems; robot image systems for identifying plant growth; and adaptive robot chassis (ARC) for sorting strawberry flowers. (Kumar, Rawat, Mohd, & Husain, 2021)

Figure 4-10 Robocrop picking crops

Source: Adapted from Figure 3, p4 i**n**(Kumar, Rawat, Mohd, & Husain, 2021)

"The performance of the Robocrop completely depends on input image features. If the input image contains more dominant features, then it shows outstanding results. In every sample of an input image, the crop must present more shrubbery than the wildflower and the crop shrubbery should be near to the mean of the RGB color band. A typical Robocrop system consists of a Robocrop console part, a hydraulic-based shaft, a three-point linkage frame, a high-definition camera, various types of speed sensors, an ADC adapter, and infrastructure." (Machleb, Peteinatos, Kollenda, And´ujar, & Gerhards, 2020) See Figure 4-10.

PREDICTIVE ANALYTICS

Learning models are developed to trail and forecast various environmental effects on crop yield such as weather changes. For this, ML algorithms account for a significant role. ML algorithms in association with the satellites investigate crop sustainability, predict the weather, and assess farms to know about the existence of pests and diseases. ML models are exceptionally good at delivering high standard data or information that is perpetually updated at a quick rate. The data sources such as precipitation, wind speed, solar radiation, and temperature along with historical values are important for predictive analysis. The obtained analysis accounts for an important role for adequate scheduling and crop selection for particular agricultural land (Imran, Ahmad, & Kim, 2020).

Table 4-1 Sensors and Types of Measures considered by the Respective Sensors

Sr. no.	Type of sensor	Measurement
1	Temperature sensor	Soil temperature Noncontact shell temperature
2	Moisture sensor	Soil wetness Conductivity Volumetric water content Water potential
3	Solar radiation	Active radiation UV radiation Solar-shortwave
4	Weather	Rainfall Warmth Moisture Air pressure Speed of wind Flow direction of wind
5	NPK soil sensors	Nitrogen level Phosphorous level Potassium level pH level Temperature level Moisture level

Source: Adapted from Table 1, p3 in (Kumar, Rawat, Mohd, & Husain, 2021)

INTELLIGENT AI AND AGRICULTURE INTERSECTION

In Section III of (Nichols R. K., et al., 2022) our Hope was to improve the global food supply by as much as 1-2%.[18] Dr Zheng in his book (Zheng, 2023) focuses on five areas of research and presents case studies. These are:

1. AI – and its role in agriculture and its potential to feed the world,
2. Agriculture Technology,
3. Intelligent Technologies,
4. Food Security, and
5. Sustainability.

Agriculture is a critical industry that plays a vital role in ensuring food security and sustainability. The agriculture sector faces numerous challenges such as climate change, limited resources, and growing demand for food. Artificial intelligence (AI) has emerged as a promising tool to address these challenges by providing intelligent solutions to optimize agricultural practices. (Zheng, 2023)

Dr Zheng states that "machine learning techniques have numerous applications in agriculture, including:" (Zheng, 2023)

Crop-yield prediction: ML algorithms can analyze historical weather data, soil moisture levels and content, to predict crop yields and optimize inputs.

Pest Management: ML can be used to develop predicative models for pest outbreaks, enabling farmers to take preventive measures before damage occurs.

Soil Analysis: ML algorithms analyze the soil samples, identify nutrient deficiencies, and recommend fertilization strategies.

Livestock Monitoring: ML algorithms can monitor animal behavior and health data, allowing farmers to detect early signs of disease or distress. ML is also used in monitoring global migration patterns.

BIO-THREATS TO AGRICULTURE FROM SPACE [19]

For every good there is an opposing evil. The first sections addressed the good side of IA technology to improve crop yields and to endure the Hope of our team to feed the global population. But there is evil too in the form of Bio-Threats to the planet's agricultural resources. These must be addressed and the threats they provide must be countered.

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. (Nichols R. K., et al., 2022) (Nichols, et al., 2021) Similarly, research reports, papers, and special government studies have been completed detailing *effective plant-advanced bioterrorism countermeasures*. These are CLASSIFIED and not OSI.

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,**[20]** a subset of bioterrorism.* [21] (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 for farmers and disease specialists. We have seen (supra) that these can be addressed using AI and sensors.

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. (S. Sincavage, 2022)

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 charts about Agriculture and Zoonotic Bioterrorism. *Figures 4-11 to 4-18 portray the threats that must be considered in every risk assessment to develop detection, mitigation, and recovery countermeasures*. (Nichols, et al., 2021) (S. Sincavage, 2022)

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) (S. Sincavage, 2022)

Developing a consensus for a list of the major bioterrorist threats and action items is 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. 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

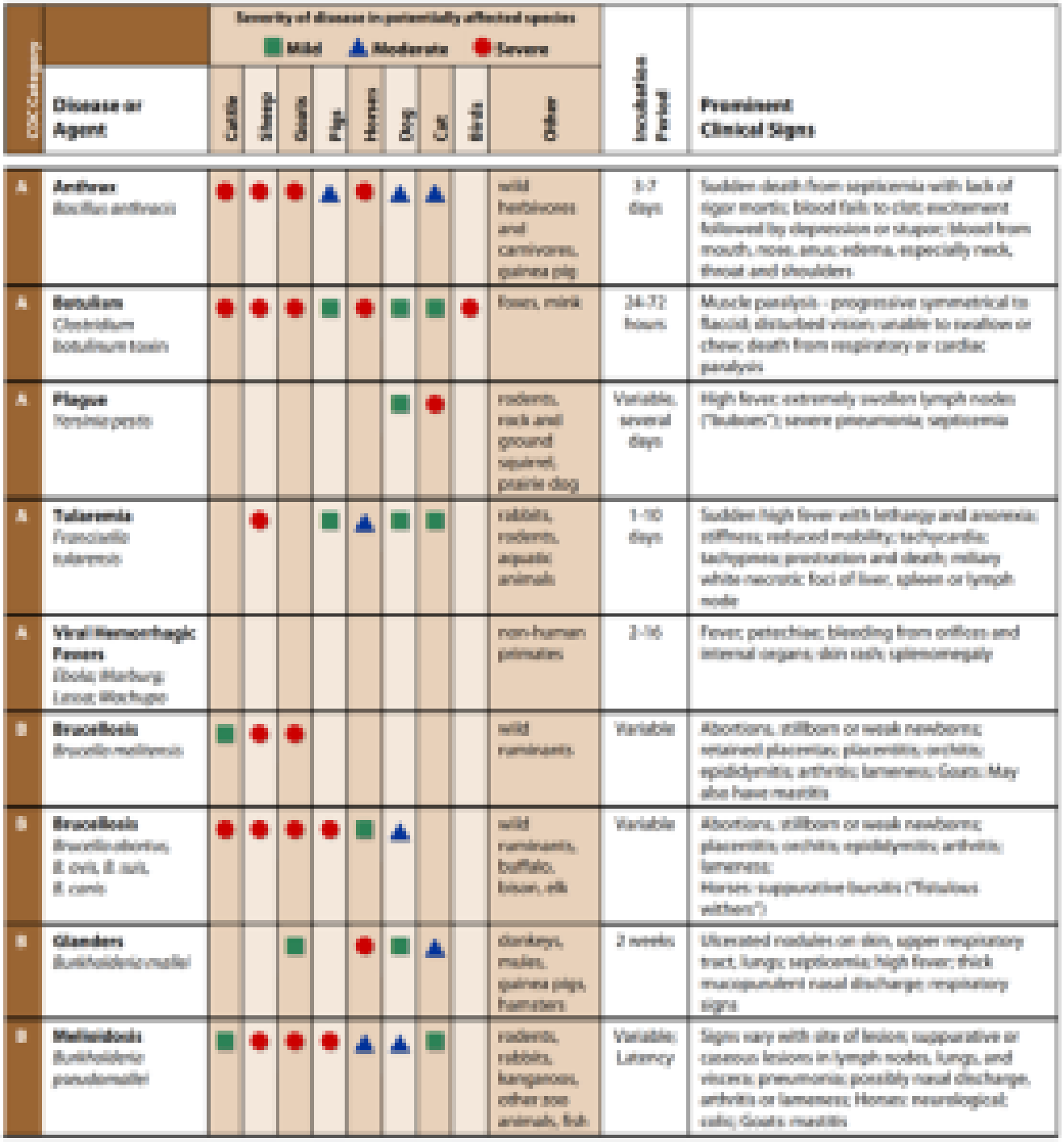
large amounts to be disseminated to cause mass casualties. The only way to cause mass damage is to use a respirable aerosol. This is also a danger to the perpetrators. (Howard, 2013) (Nichols & Carter, 2022) (S. Sincavage, 2022)

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 manage the causative organisms without risk of infection. There is no need for vaccination, special precautions, or prophylactic antibiotic use. (Howard, 2013) (Nichols & Carter, 2022) (S. Sincavage, 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)

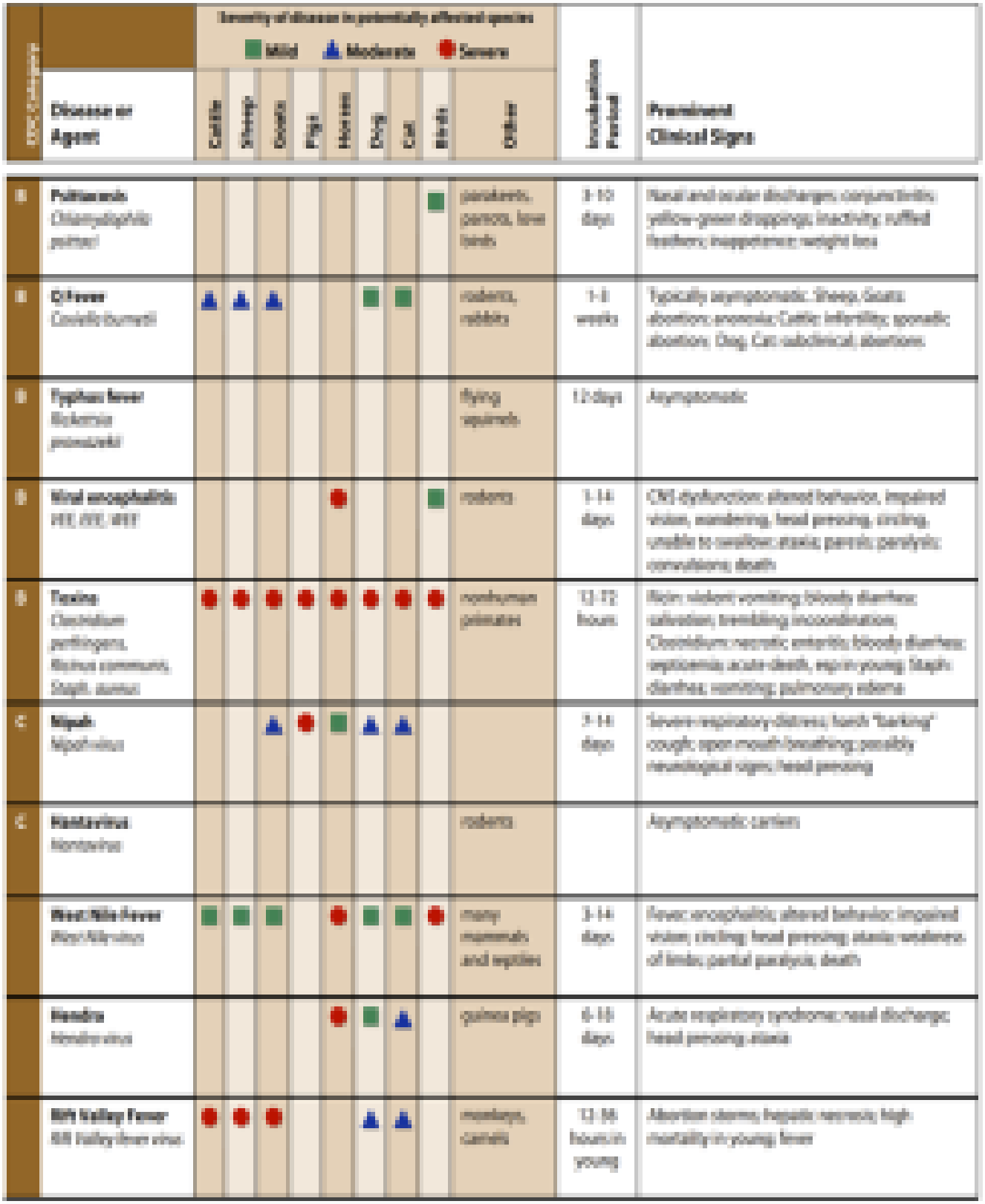
Figure 4-11 Animal Disease From Potential Bioterrorist Agents I



Biocategory	Disease or Agent	Severity of disease in potentially affected species: ■ Mild ▲ Moderate ● Severe									Incubation Period	Prominent Clinical Signs
		Cattle	Sheep	Goats	Pigs	Horses	Dog	Cat	Birds	Other		
A	**Anthrax** *Bacillus anthracis*	●	●	●	▲	●	▲	▲		wild herbivores and carnivores, guinea pig	1-7 days	Sudden death from septicemia with lack of rigor mortis; blood fails to clot; excitement followed by depression or stupor; blood from mouth, nose, anus; edema, especially neck, throat and shoulders
A	**Botulism** *Clostridium botulinum* toxin	●	●	●	■	●	■	■	●	foxes, mink	24-72 hours	Muscle paralysis - progressive symmetrical to flaccid; disturbed vision; unable to swallow or chew; death from respiratory or cardiac paralysis
A	**Plague** *Yersinia pestis*						■	●		rodents, rock and ground squirrel, prairie dog	Variable, several days	High fever; extremely swollen lymph nodes ("buboes"); severe pneumonia; septicemia
A	**Tularemia** *Francisella tularensis*		●		■	▲	■	■		rabbits, rodents, aquatic animals	1-10 days	Sudden high fever with lethargy and anorexia; stiffness; reduced mobility; tachycardia; tachypnea; prostration and death; miliary white necrotic foci of liver, spleen or lymph node
A	**Viral Hemorrhagic Fevers** *Ebola; Marburg; Lassa; Machupo*									non-human primates	2-16	Fever; petechiae; bleeding from orifices and internal organs; skin rash; splenomegaly
B	**Brucellosis** *Brucella melitensis*	■	●	●						wild ruminants	Variable	Abortions, stillborn or weak newborns; retained placentas; placentitis, orchitis; epididymitis; arthritis; lameness. Goats: May also have mastitis
B	**Brucellosis** *Brucella abortus, B. ovis, B. suis, B. canis*	●	●	●	●	■	▲			wild ruminants, buffalo, bison, elk	Variable	Abortions, stillborn or weak newborns; placentitis, orchitis; epididymitis; arthritis; lameness; Horses: suppurative bursitis ("fistulous withers")
B	**Glanders** *Burkholderia mallei*			■		●	■	▲		donkeys, mules, guinea pigs, hamsters	2 weeks	Ulcerated nodules on skin, upper respiratory tract, lungs; septicemia; high fever; thick mucopurulent nasal discharge; respiratory signs
B	**Melioidosis** *Burkholderia pseudomallei*	■	●	●	●	▲	▲	■		rodents, rabbits, kangaroos, other zoo animals, fish	Variable; Latency	Signs vary with site of lesion; suppurative or caseous lesions in lymph nodes, lungs, and viscera; pneumonia; possibly nasal discharge, arthritis or lameness; Horses: neurological; cats; Goats: mastitis

Source: (APHIS & USDA, 2022)

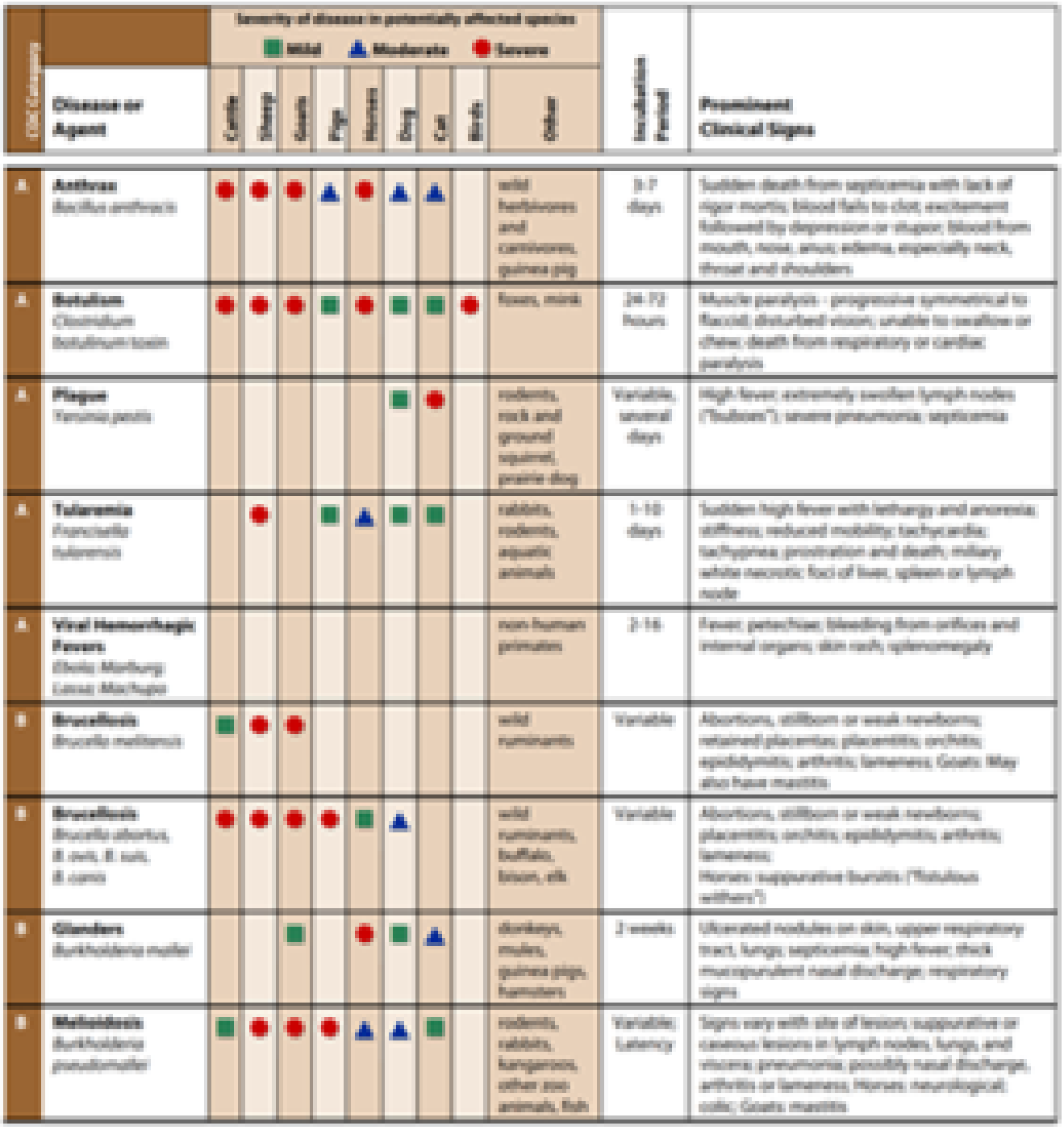
Figure 4-12 Animal Disease From Potential Bioterrorist Agents II



Risk Category	Disease or Agent	Severity of disease in potentially affected species: Mild / Moderate / Severe — Cattle	Sheep	Goats	Pigs	Horses	Dog	Cat	Birds	Other	Incubation Period	Prominent Clinical Signs
II	**Psittacosis** *Chlamydophila psittaci*								■	parakeets, parrots, love birds	3-10 days	Nasal and ocular discharges; conjunctivitis; yellow-green droppings; inactivity; ruffled feathers; inappetence; weight loss
II	**Q Fever** *Coxiella burnetii*	▲	▲	▲			■	■		rodents, rabbits	1-3 weeks	Typically asymptomatic. Sheep, Goats: abortion; anemia. Cattle: infertility; sporadic abortion. Dog, Cat: subclinical; abortions
II	**Typhus fever** *Rickettsia prowazekii*									flying squirrels	12 days	Asymptomatic
II	**Viral encephalitis** *VEE, EEE, WEE*					●			■	rodents	1-14 days	CNS dysfunction; altered behavior, impaired vision, wandering, head pressing, circling, unable to swallow; ataxia; paresis; paralysis; convulsions; death
III	**Tetanus** *Clostridium perfringens, Ricinus communis, Staph. aureus*	●	●	●	●	●	●	●	●	nonhuman primates	12-72 hours	Rizin: violent vomiting, bloody diarrhea; salivation; trembling; incoordination; Clostridium: necrotic enteritis; bloody diarrhea; septicemia; acute death, esp in young; Staph: diarrhea, vomiting, pulmonary edema
IV	**Nipah** *Nipah virus*			▲	●	■	▲	▲			3-14 days	Severe respiratory distress; harsh "barking" cough; open mouth breathing; possibly neurological signs; head pressing
IV	**Hantavirus** *Hantavirus*									rodents		Asymptomatic carriers
	West Nile Fever *West Nile virus*	■	■	■		●	■	■	●	many mammals and reptiles	3-14 days	Fever; encephalitis; altered behavior; impaired vision; circling; head pressing; ataxia; weakness of limbs; partial paralysis; death
	Hendra *Hendra virus*					●	■	▲		guinea pigs	6-15 days	Acute respiratory syndrome; nasal discharge; head pressing; ataxia
	Rift Valley Fever *Rift Valley fever virus*	●	●	●			▲	▲		monkeys, camels	12-36 hours in young	Abortion storms; hepatic necrosis; high mortality in young; fever

Source: (APHIS & USDA, 2022)

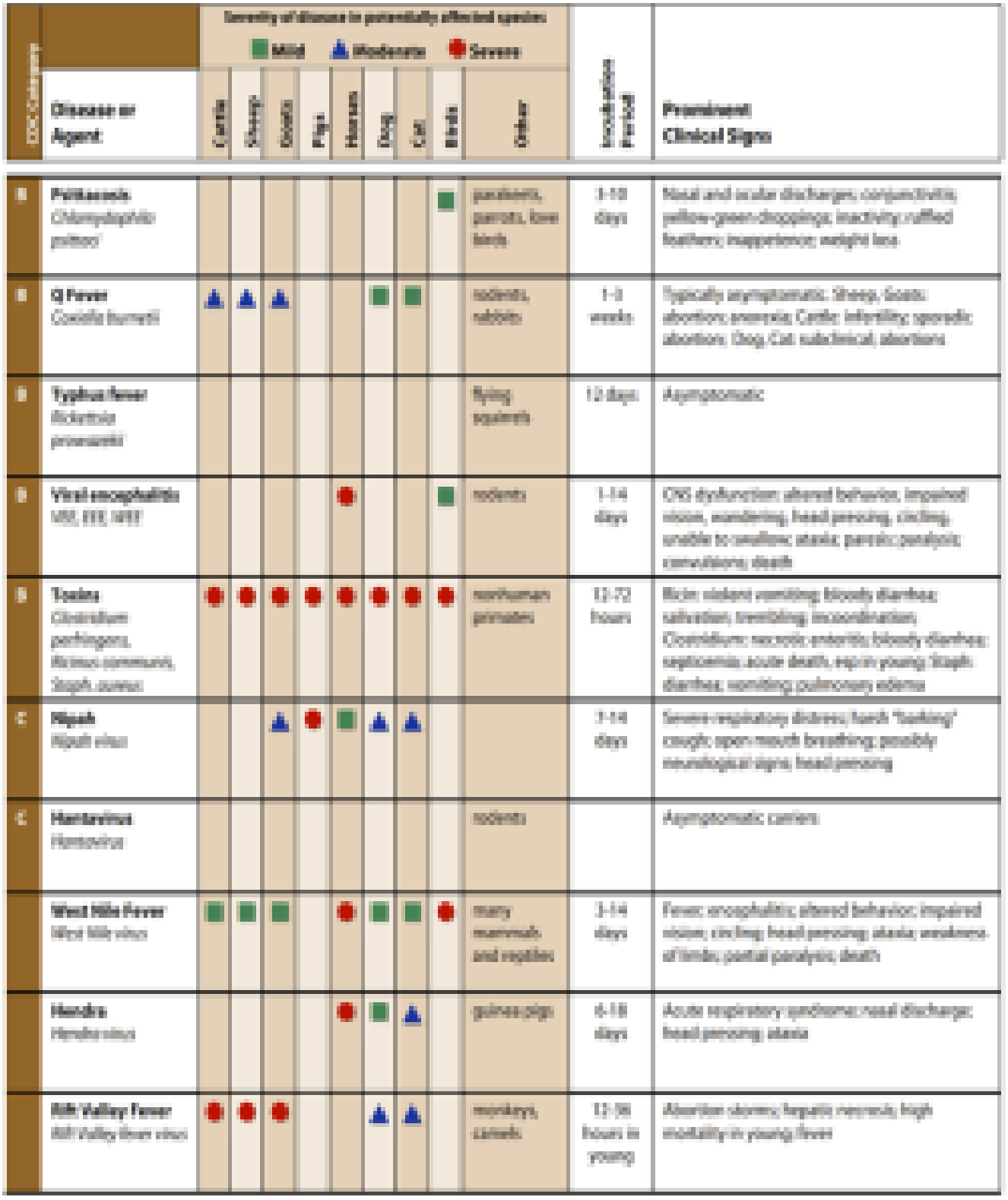
Figure 4-13 Human Disease From Potential from Bioterrorist Agents I



CDC Category	Disease or Agent	Severity of disease in potentially affected species: Mild / Moderate / Severe — Cattle	Sheep	Goats	Pigs	Horses	Dogs	Cat	Birds	Other	Incubation Period	Prominent Clinical Signs
A	**Anthrax** *Bacillus anthracis*	●	●	●	▲	●	▲	▲		wild herbivores and carnivores, guinea pig	1-7 days	Sudden death from septicemia with lack of rigor mortis, blood fails to clot; excitement followed by depression or stupor; blood from mouth, nose, anus; edema, especially neck, throat and shoulders
A	**Botulism** *Clostridium botulinum* toxin	●	●	●	■	●	■	■	●	foxes, mink	24-72 hours	Muscle paralysis - progressive symmetrical to flaccid; disturbed vision; unable to swallow or chew; death from respiratory or cardiac paralysis
A	**Plague** *Yersinia pestis*						■	●		rodents, rock and ground squirrel, prairie dog	Variable, several days	High fever; extremely swollen lymph nodes ("buboes"); severe pneumonia; septicemia
A	**Tularemia** *Francisella tularensis*		●		■	▲	■	■		rabbits, rodents, aquatic animals	1-10 days	Sudden high fever with lethargy and anorexia; stiffness; reduced mobility; tachycardia; tachypnea; prostration and death; miliary white necrotic foci of liver, spleen or lymph node
A	**Viral Hemorrhagic Fevers** *Ebola; Marburg; Lassa; Machupo*									non-human primates	2-16	Fever; petechiae; bleeding from orifices and internal organs; skin rash; splenomegaly
B	**Brucellosis** *Brucella melitensis*	■	●	●						wild ruminants	Variable	Abortions, stillborn or weak newborns; retained placentas; placentitis; orchitis; epididymitis; arthritis; lameness. Goats: May also have mastitis
B	**Brucellosis** *Brucella abortus, B. suis, B. canis*	●	●	●	●	■	▲			wild ruminants, buffalo, bison, elk	Variable	Abortions, stillborn or weak newborns; placentitis; orchitis; epididymitis; arthritis; lameness; Horses: suppurative bursitis ("fistulous withers")
B	**Glanders** *Burkholderia mallei*			■		●	■	▲		donkeys, mules, guinea pigs, hamsters	2 weeks	Ulcerated nodules on skin, upper respiratory tract, lungs; septicemia; high fever; thick mucopurulent nasal discharge; respiratory signs
B	**Melioidosis** *Burkholderia pseudomallei*	■	●	●	●	▲	▲	■		rodents, rabbits, kangaroos, other zoo animals, fish	Variable; Latency	Signs vary with site of lesion; suppurative or caseous lesions in lymph nodes, lungs, and viscera; pneumonia, possibly nasal discharge, arthritis or lameness; Horses: neurological; colic; Goats: mastitis

Source: (APHIS & USDA, 2022)

Figure 4-14 Human Disease From Potential from Bioterrorist Agents II



Source: (APHIS & USDA, 2022)

Figure 4-15 USDA High Consequence Foreign Animal Diseases and Pests I

Disease or Agent	Humans Affected	Species Affected	Incubation Period	Mode of Transmission	Prominent Clinical Signs in Animals
Tier 1: Diseases of national concern that pose the most significant threat (highest risk and consequence) to animal agriculture in the U.S.					
African swine fever virus	No	domestic and wild pigs	5-15 days	direct contact with body fluids (blood); contaminated objects; ticks	High fever; recumbency; skin reddening; cyanotic blotching on ear, tail or legs; enlarged friable spleen; hemorrhagic lymph nodes; swollen tonsils; petechiae; fibrinous pericarditis; death
Classical swine fever virus (hog cholera)	No	pigs	2-14 days	ingestion (uncooked meat); contaminated objects; aerosol; direct contact	Variable. Fever, dullness; ataxia; constipation followed by diarrhea; cyanosis of abdomen and ears; abortions, stillbirths, mummification, congenital malformations; death
Foot-and-mouth disease virus	Rare	cattle, sheep, goats, pigs	1-8 days	aerosol; direct contact; ingestion; contaminated objects	Fever, vesicles and erosions in mouth, nares, muzzle, and feet (coronary band, interdigital or teats); depression, anorexia; salivation, nasal discharge; sloughing of hoof; abortion
Avian influenza virus (highly pathogenic)	Yes	chicken, turkey, pigs, waterfowl, cats, dogs	3-7 days	aerosol; direct contact with body fluids; ingestion; contaminated objects	Depression; respiratory signs (coughing, sneezing, nasal discharge); ataxia, green watery diarrhea, swollen, cyanotic combs and wattles; edema of eyes and neck; hemorrhage of legs, decreased egg production, death.
Newcastle disease virus (virulent)	Yes	poultry, other avian species	2-15 days	direct contact with feces and respiratory droplets; fomites,	Respiratory signs (coughing, gasping); neurological signs (muscle tremors, circling, paralysis), green watery diarrhea, decreased egg production
Tier 2: Diseases transmitted primarily by pests; disease spread depends largely on the presence of pests in the environment and ability to disease between animals					
Heartwater (Ehrlichia (Cowdria) ruminantium	No	cattle, sheep, goats, wild ruminants	7-16 days	Amblyomma ticks	Fever, respiratory distress, lacrimation, neurologic signs (tongue protrusion, circling, high stepping gait); convulsions, death. Post mortem lesions: hydropericardium, ascites, hydrothorax, petechiae
New World Screwworm (Cochliomyia hominivorax	Yes	mammals, birds	5-7 days	eggs laid in wounds	Variable diameter openings containing migrating larvae; death can occur from toxicity or secondary infections
Rift Valley fever	Yes	cattle, sheep, goats, dogs, cats, camels	12-36 hours in young	mosquitoes; other insects, ticks; in utero; direct contact with infected tissues or aerosol	High mortality in newborn animals; fever, hemorrhagic diarrhea, abdominal pain, bloody nasal discharge; abortion storms in adults
Venezuelan equine encephalitis	Yes	horses, wild rodents, wild birds	1-6 days	mosquitoes	Fever; tachycardia; neurological signs indicative of encephalitis (altered behavior, hypersensitivity, involuntary muscle movement, impaired vision, paresis, paralysis, convulsions); death; disease can be mild or asymptomatic

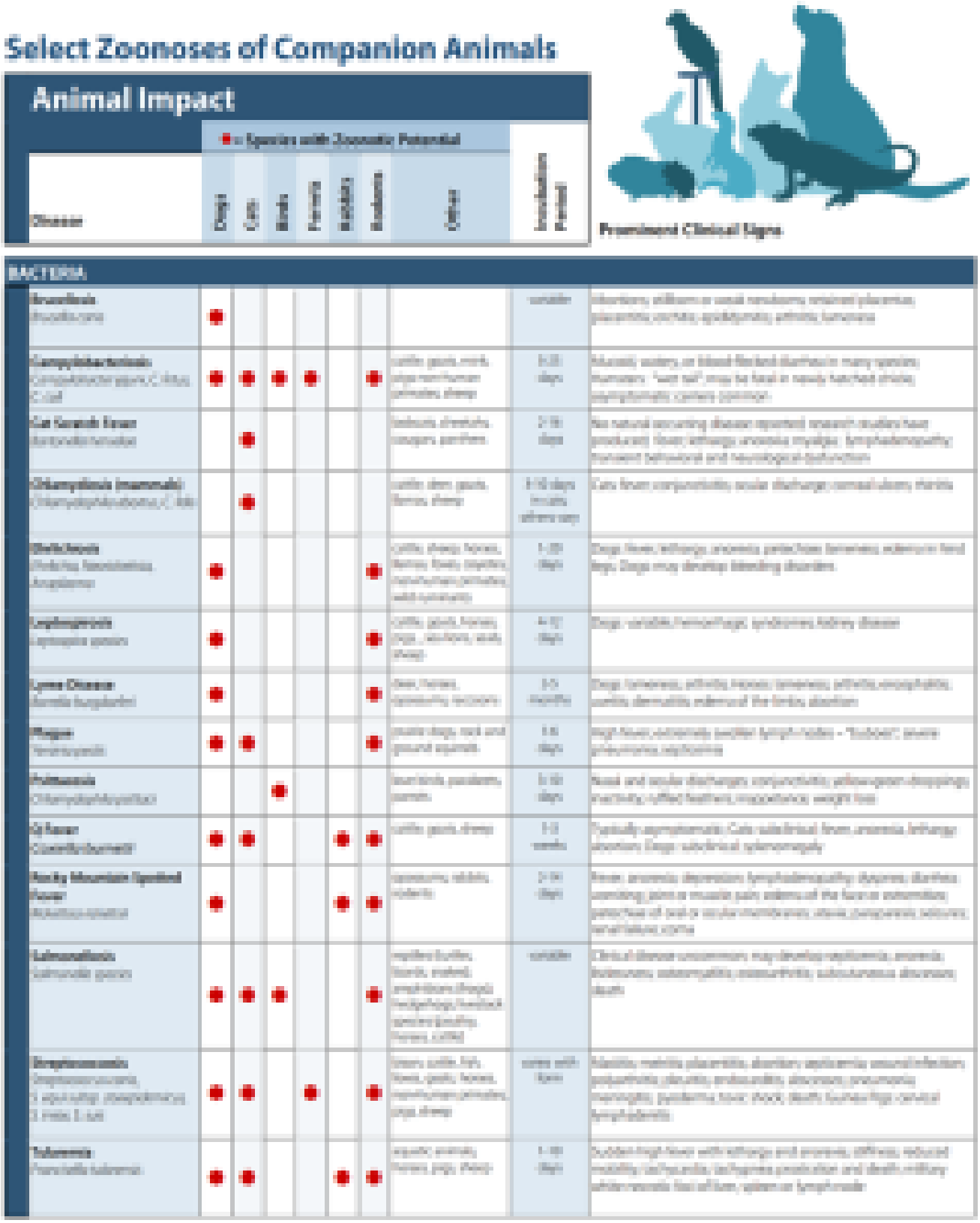
Source: (APHIS & USDA, 2022)

Figure 4-16 USDA High Consequence Foreign Animal Diseases and Pests II

Disease or Agent	Humans Affected	Species Affected	Incubation Period	Mode of Transmission	Prominent Clinical Signs in Animals
Tier 3: Diseases and pests that pose less risk and fewer consequences but still have potential negative impact on animal or human health					
African horse sickness virus	No	horses, zebras, donkeys, mules, camels	5-7 days	Culicoides midges, mechanically by other vectors	Variable forms; fever; severe dyspnea; spasmodic cough; serosanguinous nasal discharge; edema of supraorbital fossa, head, neck, and chest; profuse sweating; hydrothorax; hydropericardium
Contagious bovine pleuropneumonia *Mycoplasma mycoides mycoides*	No	cattle	30-121 days	close contact with respiratory droplets and other body fluids	Dyspnea, tachypnea, cough, fever; calves may have polyarthritis with or without pneumonia. Post mortem lesions: fibrinous, thickened, hyperemic "marbled" lung tissue; thickened interlobular septa
Contagious caprine pleuropneumonia *Mycoplasma capricolum M.F38/ M. mycoides capri*	No	goats	6-10 days	direct contact with respiratory droplets	Respiratory signs (coughing, labored respiration, frothy nasal discharge); fever; septicemia, lethargy; anorexia; death. Post mortem lesions: fibrinous pneumonia, no thickening of interlobular tissue
Glanders *Burkholderia mallei*	Yes	horses, dogs, goats, cats	14 days	direct contact, fomites, inhalation, ingestion, reproductive	Ulcerated nodules on skin, upper respiratory tract, lungs; septicemia; high fever; thick mucopurulent nasal discharge; respiratory signs
Hendra virus	Yes	horses, cats, dogs	6-18 days	ingestion, inhalation, close contact; fomites	Acute respiratory syndrome; nasal discharge; head pressing; ataxia
Melioidosis *Burkholderia pseudomallei*	Yes	sheep, goats, pigs, horses, dogs, cattle, cats	Variable latency	ingestion, inhalation, entry through wounds or abrasions	Signs vary with site of lesion; suppurative or caseous lesions in lymph nodes, lungs, and viscera; pneumonia; possibly nasal discharge, arthritis or lameness; Horses: neurological cells; Goats: mastitis
Nipah virus	Yes	pigs, goats, dogs, cats, horses	7-14 days	aerosol, direct contact with respiratory secretions	Severe respiratory distress; harsh "barking" cough; open mouth breathing; possibly neurological signs; head pressing
Peste des petits ruminants virus	No	goats, sheep	3-10 days	close contact with body fluids; aerosol; contaminated objects	Sudden death; fever; nasal discharge; respiratory distress; bronchopneumonia; necrotic stomatitis; diarrhea; death
Rinderpest virus	No	cattle, sheep, goats, pigs	3-15 days	direct or close contact with body fluids	High fever; tachypnea; tachycardia; oculonasal discharge; oral erosions and necrosis; watery to hemorrhagic diarrhea; abdominal pain; weakness; recumbency; sudden death
Tropical bont tick *Amblyomma variegatum*	Yes	cattle, sheep, goats, horses, dogs		direct contact (bite) of tick	Large wounds can damage skin and secondary infections; can transmit agents for heartwater and African tick-bite fever

Source: (APHIS & USDA, 2022)

Figure 4-17 Selected Zoonoses of Companion Animals I



Source: (CFSPH, 2022)

Figure 4-18 Selected Zoonoses of Companion Animals II

Source: (CFSPH, 2022)

MONITORING OF PLANT PATHOGENS

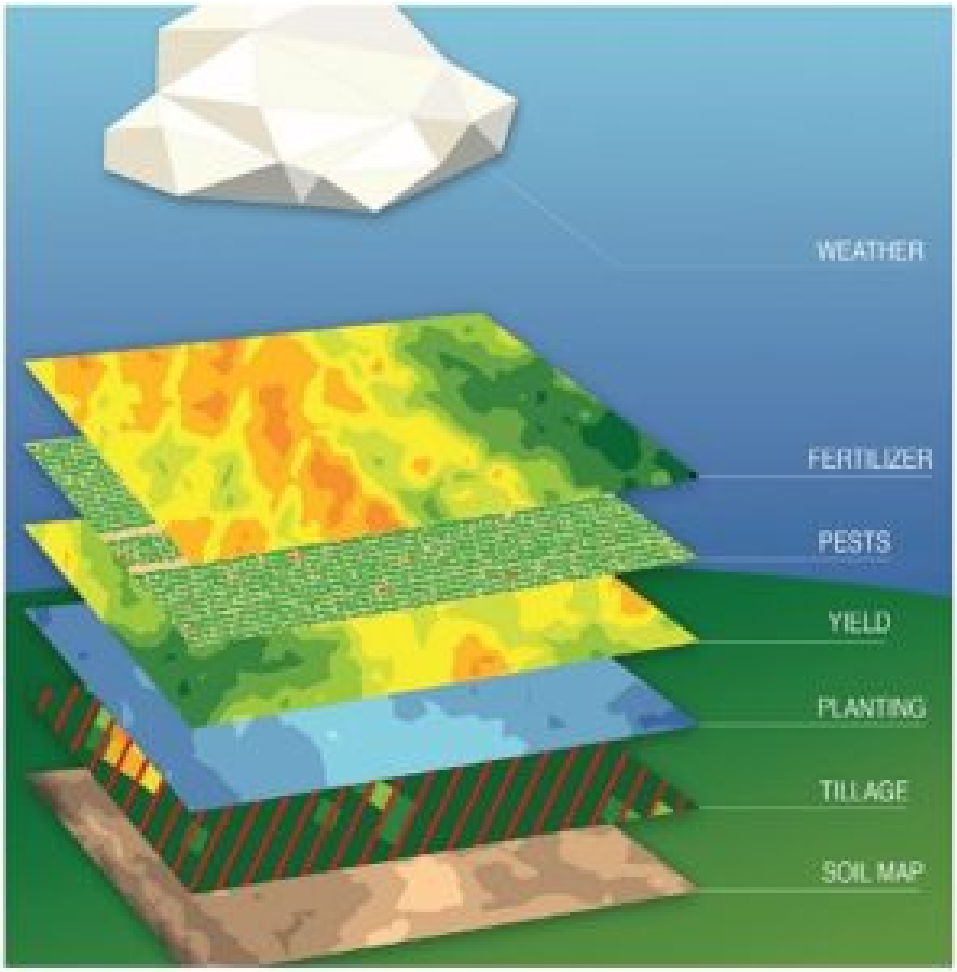
What is needed?

Answer: A real-time monitoring and communication of abnormalities within livestock and crops using satellite technology. Figure 4-19 shows the operating and planned NASA Earth Fleet through 2023. The Landsat series is particularly useful for agricultural bioterrorism studies. (NASA, 2021)

Figure 4-19 NASA Earth Fleet

Source: (NASA, 2021)

Figure 4-20 Layers of Agriculture Investigation



Source: (NASA, 2021)

Figure 4-20 shows the agriculture density map where satellites must penetrate with MASINT [22]sensors. (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 remarkably 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

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) (S. Sincavage, 2022) details satellite imaging techniques monitoring of invasive plants.

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 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, resistant to current herbicides. The superweed was 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

Global agriculture / farming are converting to using AI. This translates directly into the global food growth, production and delivery to consumers. The food industry is using the basic level of artificial intelligence. Every day the role of AI is becoming vital due to its capability to escalate hygiene, food protection, and waste management system. AI is going to transform the food processing industry because it has so much potential to generate reasonable and healthier productivity for clients and employees. Employment of AI and ML in food production and eatery businesses is already taking business to a new level by minimizing human mistakes in manufacturing. AI enables low costs for packing as well as conveyance, increment in customer pleasing, rapid services, voice searching, and more personalized orders. The impact of AI in this sector is global.

However, 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.[23] 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.[24]

REFERENCES

87-of-us-agriculture-businesses-are-currently-using-ai. (2021, December 12). Retrieved from www.agrinews-pubs.com/: https://www.agrinews-pubs.com/news/science/2021/12/07/87-of-us-agriculture-businesses-are-currently-using-ai/

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

Allied Market Research. (2023, March). *internet-of-things-iot-in-agriculture-market.* Retrieved from www.alliedmarketresearch.com/: https://www.alliedmarketresearch.com/internet-of-things-iot-in-agriculture-market

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.

Bhattacharyya, S., Sarkar, P., Sarkar, S., Sinha, A., & Chanda, &. S. (2020). Prototype model for controlling of soil moisture and ph. in smart farming system. *Computational Advancement in Communication Circuits and Systems*, pp. pp. 405–411, Springer.

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

Columbus, L. (2021, Feburary 17). *10-ways-ai-has-the-potential-to-improve-agriculture-in-2021.* Retrieved from www.forbes.com/: https://www.forbes.com/sites/louiscolumbus/2021/02/17/10-ways-ai-has-the-potential-to-improve-agriculture-in-2021/?sh=15d08c507f3b

Definition of Artificial Intelligence . (2023). https://www.merriam-webster.com/dictionary/artificial%20intelligence.

Dictionary.com. (2023, 6 27). *Sagacity Definition.* Retrieved from www.dictionary.com: www.dictionary.com

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

escoffier.edu. (2023). *9 Ways Artificial Intelligence is Changing the Food Industry.* Retrieved from www.escoffier.edu: https://www.escoffier.edu/blog/world-food-drink/how-artificial-intelligence-is-changing-the-food-industry/

Fedorova, E., Darbasov, V., & Okhlopkov, &. M. (2020). The role of agricultural economists in study on problems related to regional food safety. *E3S Web of Conferences*, pp. vol. 176, p. 5011.

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.

Imran, S., Ahmad, S., & Kim, &. D. (2020). Quantum GIS based descriptive and predictive data analysis for effective planning of waste management. *IEEE Access*, pp. vol. 8, pp. 46193–46205.

Integrate UAV Technology with Yield Maps. (2023). Retrieved from www.petersonfarmsseed.com: https://www.petersonfarmsseed.com/3352-2/

Kumar, I., Rawat, J., Mohd, N., & Husain, &. S. (2021, July 12). *Opportunities of Artificial Intelligence and Machine Learning in the Food Industry.* Retrieved from https://www.hindawi.com/journals/: https://www.hindawi.com/journals/jfq/2021/4535567/

Larson, H. (2022). Humanitarian Use of Space Technologies to Improve Global Food Supply & Cattle Management. In R. K. Nichols, C. M. Carter, J.-P. Hood, M. J. Jackson, S. M. Joseph, H. Larson, . . . Sincavage, *SPACE SYSTEMS: EMERGING TECHNOLOGIES AND OPERATIONS* (pp. 545-589). Manhattan, KS: NPP eBooks. 47.

Machleb, J., Peteinatos, G. G., Kollenda, B. L., And´ujar, D., & Gerhards, &. R. (2020). Sensor-based mechanical weed control: present state and prospects. pp. vol. 176, Article ID 105638.

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

Mumm, H. C. (2022). Drones and Precision Agricultural Mapping. In R. K. Nichols, C. M. Carter, J.-P. Hood, M. J. Jackson, S. M. Joseph, H. Larson, . . . Sincavage, *Space Systems: Emerging Technologies and Operations* (pp. 472-507). Manhattan, KS: NPP eBooks. 47.

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. (2002). *Wireless security : models, threats, and solutions* .

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

Nichols, R. K. (2022). Section 3.0 Cyber Risk Assessments – Ryan-Nichols Equations.

Nichols, R. K., Carter, C. M., Hood, J.-P., Jackson, M. J., Joseph, S. M., Larson, H., . . . S. (2022). *Space Systems: Emerging Technologies and Operations (2022).* Manhattan, KS: https://newprairiepress.org/ebooks/47/.

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

Payne, J. (2021, Sep 28). *artificial-intelligence-in-food-industry.* Retrieved from https://www.aptean.com/: https://www.aptean.com/en-US/insights/blog/artificial-intelligence-in-food-industry

Raut, R., Varma, H., Mulla, C., & Pawar, &. V. (2018). "Soil monitoring, fertigation, and irrigation system using IoT for agricultural application. *Intelligent Communication and Computational Technologies*, pp. pp. 67–73, Springer, Singapore.

Ryan, J. J. (2022). Civilian use of Space for Environmental, Wildlife Tracking, & Fire Risk Zone ID. In R. K. Nichols, C. M. Carter, J.-P. Hood, M. J. Jackson, S. M. Joseph, H. Larson, . . . Sincavage, *Space Systems: Emerging Technologies and Operations* (pp. 508-544). Manhattan, KS: https://newprairiepress.org/ebooks/47/.

Sincavage, C. C. (2022). Bio-threats to Agriculture-Solutions from Space. In R. K. Nichols, C. M. Carter, J.-P. Hood, M. J. Jackson, S. M. Joseph, H. Larson, . . . Sincavage, *Space Systems: Emerging Technologies and Operations* (pp. 408-431). Manhattan, KS: NPP eBooks #47.

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.

Strange, R. (1993). *Plant Disease Control.* London: Chapman and Hall.

Teske A. L., G. C. (2019). Optimized dispensing of predatory mites by multirotor UAVs in wind: a distribution pattern modelling approach for precision pest management. . *Biosyst. Eng.* , pp. 187: 226–238. Retrieved from Teske A. L., G. Chen, C. Nansen, and Z. Kong. 2019. Optimized dispensing of predatory mites by multirotor UAVs in wind: a distribution pattern modelling approach for precision pest management. Biosyst. Eng. 187: 226–238.

Top 5 2023 Agriculture Trends to Watch. (2023). Retrieved from www.agmatix.com/: https://www.agmatix.com/blog/top-5-2023-agriculture-trends-to-watch/

University of Nottingham SOCIP. (2016, 9 13). *artificially-intelligent-food-gbp100m-year.* Retrieved from https://phys.org : https://phys.org › news › 2016-09-artificially-intelligent-food-gbp100m-year.pdf

University of Sydney. (2017). *Digital Farmland* . Retrieved from http://confluence.acfr.usyd.edu.au/display/AGPub/Our+Robots: http://confluence.acfr.usyd.edu.au/display/AGPub/Our+Robots

University of Sydney. (2022, 11 2). *Can-robots-and-ai-help-address-the-world-s-food-security-issues.* Retrieved from https://www.sydney.edu.au/news-opinion/: https://www.sydney.edu.au/news-opinion/news/2022/11/02/can-robots-and-ai-help-address-the-world-s-food-security-issues-.html

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

WIZATA. (2023). *how-the-food-industry-can-benefit-from-ai.* Retrieved from https://www.wizata.com/: https://www.wizata.com/knowledge-base/how-the-food-industry-can-benefit-from-ai

Yu, X., Lin, Y., & Wu, a. H. (2020). Targeted next-generation sequencing identifies separate causes of hearing loss in one deaf amily and variable clinical manifestations for the p.R161C Mutation in SOX10. *Neural Plasticity*, pp. vol. 2020, pp. 1–8,.

Zheng, M. (2023). *Artificial Intelligence and Agriculture: How Intelligent Technologies Can Help Feed the World.* Wuhan, China: zhengpublishing.com .

ENDNOTES

[1] Quote by Managing editor Prof. Randall K. Nichols, DTM.

[2] Think Robin Williams in the 1999 movie *Bicentennial Man*

[3] In the authors view, this is an extreme position by Dr. Zheng and the authors do not agree with the totality of the statement. However, they agree with effects of *naturally caused* disasters and *force majeure*. "Environmental footprints" is a tricky phrase. To the extent that man can provide sustainable practices involving naturally caused climate events, we concur. However, the current use of climate hysteria with penalties on the life sustaining element of carbon (or carbon credits) is a fraud and misuse of real scientific information for political purposes. We agree with Dr Zheng that this is a global concern because the hysteria has reached the level of almost political intrigue and power adjustment. For those who need further clarification and perhaps a change of view see: (Wrightstone, 2017) and the author's definitive position in: (R.K. Nichols, 2021)

[4] Author opinion.

[5] Louis Columbus's full article can be heard at: https://www.forbes.com/sites/louiscolumbus/2021/02/17/10-ways-ai-has-the-potential-to-improve-agriculture-in-2021/?sh=15d08c507f3b (voice)

[6] CAGR = compound annual growth rate

[7] Covered superbly by Dr Larson in (Larson, 2022)

[8] The author owns a small farm in Arkansas. Deer are the bane of our soybeans and wheat.

[9] Authors remarks at end based on SME experience. In one SCIF and TOC installation I managed, every door that was opened or closed gave alarms at 24/7. Considering the TOC and SCIF were part of a cybersecurity educational building with three specialized labs, and teaching facilities for about 800 students, the traffic hourly was beyond unreasonable to be watching nine screens. I can imagine watching empty fields at night using IR when 50 or so deer cross the acreage. Filtering the systems for time-based and animal-based temperature changes is required. ML systems can be trained to id people, vehicles, or animals.

[10] KSU has been pioneering / researching this discipline for a decade. They are the leader of the pack.

[11] KSU has installed multiple weather stations around the state to enhance drone research on agricultural mapping operations.

[12] Primarily for small farmers.

[13] "It's projected that APAC will need to increase food production by up to 77 percent to feed its communities by 2050. Bold steps must be taken to accelerate progress towards addressing the major drivers of food insecurity, malnutrition, and equal access to food – as well as drive smart solutions that give back power to local farmers," said Professor Sukkarieh. (University of Sydney, 2022)

[14] Author affiliations in order: Graphic Era Hill University, Dehradun, Uttarakhand, India, DIT University, Dehradun, Uttarakhand, India Graphic Era Deemed to be University, Dehradun, Uttarakhand, India, College of Engineering & Technology, Samara University, Semera, Ethiopia

[15] (Kumar, Rawat, Mohd, & Husain, 2021) has 53 excellent references backing up their research.

[16] NGS = Next generation sequencing – replaces DNA approach in the food security region.

[17] Sagacity- foresight, discernment, keen perception, to make good judgements (Dictionary.com, 2023)

[18] This would be a wonderful legacy for the author and the KSU Wildcat Team if even small part of the *Hope* and "word" got to the right decision-makers in every country. The world population is growing – big time. Lots of hungry families. WE would like to improve their lives.

[19] A decent portion of this section has been summarized from our own textbook Chapter 8" Bio-Threats

To Agriculture From Space- Solutions From Space (S. Sincavage, 2022). The managing editor deemed the material an excellent counterpoint to the positivity of the first two sections.

[20] 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)

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

[22] 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)

[23] Obviously, the US is not only country concerned about this threat. Other countries are addressing the bio-threats in valuable ways and if possible, intelligence should be shared to decrease the global risks. Countries sharing information unfortunately has limitations.

[24] Where there is Good, there is Evil.

5.

THE REALITY OF CYBORGS AND A LOOK INTO THE FUTURE [JOHNSON]

LEARNING OUTCOMES

1. The future of enhanced humans- explore the potential for our military, commercial and medical status.
2. Understand the practical side of enhancing human capabilities and merging with machines
3. Look into the future, explore a framework for humanities acceptance of Cyborgs/Enhanced Humans

An important scientific innovation rarely makes its way by gradually winning over and converting its opponents: it rarely happens that Saul becomes Paul. What does happen is that its opponents gradually die out, and that the growing generation is familiarized with the ideas from the beginning: another instance of the fact that the future lies with the youth.

Paraphrased as "Science progresses one funeral at a time".

— Max Planck (Planck, 1949)

WHAT IS A CYBORG?

The Merriam-Webster dictionary definition is "a bionic human" (Merriam-Webster, 2023) whereas the Britannica's expands the definition to "a person whose body contains mechanical or electrical devices and whose abilities are greater than the abilities of normal humans" (Britannica). The term is a popular theme in science fiction. Futurists are considering the theory and application. Modern science and medicine is well on its way to realizing the definitions and pop culture references of cyborg in modern society. At its most base comparison, a human with a prosthetics, by the definitions cited, could be (and in some cases, are) considered a cyborg.

This chapter will define what a cyborg is and how they are created, the current medical and scientific research into enhanced humans inclusive of those who already consider themselves cyborgs and what direction society is heading regarding human minds, bodies, and limbs whose enhanced abilities far outreach those who are not. Risks will be considered, narrowly focusing on risks to society and to the enhanced humans themselves.

The working definition of Cyborgs for this text will be Cyborgs are enhanced humans with increased capability resulting in increased human abilities.

This chapter complements chapter 12 later in this text. The student reader will understand enhanced human's potential to enable the future, understand the practical side of enhancing human capabilities and merging with machines creating a framework for humanities acceptance of Cyborgs/Enhanced Humans.

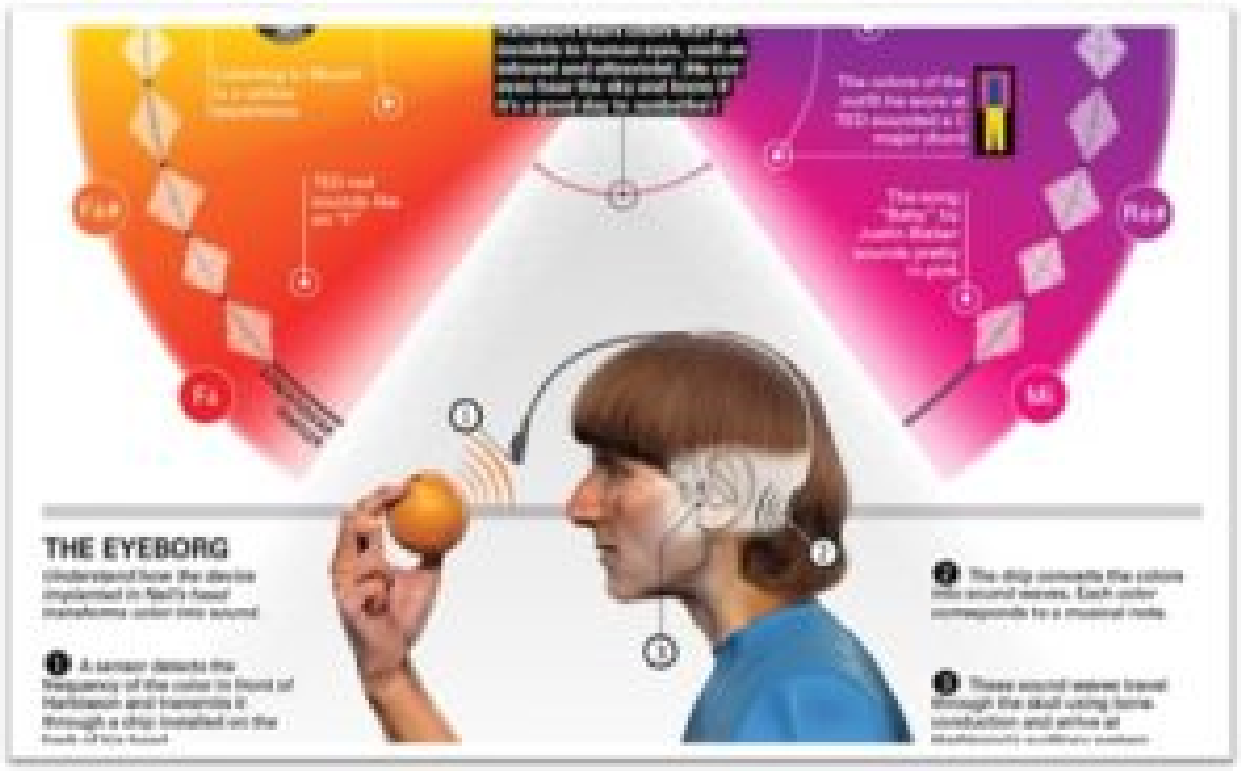
HOW ARE CYBORGS CREATED?

Increasing human capability through mechanical or electrical means resulting in improved biological, bio-mechanical or neurological human abilities. Mechanical means are inclusive of the range of prosthetics that allow veterans who've lost limbs sustained in combat the ability to walk, to grab items through the pioneering research at the Massachusetts Institute of Technology (MIT) in the field of Agonist-antagonist Myo-neural Interface (AMI), a method to restore proprioception to persons with amputation, or the ability of amputees to feel and have better control of their prosthetic limbs (MIT Media Lab). Physical implants like those of Amal Graafstra whose radio frequency ID chips implanted in his hands allowing him to start his motorcycle (Swain, 2014) and remotely open doors; and Rob Spence, who lost vision in his right eye, then implanted a tiny camera, producing a documentary about his life as a cyborgs (Swain, 2014). Future neurological advancements predict brains implanted with chips that are modified by DNA.

Medical and scientific research into prosthetics is the precursor to future advancement into cyborgs, cybernetics, and the human-machine interface. The field covers advancements in the medical, scientific, and commercial communities. The human-machine interface is inclusive of wearable technology to implanted technology. Three current examples of medical, scientific, and commercial cyborg creation are Dr Stephen Mann, who promotes wearable technology, Neil Harrison, a color-blind artist whose neurological implant allows him to hear sound, and Hugh Herr at MIT builds prosthetic knees, legs and ankles that fuse biomechanics with microprocessors to restore (and enhance) normal gait, balance, and speed.

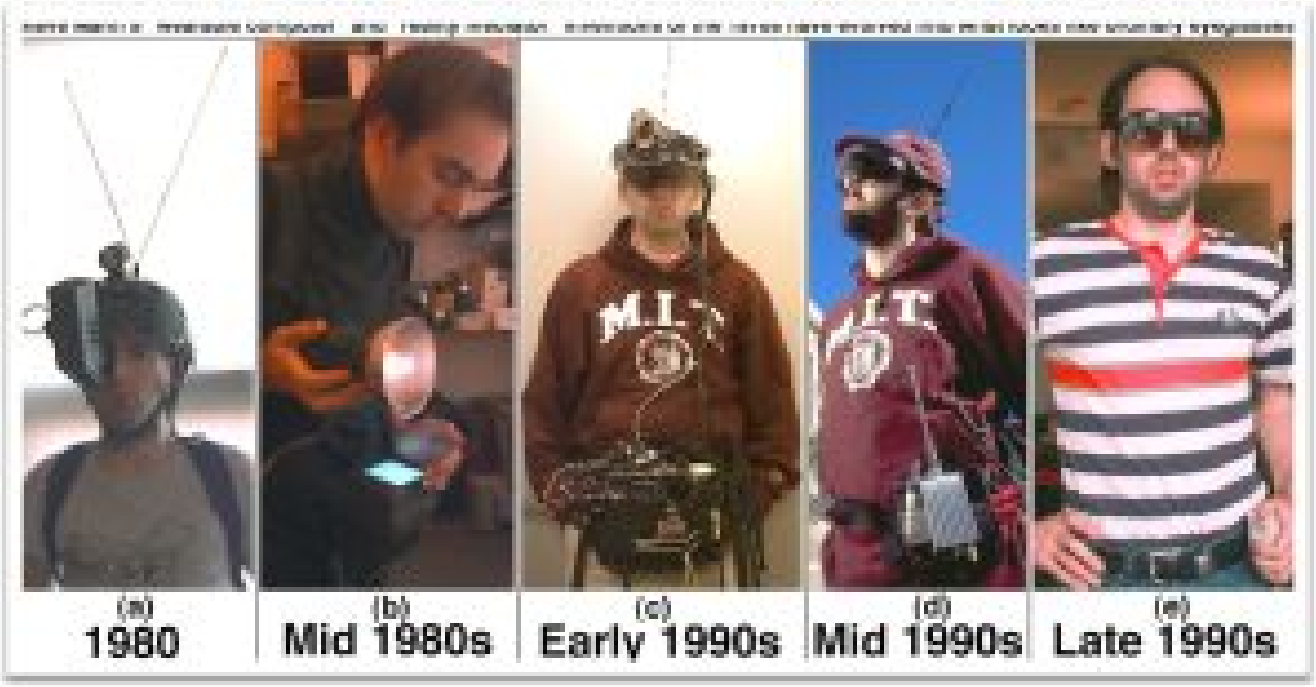
Stephen, Neil, and Hugh, and those cited above, chose their implants. They made the concise decision to fuse mechanical, electrical and computer technology into their human form, increasing their human capability. In his 2018 TED talk, Hugh Herr envisions that by the end of the 21st Century, nervous systems will be linked to exoskeletons, augmenting humans' strength, and power. He extrapolates this human augmentation into non-anthropomorphic structures such as wings, allowing humans the ability to fly (Herr, 2018).

Figure 5-1 Neil Harbisson, a color-blind artist whose neurological implant allows him to hear sound



Source: *(Walters, 2013)*

Figure 5-2 Steve Mann's wearable computer



Source: *(Case, 2013)*

This generates questions on the future legal and moral structure for human-machine modification. Who gets to approve modifications? When in the human growth cycle can (or should) modifications be made? Will modifications become genetic, or remain implants? Before reaching legal maturity, much less physical or mental maturity, where does the decision reside, with the parents or the individual? What will be the societal impacts? How much government oversight will there be regarding regulations and oversight? Much less religious and political ramifications.

HOW ARE MODIFICATIONS MADE?

Most of the progress in current medical and scientific technology is limited to surgical implants, and prosthetics. Other research and innovation include the world of wearable computing. Dr Mann considers himself a cyborg promoting a cyborg lifestyle. His experiments in wearable computing follows Moore's Law, from the late 1970's evolving from backpack computers through augmented reality eyeglasses of the 2020's (Case, 2013). Dr Mann's view includes "unlike other computers (including laptops and PDAs), a WearComp is inextricably intertwined with its wearer – WearComp's 'always ready' characteristic leads to a new form of synergy between human and computer" (Mann, 2012).

This coincides with research into robotics and computing, the fields of creating android, and human-like machines. The advances in Artificial Intelligence, machine learning, robotics, engineering, and nanotechnology all portend cross-over potential between robotics research and cyborg research. Machines and robots will eventually possess the capacity to learn. Artificial Intelligence's end state is to replicate human intelligence, to reason, discover meaning, to generalize, and perform (McCarthy, 2006). Machine Learning, a sub-field of AI, allows the computer to learn without programming (Brown, 2021). Following Moore's law, it is inevitable that the distinct areas of research, development, and implementation of AI and robotics will eventually merge with the medical and scientific research in bionics and wearable technology, creating cyborgs.

In Darwin's The Origin of Species, he writes "Natural Selection, as we shall hereafter see, is a power incessantly ready for action, and is immeasurably superior to man's feeble efforts, as the works of Nature are to those of Art." (Darwin, 1859). Evolution can be characterized by adaptation for survival. Humans environmental and climate change adaptation is exhibited by the differences in skin pigmentation. We have evolved from hunter-gathers to the domestication of animals and grains leading to an agrarian society (Max, 2017). Humanity's current stage of evolution results from environmental pressure coupled with our own nature to improve the world around us through technological and scientific progress The modern era is no different, driven by medicine to restore their fellow humans' abilities, to science to increase humanities capabilities, humanity is evolving. Into cyborgs.

Figure 5-3 Evolution of Cyborg

Source: *(Kytaiko, 2023)*

THE CURRENT STATE OF CYBORGS (2023)

Neil Harbisson was born with achromatopsia, total color blindness. Rob Spence lost vision in his left eye. Adrianne Haslet-Davis lost her foot in the Boston Marathon terror attack in 2013. All have chosen to become cyborgs through medical procedures. Neil hears color through a fiber optic device and microchip implanted in his skull. The antenna, above his right eye "...picks up the colors in front of him, and a microchip implanted in his skull converts their frequencies into vibrations on the back of his head. Those become sound frequencies, turning his skull into a sort of third ear" (Max, 2017). Rob Spence lost sight in his right eye after a weapons accident as a teenager. He chooses to replace his eye with a miniaturized camera, recording his life first person point of view of the world, declaring himself an Eyeborg (Kell, 2010). Adrianne Haslet-Davis, a ballroom dancer lost her left leg in the 2013 terror attack on the Boston Marathon (Thompson, 2022). MIT's Media Lab, built her a bionic limb, enabling her to regain her dancing life, through research expertise in prosthetics, robotics, machine learning and biomechanics (Herr, 2014).

The current state of medical research and surgical procedures combining machines with man will yield enhanced humans, cyborgs whose abilities exceed those of their fellow humans. This section will explore the current state (as of 2023) of research, development, and the lives of cyborgs. Along with prosthetics, eye replacements, and bionics, the areas of brain-computer interfaces, Agonist-antagonist Myoneural Interface (AMI), subdermal microchips, and exoskeletons are going to be reviewed.

Rob Spence lost his playing with a gun at age 13. As an adult, he has replaced his eye with a prosthetic eye fitted with a camera, recording his life as a "Eyeborg" (Warrick, 2017). His bionic eye, described as more a spherical contact lens, consists of a battery, video camera, video transmitter, attached to a circuit board (Spence, 2014). The company Second Sight's product, the Argus II, "...converts images from cameras, into signals that the electrodes implanted in the eye can use, and that the brain can interpret. The Argus II allows Fran Fulton, 66, who is blind due to retinitis pigmentosa – a degenerative eye disease that slowly causes light-sensitive cells in the retina to die off, too see again through her camera equipped glasses. The Argus II is early in its development,

allowing Fran and the other 6 people equipped to see black & white pixelated image. Second Sights next phase seeks to skip the retinal layer, and implant electrodes into the visual area of the brain (Eveleth, 2014).

Figure 5-4 Rob Spence, Eyeborg

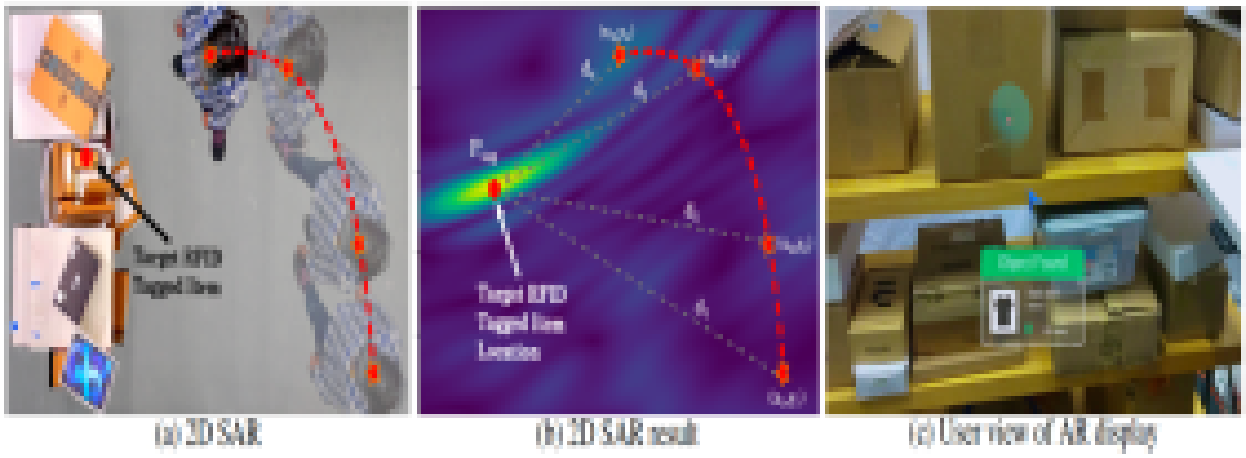
Source: *(BBC Click, 2017)*

Figure 5-5 a& b Detail of Rob Spence prosthetic eye.

Source: *(Ghose, 2017)*

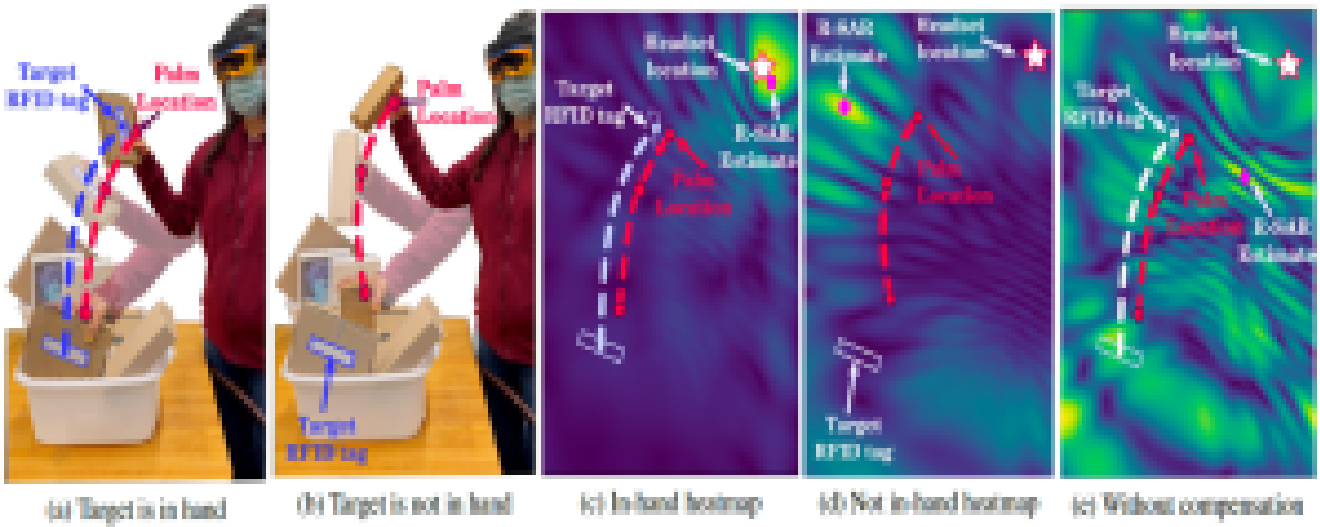
MIT (as of March 2023) uses a Microsoft HoloLens to design implement augmented reality (AR) system with non-line-of-sight perception. This system augments AR headsets with radio frequency (RF) sensing enabling the operator to see RFID tagged objects that are normally outside the spectrum of light for the human eye. The tech utilizes innovative algorithms, radiation and bandwidth capabilities, and localization of line-of-sight and non-line-of-sight objects. A driver for this innovative tech is the desired effect boosting efficiency in manufacturing, warehousing, logistics, and retail. The outcome is creating efficiency in worker labor by "...by visualizing assembly tasks, automatically labeling tools in the environment, and helping users find parts they need. More generally, AR head- sets are expected to make workers more efficient by an- notating their environments, visualizing their next tasks, and guiding them in executing these tasks (Boroushaki, Lam, Dodds, Eid, & Adib, 2023).

Figure 5-6 Augmented Reality SAR



Source: *(Boroushaki, Lam, Dodds, Eid, & Adib, 2023)*

Figure 5-7 VAR & RF-visual in hand verification



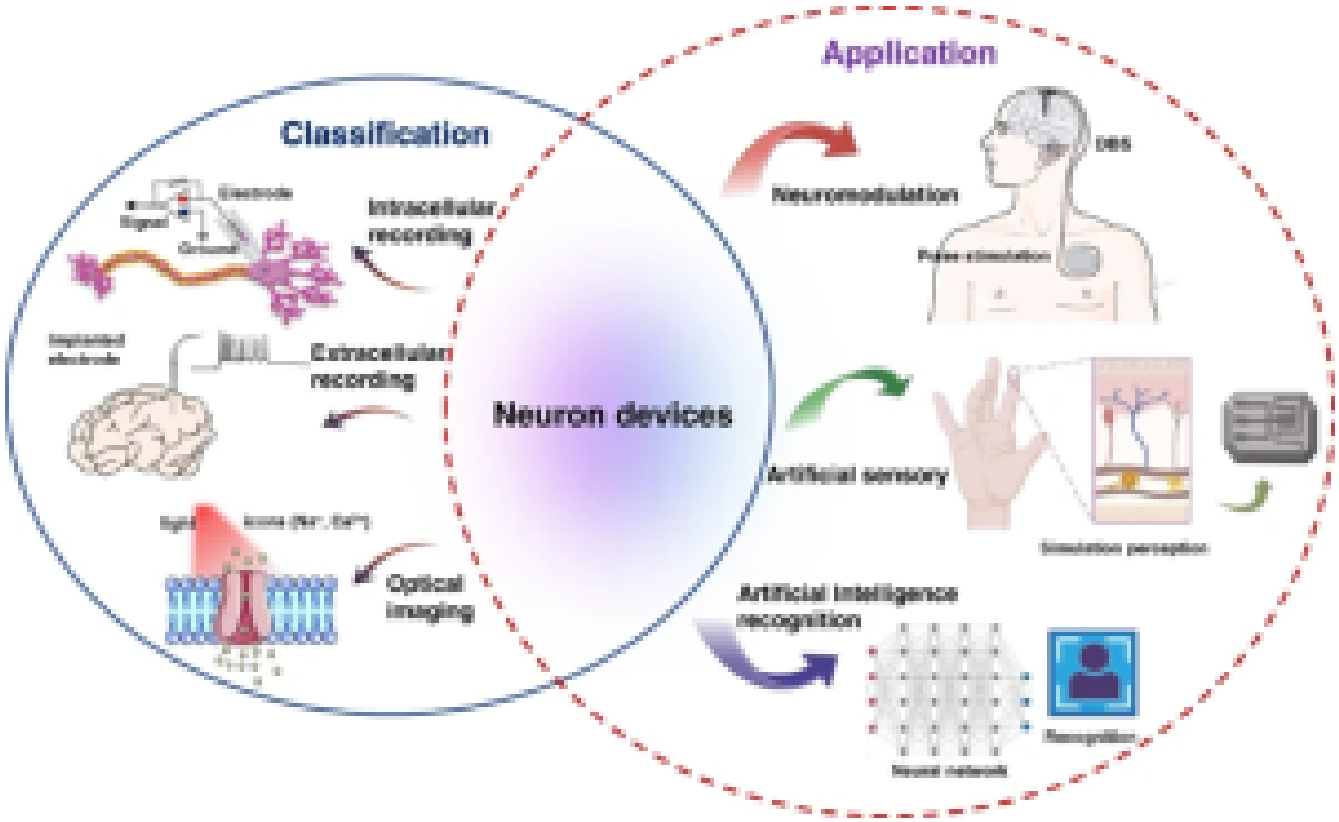
Source: *(Boroushaki, Lam, Dodds, Eid, & Adib, 2023)*

In 1998, Kevin Warwick, a professor of Department of Cybernetics at the University of Reading, self-

experimented with a silicon chip implanted in his arm allowing a computer to monitor his movements. Communicating via radio waves to a network of antennas that transmitted signals to a computer programmed to respond to his actions, a voice box saying "hello" as he entered rooms, or doors opening on his approach. His first self-experiment consisted of a glass-capsule implanted under his skin, on top of the muscles. His following attempt will focus on "biomedical signal processing – i.e., creating software to read the signals the implant receives from my nervous system and to condition that data for retransmission" (Warwick, 2000). Warwick's self-experiments complement research at Neural Engineering Clinic in Augusta, Maine using technology treating patients with damaged central nervous systems to achieve basic muscle function and at Emory University, Atlanta, GA, who implanted a transmitter in the brain of a stroke patient transmitted a signal from the brain to a computer operating it (Warwick, 2000).

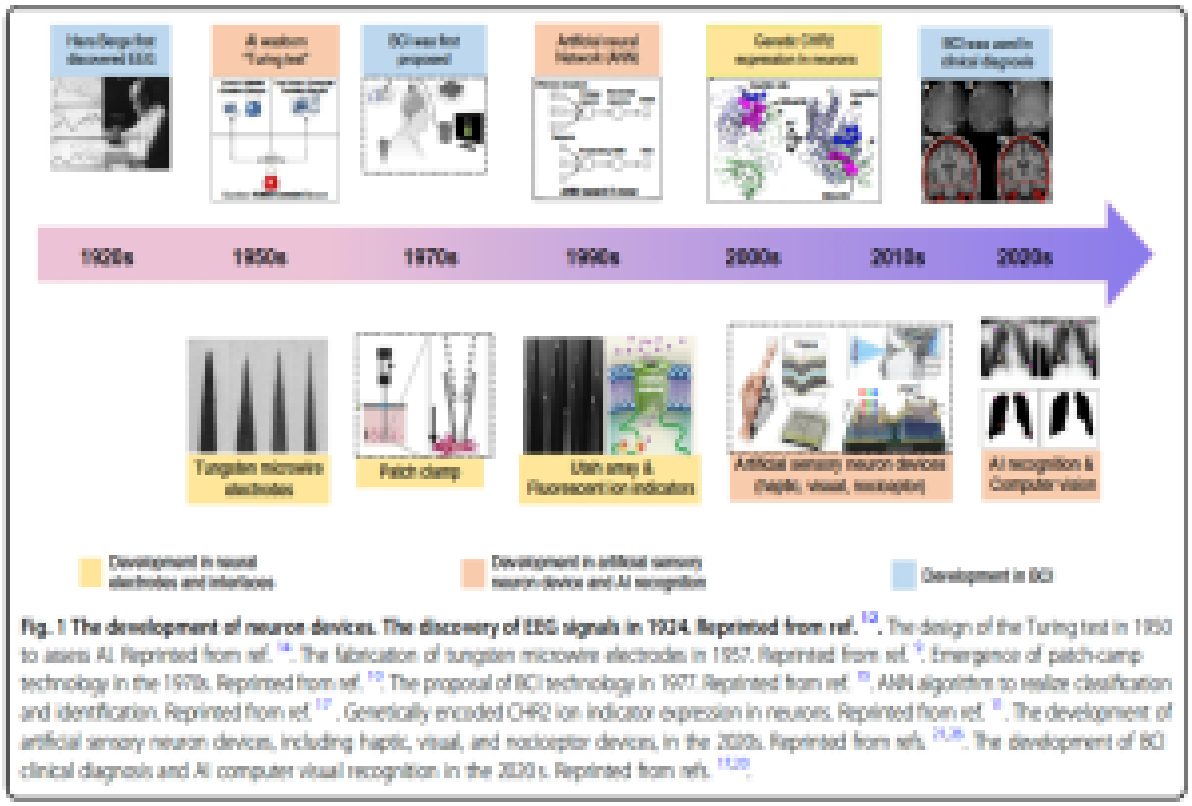
Neuro-prosthetics, a multidisciplinary filed at the intersection of neurosciences and biomedical engineering, whose focus is replacing or modulating areas of the nervous system impaired through disease degeneration or accident. For 60 years, the field has evolved to the point of commercial application of the tech treating cognitive functions and memory issues (Gupta, Vardalakis, & Wagner, 2023). Brain Machine Interfaces (BMI) or are "device that translates neuronal information into commands capable of controlling external software or hardware such as a computer or robotic arm. BMIs are often used as assisted living devices for individuals with motor or sensory impairments." Brain Control Interfaces (BCI) a system that analyzes signals from the central nervous system and translates them into machine commands (Nature, 2023). Synchron is a neural interface company that designs and develops an endovascular, implantable brain-computer interface, which allows a patient's thoughts to be transmitted wirelessly through the skin to control an array of digital devices (Zomorodi, Gutierrez, & Meshkinpour, 2023). Their product Stentrode — "an implantable brain-computer interface that collects and wirelessly transmits information directly from the brain, without the need for open surgery" During human trials, Phil O'Keefe, whose paralysis cannot use his hands or fingers, is able to Tweet his thoughts using Synchron's tech using blue-tooth (Oxley, 2022).

Figure 5-8 Brain Control Interface



Source *(Gupta, Vardalakis, & Wagner, 2023)*

Figure 5-9 Development of neuron devices



Source: *(Wang, Liu, Wang, Zhao, & Zhang, 2022)*

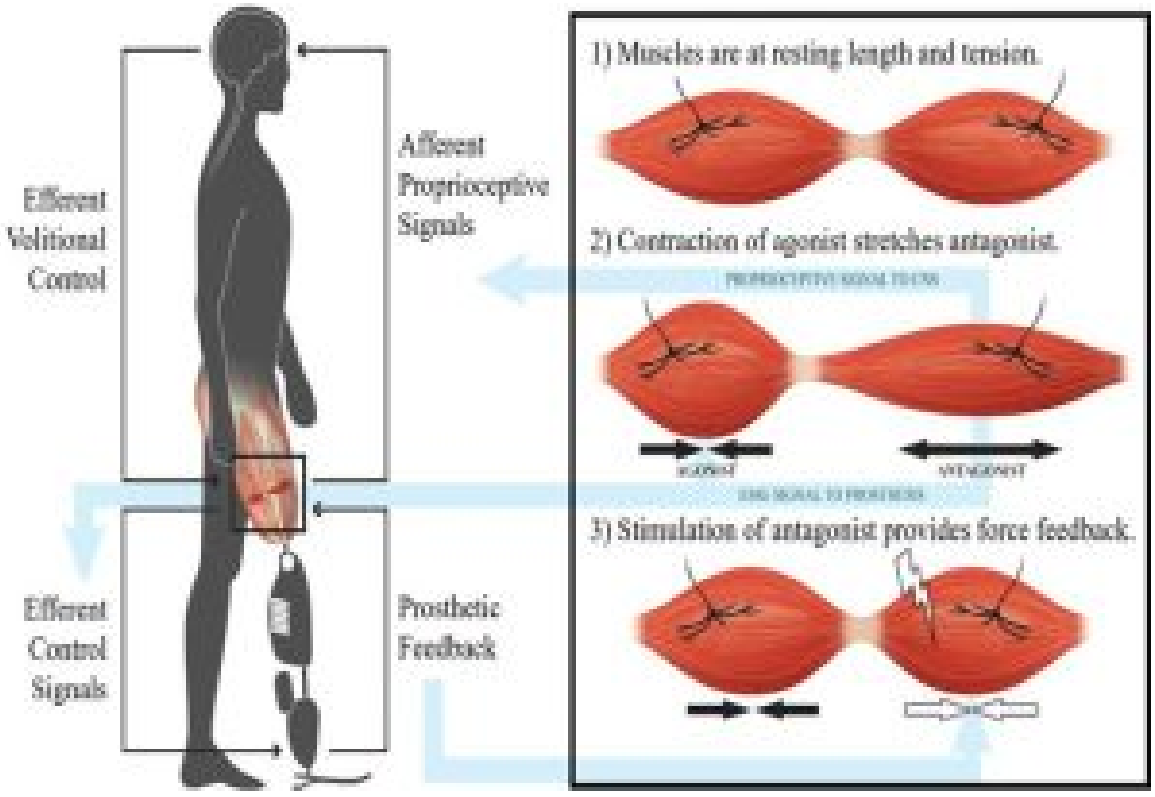
Bionics, as defined by Britannica, is the science of constructing artificial systems that have some of the characteristics of living systems (Britannica, 2022). Merriam-Webster defines cybernetics as the science of communication and control theory that is concerned especially with the comparative study of automatic control systems (such as the nervous system and brain and mechanical-electrical communication systems) (Merriam-Webster, 2023). They both use the study of living systems, bionics searching for innovative uses of machines and systems, where cybernetics pursues the reason behind living beings control systems and processes.

Human augmentation, the addition of robotic body parts that increase our capability, is being worked on at Cambridge University. They have designed a 3D thumb to be added to any hand. Dani Clode, the designer, stresses that, in addition to assisting those missing limbs, the augmented thumb does not take away from the user, seeking to increase ability and capability. This device, instead of using brain control interface, is "connected to two wrist-based motors that are hooked up to a battery and microcontroller on the upper arm. This system is wirelessly connected to microcontrollers mounted on the wearer's shoes or ankles, which are connected to pressure sensors underneath the two big toes." (Davis, 2023)

Prosthetics range from a simple replacement limb to limbs that can manipulate objects, hands that grasp, and lower limbs that articulate at joints to emulate movement. Simple prosthetics that can grasp are designed as described above, the wearer manipulates an interface to articulate the prosthetic hands. In the Massachusetts

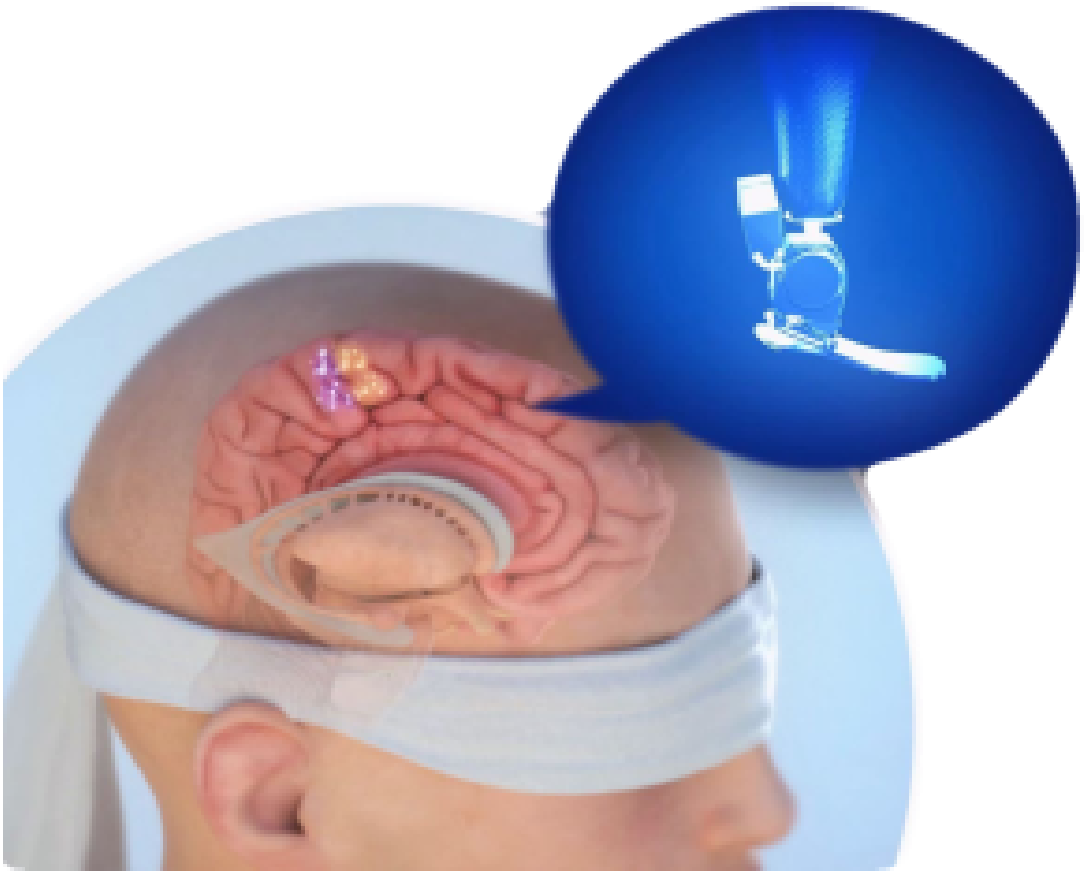
Institute of Technology labs, they are conducting research and application into Agonist-antagonist Myoneural Interface (AMI) and Neuro-Embodied Design. AMI closes the gap in conventional prosthetics providing the wearer proprioception, the ability to sense position, speed, and torque of their limbs, allowing precise control of their limbs. AMI's goal is to restore amputees with proprioception (Hsieh).

Figure 5-10 Agonist-antagonist Myoneural Interface (AMI) and Neuro-Embodied Design



Source: *(Hsieh)*

Figure 5-11 Agonist-antagonist Myoneural Interface (AMI) and Neuro-Embodied Design



Source: *(Hsieh)*

Dr Hugh Herr, of the MIT Media Lab, director of the biomechatronic research group and co-director of the MIT Center for Extreme Bionics, describes bionics as "this glorious interplay between biology and engineering design." He himself is a double amputee who enjoys full ability to walk, run and climb due to AMI and neuro-embedded design which he describes as a method to "co-design the biological body with [a] synthetic construct to maximize bi-directional communication between the device and the human nervous system." (Snyder, 2021). Or, a bionic limb, powered by a computer, that sends and receives signals from the central nervous system. AMI and neuro-embedded design's practical effects are demonstrated in two TED talks by Dr Herr, culminating in the stories of Adrianne Haslet-Davis, who lost her leg in the Boston Marathon bombing, re-gaining the ability to climb again (Herr, 2014) and Jim Ewing, regaining the ability to mountain climb (Herr, 2018).

Figure 5-12 Dr. Hugh Herr & AMI prosthetic legs

Source: (Dann, 2015)

Figure 5-13 Dr. Herr & Adrianne Haslet-Davis, a ballroom dancer lost her left leg in the 2013 terror attack on the Boston Marathon

Source: *(Bast, 2014)*

In an anatomical sense, an exoskeleton is a rigid or articulated envelope that supports and protects the soft tissues of certain animals (Editors of Encyclopedia Britannica, 2017). In human sense, an exoskeleton is application of robotics and biomechatronic towards the augmentation of humans in the performance of a variety of tasks (Exoskelton Report). In simpler terms, an exoskeleton is a tool, using robotics, that exponentially increases the capability of the human form. The International Federation of Robotics classifies robots in two sectors, Service Robots and Manufacturing Robots (Muller, 2022), where exoskeletons can cross-over into both realms. One source that provides a survey of the exoskeleton sector adds Consumer, Industrial, Medical and Military applications to the mix. The ExoskeletonReport.com identifies 120 companies (as of April 2023) that provide exoskeletons in one (or more) of their categories (Exoskelton Report).

Consumer applications include sports and educations exoskeletons. Industrial applications range from arm, back and limb support to tools use and powered gloves. The medical applications garner the largest range of applications and companies provide exoskeletons. Medical uses include upper and lower body fixed and mobile rehabilitate and assistive functions (Exoskelton Report). Medical exoskeletons support faster therapy, recovery and rehabilitation from injuries or damage to the central nervous system including exoskeletons enabling wheelchair bound patients the ability to stand, walk, turn and climb (2020). The smallest tracked category, the military sector, possess the potential to have the most outsized impact on the military and civilian sector.

The initial aim of military applications is to create a distinct advantage to Soldiers to accomplish their mission and complete their task. Harvard's Wyss Institute for Biologically Inspired Engineering, in partnership with the Defense Advanced Research Projects Agency (DARPA), develop exoskeletons that reduce fatigue and minimize Solider injury. DARPA TALOS (Tactical Assault Light Operator Suit) projects goals is to develop an exoskeleton that us "Engineered with full-body ballistics protection; integrated heating and cooling systems; embedded sensors, antennas, and computers; 3D audio (to indicate where a fellow warfighter is by the sound of his voice); optics for vision in various light conditions; life-saving oxygen and hemorrhage controls" (Jacobson, 2015).

Figure 5-14 DARPA conception of an Exoskeleton for Soldiers

Source: DARPA Warrior Web Program

Figure 5-15 The Human Universal Load Carrier, or HULC

Source: Lockheed Martin – HULC & *(Edwards, 2012)*

The word "cyborg," coined by Manfred Clynes (1960), is a combination of "CYBernetic" and "ORGanism" (cyborg conference INTRO). In this text, the working definition of a cyborg is the increase in human capability through mechanical or electrical means resulting in improved biological, bio-mechanical or neurological human abilities (author, 2023). Further classifying cyborgs into a taxonomy would be helpful later when discussing the legal, moral, and ethical status of cyborgs. Futurists are establishing a theoretical discussion of class and type of cyborg to set a framework. From the 2021 Cyborg Conference, Monika Michalowska, Steve Fuller and Steve Mann provide a "fundamental taxonomy of cyborgs: a Type I cyborg is one in which a human enters a vessel or other environment (e.g., boat, "wearables," spacesuit), and a Type II cyborg is one in which a vessel enters a human (e.g., "implantable"), or hybrids of Type I and Type II (Mann et. al., 2021)." (Michalowska, 2021). Cyborgs taxonomy can be further categorized in division and category based on structure and role. The division of cyborgs could be biomedical cyborgs, digital cyborgs, and robotic cyborgs. Categorization could include material cyborgs and information cyborgs (Michalowska, 2021).

WHERE ARE WE HEADED (WITH CYBORGS)?

General (retired) Paul Gorman described a version of 21st Century Cyborg warriors for DARPA in 1985. He described a "integrated-powered exoskeleton" that "...offered protection against chemical, biological, electromagnetic, and ballistic threats, including direct fire from a .50-caliber bullet" and "incorporated audio, visual, and haptic [touch] sensors". He imagined that each "each soldier would have his own physiological specifications embedded on a chip within his dog tags. And "he would insert one dog-tag into a slot under the chest armor, thereby loading his personal program into the battle suit's computer." (Jacobson, 2015). In Annie Jacobson's article, she reminds the reader "That connecting the human brain to a machine would produce a matchless fighter has not been lost on DARPA."

Imagine the combing of the current medical and tech research, development and practical in robotics, bionics, prosthetics, brain-machine/brain-computer interfaces into a Cyborg, the combination of human, computer and machine that exceeds human capability. In the previous section, we described the current state of Cyborgs, all external to the human body. But what of internal to the brain and body? At the atomic level and neural level. This section will discuss Nanotechnology, neuro-interfaces, and neural networks.

Nanorobots are microscopic machines small enough to flow through human blood veins. One use of nanorobots that is applicable to Cyborgs is real-time monitoring and imaging. Nanorobots can be outfitted with monitors, sensors, and the capability to deliver medicine at the cellular level as well as the potential to conduct surgical procedures at the nano-level. Potential uses of sensors include real-time monitoring of physiological parameters of blood pressure, heart rate, and glucose levels. The monitor nanorobots would be fitted with transmitters to communicate with medical personal in real-time. Imaging sensors allows doctors to see the level of detail not available in current X-ray, MRI, and CTI scans. Nanorobots, controlled by doctors could perform minimally invasive procedures and deliver medicine to the cellular level increasing their effectiveness and reduce surgical complications (Saikia, 2023).

In Section II, Brain-Machine Interface (BMI) and Brain-Control Interfaces (BCI) discussion focused on the devices that are implanted in human's brain's that are capable of transmitting control signals to external devices and chips implanted to monitor the central nervous systems sending signals to external devices. Parkinson's Disease, Alzheimer's and paralyzed patients benefit from BMI & BCI, regaining some of their cognitive functions and the ability to control prosthetics limbs. The field of Artificial Intelligence (AI), whose end state is to replicate human intelligence, to reason, discover meaning, to generalize, and perform (McCarthy, 2006) using machine learning, big data and algorithms possess the potential to advance the field of neural interfaces. Neural interfaces could combine current BMI & BCI with AI to exponentially expand human capability.

Figure 5-16 BMI & BCI for sensorimotor disorder

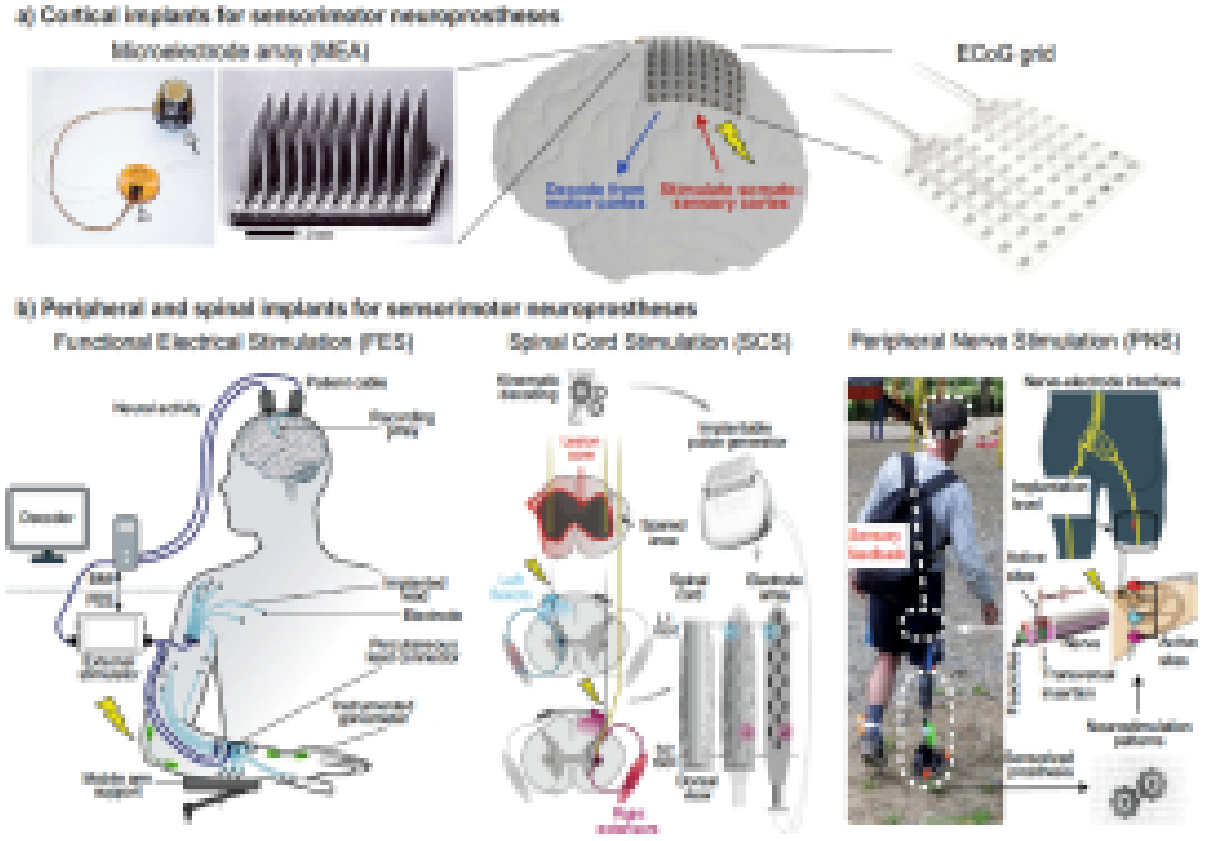


Fig. 1 Neuroprosthetic technologies for sensorimotor disorders. a Cortical implants typically used for sensorimotor neuroprostheses can be divided into two categories: intracortical MEAs such as the Utah array (10 × 10 Utah array, picture extracted with permission from ref. [18]), and epidural or subdural ECoG strips or grids with different specifications (illustrated for a 8 × 8 ECoG grid, 4 mm contact diameter, 10 mm pitch, with permission from CorTec GmbH). These implants can both record neurophysiological signals and deliver electrical stimulation. **b** Peripheral and spinal implants for sensorimotor neuroprostheses target either the motor nerves or muscles in the case of FES (adapted with permission from ref. [44]), the spinal cord in epidural SCS (adapted with permission from ref. [17]), or the sensory nerves in PNS for somatosensory feedback (adapted with permission from ref. [80]). All applications shown here used these implants for delivering electrical stimulation. Lightning bolts indicate neurostimulation.

Source: *(Gupta, Vardalakis, & Wagner, 2023)*

Figure 5-17 BMI & BCI for bi-directional thought control of prosthesis

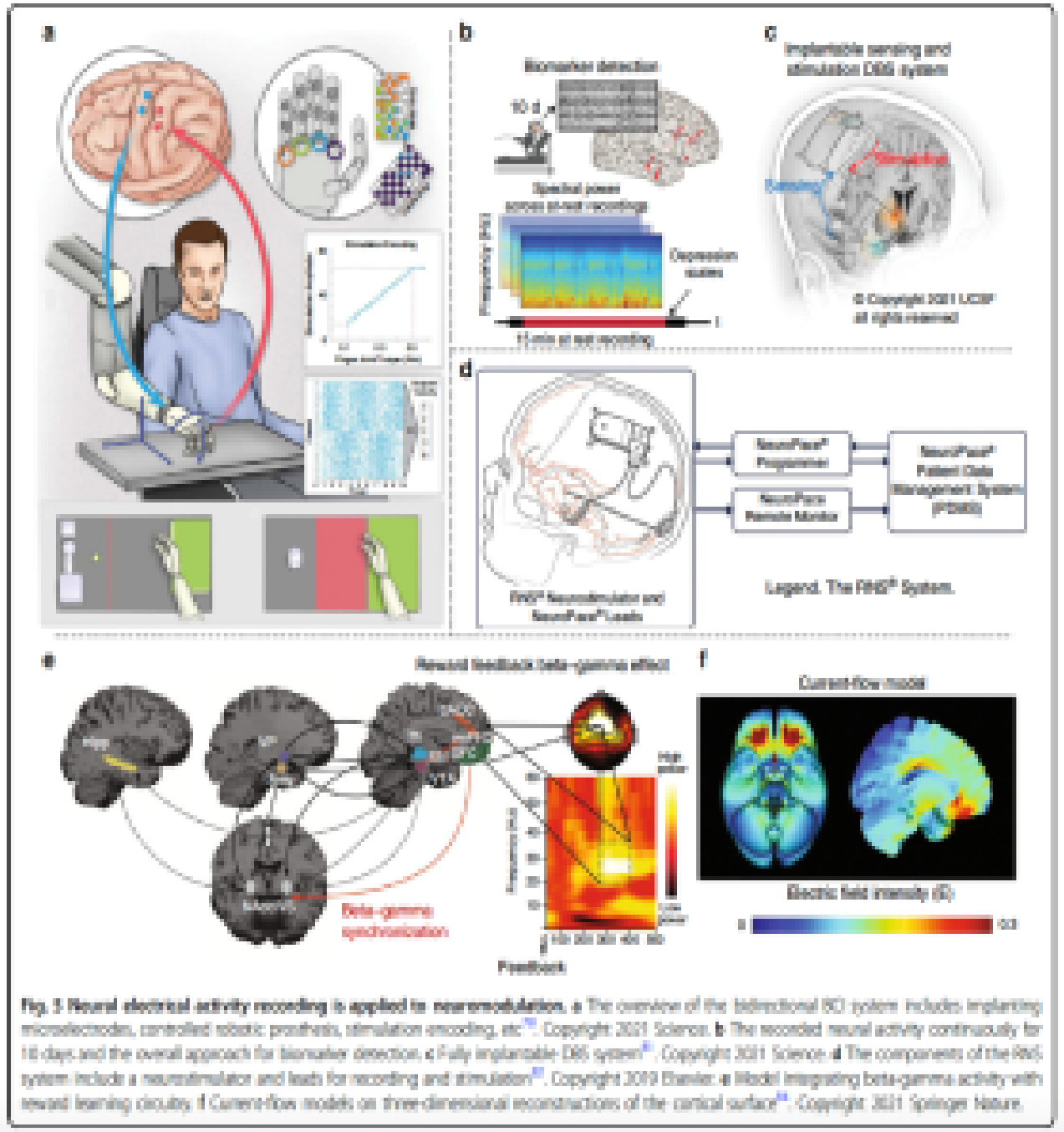


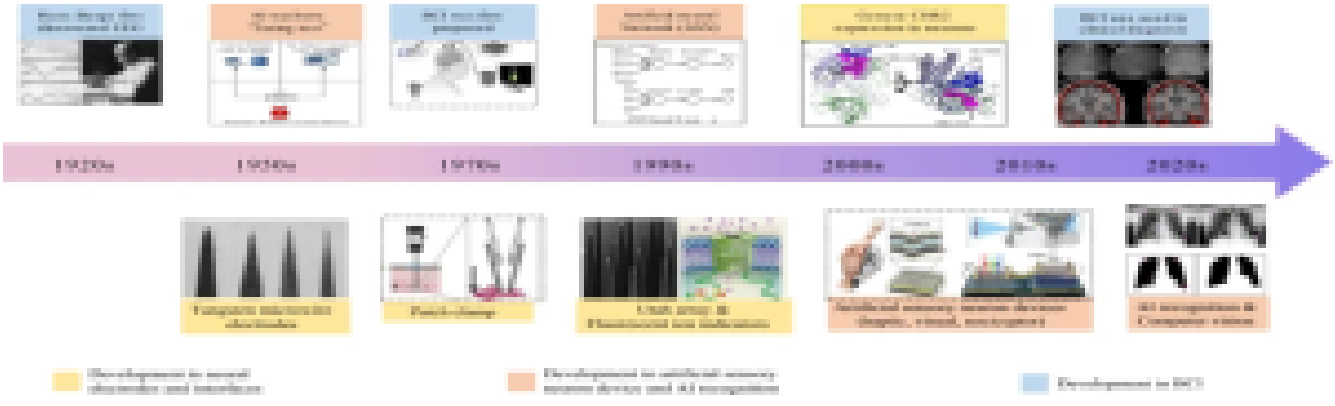
Fig. 3 Neural electrical activity recording is applied to neuromodulation. **a** The overview of the bidirectional BCI system includes implanting microelectrodes, controlled robotic prosthesis, stimulation encoding, etc.[70]. Copyright 2021 Science. **b** The recorded neural activity continuously for 16 days and the overall approach for biomarker detection. **c** Fully implantable DBS system[71]. Copyright 2021 Science. **d** The components of the RNS system include a neurostimulator and leads for recording and stimulation[87]. Copyright 2019 Elsevier. **e** Model integrating beta-gamma activity with reward learning circuitry. **f** Current-flow models on three-dimensional reconstructions of the cortical surface[88]. Copyright 2021 Springer Nature.

Source: *(Wang, Liu, Wang, Zhao, & Zhang, 2022)*

Neural interface is linking an AI brain chip with an external AI interface to communicate with machines and the external world just with thoughts (Saikia, 2023). Current neuron interfaces include devices for intracellular recordings, extracellular recordings, and optical imaging recording (Wang, Liu, Wang, Zhao, & Zhang, 2022). A 2022 article from Nature.com Microsystems & Nanoengineering section presents a survey of current and future AI Neural interface pathways including:

- Neuromodulation, the stimulation, or chemical substances applied directly to the nervous system to modify nerve cell activity.
- Bi-directional feedback for BCI control of prosthetics.
- Increased Artificial sensory neuron devices, which could "mimic complicated sensing and processing functions in biological systems, which can convert external stimuli into electrical signals"
- Artificial neuron sensory devices for mimicking the human sensory system. Bimodal artificial sensory neuron (BASE) realized the fusion of visual and haptic modalities. Pressure sensors and photodetectors are the major components of the BASE patch. Visual feedback and tactile feedback were used to create the movement of a robot's hands
- Artificial intelligence memory and recognition, A high-performance electronic device was designed to train hippocampal neurons to learn by activating their memory function through electrical stimulation. A high-performance electronic device was designed to train hippocampal neurons to learn by activating their memory function through electrical stimulation. Based on retinal photoreceptors and bipolar cells for motion detection and recognition (MDR), the two-dimensional retinal neuron hardware integrated three modules of optical perception, memory, and recognition.
- An all-optical pulse neuron device was designed to accomplish the AI task of pattern recognition. The neural network simulated by this integrated design can self-learn to complete simple recognition tasks, and it runs several orders of magnitude faster than biological neural networks; thus, it can process large amounts of data in a short time.

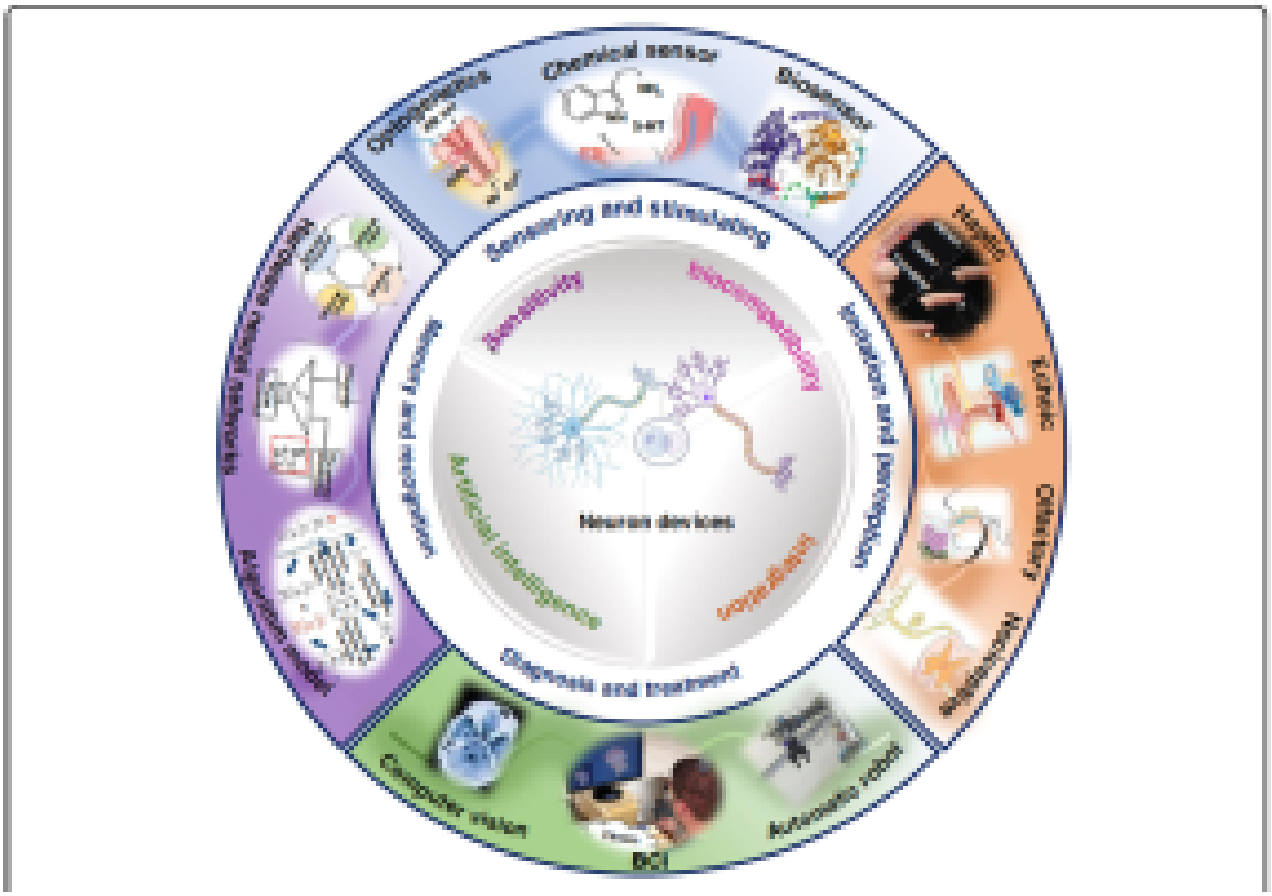
Figure 5-18 Timeline of BCI & AI development



Source: *(Wang, Liu, Wang, Zhao, & Zhang, 2022)*

A human's cognitive perception of its external environment is a complicated fusion of multiple sensory inputs. The implications of neural networks and Artificial Intelligence stands to aid in cyborg development. The current challenges of efficiency and biosafety of materials will have to be solved for AI enabled neural networks to be realized, outside of current research and development. The Figure below depicts current and future areas for the prospects of neuron interfaces. The article and survey conclude it best stating "AI technology can be used to achieve fast and efficient data processing. Combining AI with BCI and exploiting neural network algorithms will propel the development of neuron devices and improve neuroscience research" (Wang, Liu, Wang, Zhao, & Zhang, 2022)

Figure 5-19 Prospects of BCI



Source: *(Wang, Liu, Wang, Zhao, & Zhang, 2022)*

Where does genetic engineering fit into the development of cyborgs? Genetic enhancement covers the willful alteration of genes to be more than human, be it strength, cognition, or other traits. Genetic enhancements parallel cyborg enhancements as they alter the human form resulting in increased capability. It is important to note the downstream effects of genetic enhancements. If a genetic enhancement only applies

to one individual, then the genetic line remains normal, it is when the genetic modifications enter the gene pool, will the line be passed on to future generations and change the human genome (Barfiled, 2022). There is much debate on the efficacy, legality, moral, ethical, and societal effects of deliberate genetic modification, some of which will be discussed in the following sections. As this chapter focuses on cyborgs, the enhancement of human capacity with machines, gene therapy, the delivery of "a copy of a normal gene into the cells of a patient in an attempt to correct a defective gene" (Barfiled, 2022) will not be discussed beyond the above general explanation for awareness.

CYBORGS, WHAT ARE THE RISKS?

"Neuro-prosthetic devices and implants that are connected to an internal network that is itself connected to the Internet, and that are also vulnerable to infections from laptops or other device. The problem of implants being affected with a software virus is exacerbated by the fact that manufacturers often will not allow their equipment to be modified, even to add security features." (Barfiled, 2022)

RISK TO SOCIETY, A PERSPECTIVE

As a noun, risk means someone or something that creates or suggests a hazard. And as a verb, it is defined as to incur the risk or danger of *(Merriam-Webster, 2023)*. So "Risk" implies a hazard or danger. Broadly thinking, is there danger or hazard posed by Cyborgs? Conversely, is there danger or hazard to Cyborgs? This section will illuminate the topics of risk and Cyborgs, the risk to Cyborgs and what is the risk posed by Cyborgs.

What could be the risks of a cyborg? Would general society accept Cyborgs? Conversely, would Cyborgs want to be considered human by societies definitions? Would the answers change when replacing society with "government." In a world with finite resources, many of the advancements described above are currently in the research & development phase. Once Cyborgs are accepted, once the Singularity occurs, what is the risk to the acquisition of components required for industrial scale production of Cyborgs?

A 2022 Pew Research topic of AI and Human Enhancement provides some prospective of what the public's understanding and acceptance of enhanced human, Cyborgs, is. The survey covers six topics in the advancement of AI and human enhancement that possess the potential to alter society, a few of which are germane to this section, the possibilities of enhanced humans, enhanced cognitive function from computer chips implanted in the brain, and exoskeletons with AI in the workforce. In 2022, caution is the fundamental theme of the survey results. Caution relating to AI and human enhancements effect on the disparities between humans and enhanced humans and the unintended consequences of these advancements and developments. (Rainie, Funk, Anderson, & Tyson, 2022).

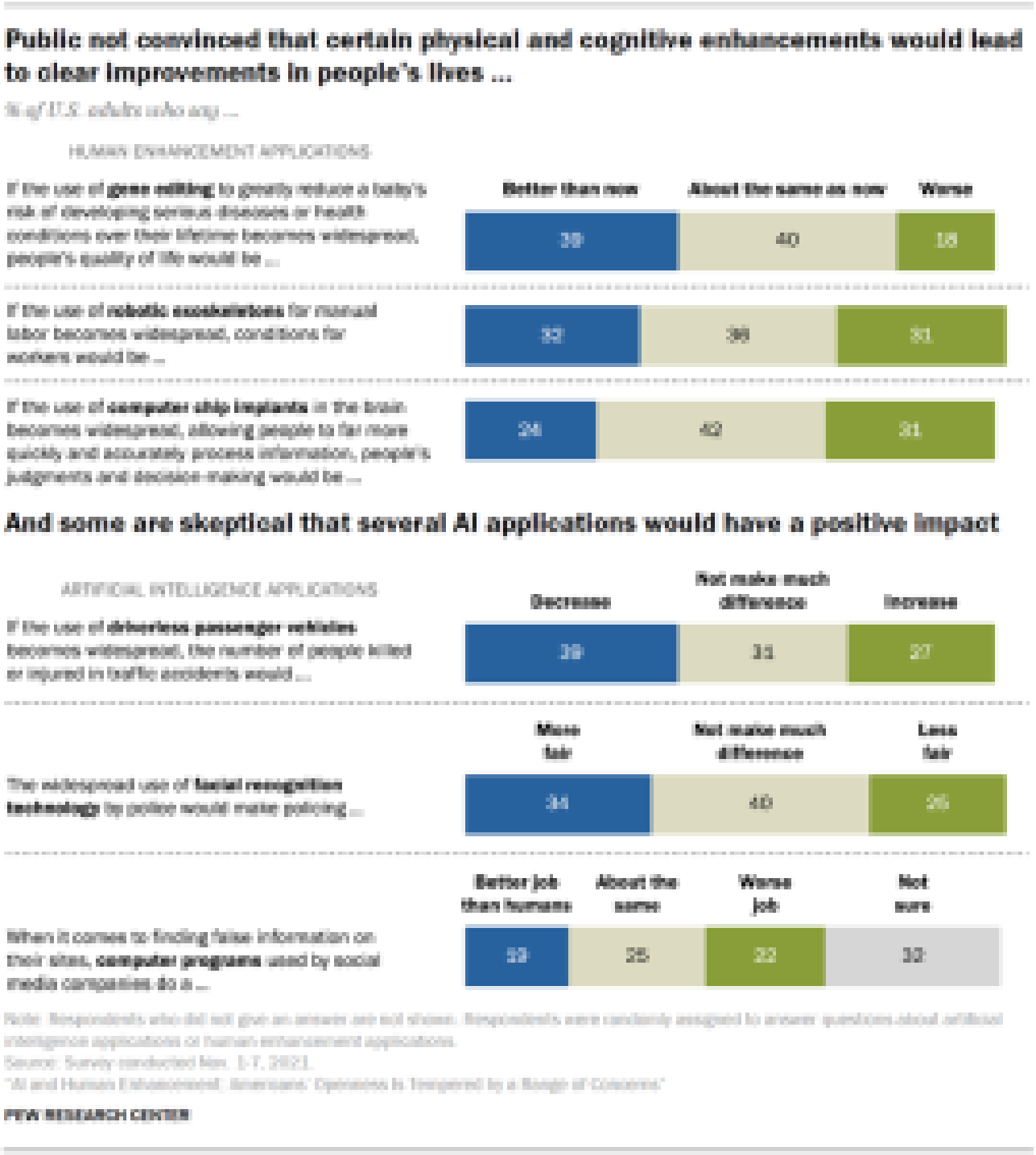
The survey results run the gamut of American public reactions to Cyborgs, and the related technology advancements. Some findings include:

- For societal benefits, more Americans view the good over bad in the use of robotic exoskeletons with a

built-in AI system to increase strength for manual labor jobs (33% vs. 24%).

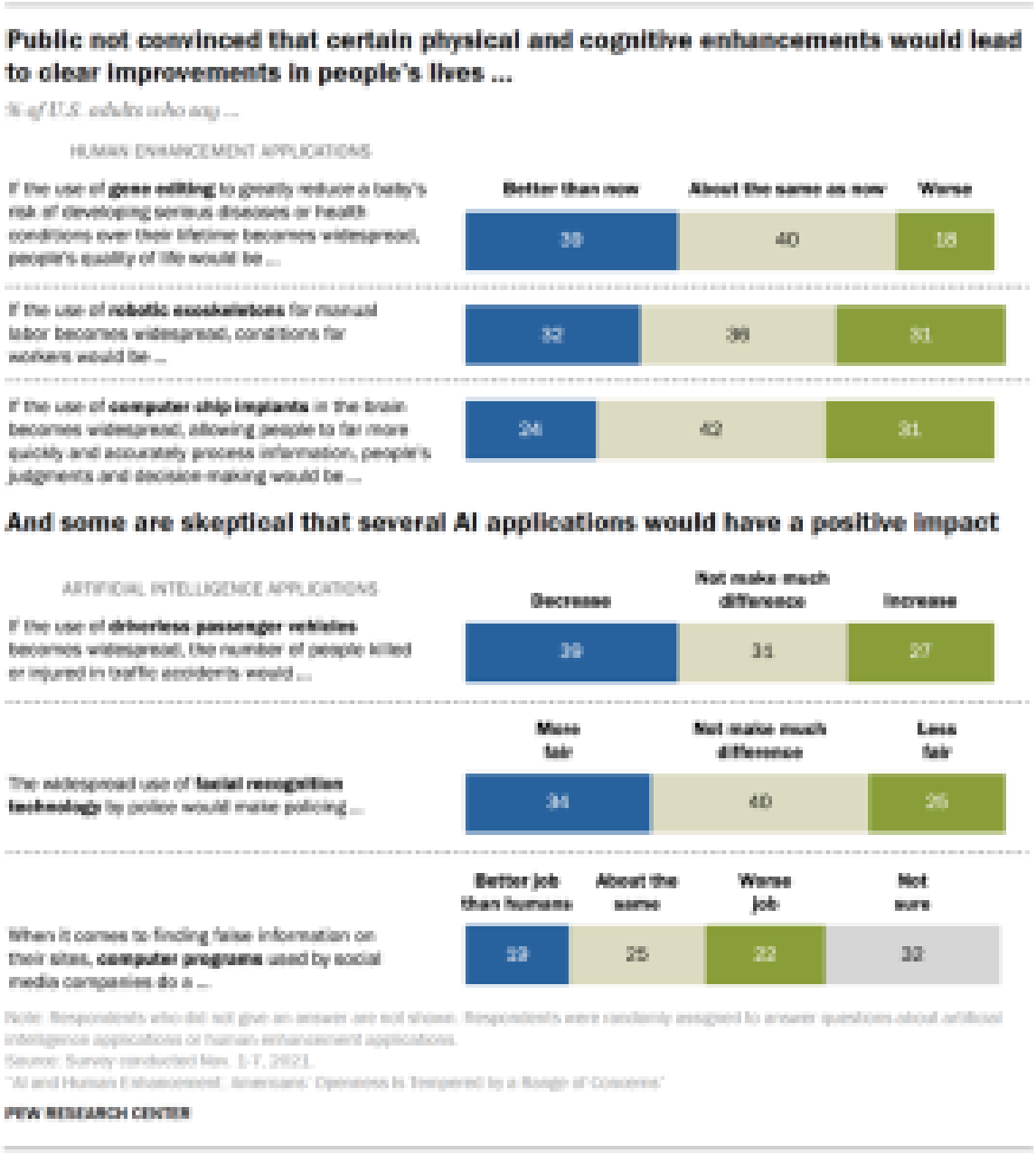
- Americans are cautious about a future with widespread use of computer chip implants in the brain to allow people to process information far more quickly and accurately: 56% say this would be a bad idea for society, while just 13% think this would be a good idea.
- Uncertainty is among the themes seen in emerging public views of AI and human enhancement applications. For instance, 42% are not sure how the widespread use of robotic exoskeletons in manual labor jobs would impact society. 45% say they are equally excited and concerned about the increased use of AI programs in daily life, compared with 37% who say they are more concerned than excited and 18% who say they are more excited than concerned.

Figure 5-20 Pew Research Center Data



Source: *(Rainie, Funk, Anderson, & Tyson, 2022).*

Figure 5-21 Pew Research Center Data



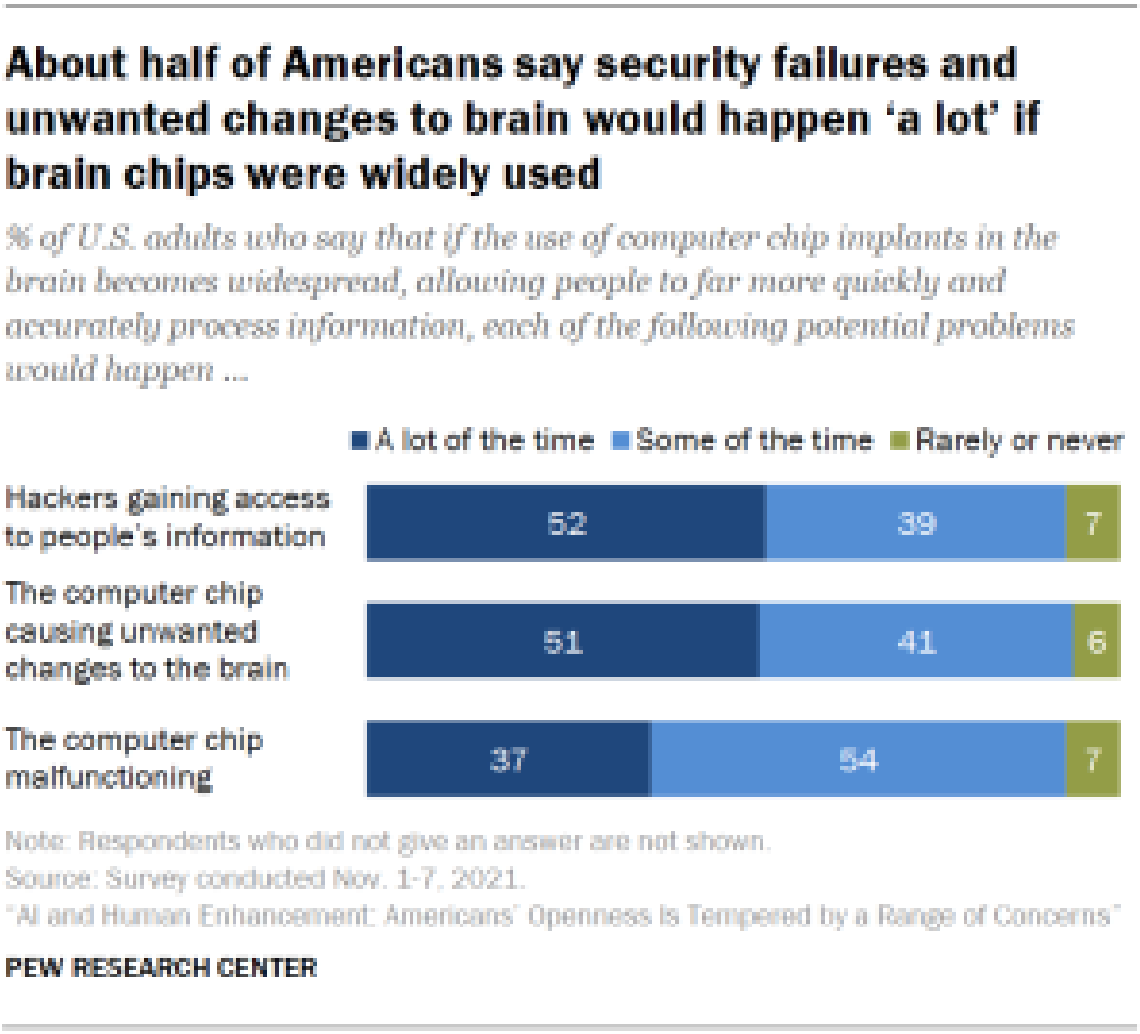
Source: *(Rainie, Funk, Anderson, & Tyson, 2022)*

What is agreed upon across the board, are the mitigating steps making the applications of human enhancement acceptable into society. For example, 7 in 10 would find driverless cars acceptable if they were labeled as such and easily identifiable. In terms of computer chip enhancements in the brain, acceptability rose if the effects could be turned on or off and implanted without surgery. Over 40% of survey respondents are more excited about the potential of enhancements that provide health benefits or disease prevention. Interestingly, 8 in 10 would "opt against" computer chip enhancements for themselves yet 6 in 10 respond that

there will be societal pressure to allow and receive these implants should they become widely available. The public are more accepting of enhancement that can be turned on or off, such as exoskeletons, than they are a brain implants that increase cognitive function (Rainie, Funk, Anderson, & Tyson, 2022).

Two interesting concerns from the Pew Research survey highlight potential risks to Cyborgs and society, the unintended consequences of cyborg enhancements, and the amount at type of government oversight and regulation. The major concerns highlighted include hackers gaining access to personal information, unwanted changes to the brain and chip malfunctions. The concern for government regulation lie along the lines of what is "enough" regulation and oversight, in the development of enhancements. What risks constitute regulation, such as the Indiana (and 10 other states) banning employers from requiring workers having devices implanted in their bodies (Marr, 2020). The survey does address the socio-economic and religious impact from respondents view-points, that enhancements "meddle with nature" and potentially increase the social-economic gap between enhanced humans, a valid concern outside the scope of this section (Rainie, Funk, Anderson, & Tyson, 2022).

Figure 5-22 Pew Research Center Data



Source: *(Rainie, Funk, Anderson, & Tyson, 2022)*

The Pew Research is one viewpoint of the risks of Cyborgs, from a societal perspective. What of the risk to cyborgs themselves? Looking at the current the advancements in Cyborg research, technology, and implementation discussed in Section III, the question of risks, vulnerabilities, impacts, and countermeasures are relevant to the safety of the cyborg, and the security of the technology (including personably identifiable and personal health information).

RISK TO CYBORGS, A CASE STUDY

Section III covers the current state of Cyborgs. The research, development and current technologies include eye replacements, implanted microchips/RFID devices, brain-computer/brain-machine interfaces, subdermal microchips, prosthetics, bionics, and exoskeletons. As stand-alone technologies, each contains inherent risk.

When considered as part of a Cyborg entity, the risk potential increases significantly, as individual lives and societal impacts are contemplated.

For the sake of space and brevity, this text will consider a risk analysis and assessment of a select few of the Cyborg technologies, using the Ryan-Nichols Risk Assessment methodology. For review, the Ryan-Nichols Risk Assessment is a threat focused methodology analyzing risk as an equation to identify threat scenarios, business objectives, improve probability calculations and predictions using probability ranges, simulate exploitable scenarios and incorporate countermeasures to reduce risk.

RISK = THREATS X VULNERABILITIES X IMPACTS / COUNTERMEASURES EQ. 5-1

Where: THREATs are real, act on a system, and represent the possibility that the attack vectors become accessible for exploitation. (The attacker has the necessary time and resources to conduct the exploit.) VULNERABILITIES are inherent weaknesses in the information system and represent vulnerabilities becoming successfully exploited. IMPACT is the business value of a successful exploit. COUNTERMEASURES represent the technical mitigations/solutions or probability that a mix of counter-technologies will reduce the active THREATS on a system. The above equation is used to calculate the Initial Risk Assessment (IRA) before any perturbation by Threats.

At time state = 0, we note that Vulnerabilities are constant and always present, and Impact is just a "delta number" and a constant. Threats and Countermeasures are independent variables; Risk is the dependent variable, Using calculus, both Vulnerabilities and Impact drop out of the IRA equation to give a compressed form:

RISK = THREATS / COUNTERMEASURES EQ 5-2

Source: (Nichols R. K., 2022)

As a case study for the Ryan-Nichols risk assessment, consider this excerpt from Woodrow Barfield's "Cyber-Humans" in the chapter "Cognitive Liberty, Brain Implants, and Neuro-prosthesis"

...a British scientist and former student of Professor Kevin Warwick, Dr. Mark Gasson, has claimed to be the first person to become infected with a computer virus. How can this be possible? In Dr. Gasson's case, purposively as part of a proof-of-concept study, but in the future, cyborg hackers could spread a virus to a person's mind by accessing brain-implant technology or by hacking into a network of wirelessly connected brains. In Dr. Gasson's study, a chip was inserted in his hand which was then infected with a software virus. Of relevance to a law of cyborgs, Dr. Gasson showed that the chip was able to pass on the computer virus to external control systems—meaning a person with cyborg "infected" technology could transmit a virus to

a machine external to the cyborg. But more importantly, if other implanted chips within a person's body, including neuro-prosthesis, had been connected to the system they too would have been infected by the virus" (2022).

With the above in mind, for this scenario, considered the near future, with a Cyborg, an enhanced human who has an RFID chip implanted in their organic limb (a hand), brain-controlled interface link to their external workstation and a neuro-link to their bionic limb (an arm-hand device and lower, limb hip to foot device). The possibility of an AI network or connected to the Internet of Things is a very real possibility but will not be considered for this analysis. Alone, each of these tech's includes their own risks, vulnerabilities, impacts, and countermeasures. As a system, each threat vector impacts the system, whereas each countermeasure reduces the risk to the system.

Each of the individual elements presents include vulnerabilities, vectors for exploitation or attack. RFID chips are common in 2023, used in a multitude of functions. Airlines track baggage using RFID tags and the FDA approved company VeriChip Corp. whose chips uses are security, art, and body-hacking (Barfiled, 2022). An RFID chip manufactured from various components, what is the security of the supply-chain of the hardware. The BCI, also manufactured and surgically installed, transmits an RF signal from the brain to the machine or workstation. Is that signal easily identifiable, and secure, on the electro-magnetic spectrum?

The bionic limb, whether an AI enabled prosthetics of the future, or the current MIT neuro-embed designed AMI limbs of Dr Hugh Herr, also present similar exploitable vulnerabilities, and vectors. A commonality of each of these components individually, or together in a Cyborg system could be their wireless communication devices.

Wireless communications are vulnerable today. They are comprised of mobile computing and communicating on the EMS via the radio frequency spectrum, satellite communications or infrared spectrum. They are low quality of service, low power and low bandwidth emanating from small devices. Historical threats include RF signal interception, mobile service access, and wireless network interference. Current security measures layers are the physical, datalink, network layers and the transfer layer, application layer.

Table 5-3 below is a look at the Ryan-Nichols Risk Assessment of the wireless communication for the Cyborg system in our case study and scenario.

TABLE 5-1 RISK = THREATS / COUNTERMEASURES (Wireless Communications)

Risks	Threats	Countermeasures
o RFID Tag components o Implant components o Bionics components o RF Signals (Wi-Fi, Bluetooth) o Data Systems Hack (internal, external, in transit, at rest, cloud) o System takeover/control	o Cryptographic attack o One-time access to encrypted information o One-time security forgery o Spoof o Vector ID for repeated access o Electro-Magnetic Pulse (EMP) attack o computer hackers o criminals o industrial or state-sponsored spies o enemy armed forces o terrorists o psychotic persons o drug lords o saboteur	o Waveforms, with anti-jam (A/J) and low probability of detection (LPD) characteristics o INFOSEC/COMSEC o Emanations security (EMSEC) The control of emanations that may compromise internal information. o Electronics security: The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of noncommunication electromagnetic radiations (for example, radar). o Transmission security (TRANSEC) The protection of transmissions (“externals”) from traffic analysis, disruption, and imitative deception. o Cryptographic security (COMSEC) The use of encryption to protect communication content (“internals”). o Survivability o Laws & Regulations o U.S. The Computer Fraud and Abuse Act o U.K. Section 3 of the Computer Misuse Act o Encryption (data, signals) o Authentication (Biometric, Multi-Factor, Zero-Trust, Quantum, etc.)

Table 5-1 Ryan Nichols Risk Assessment: Wireless components of Cyborgs. The Risk, Threats & Counter Measures are derived from the authors experience and Nichols & Lekkas

Source: Wireless Security: Models, Threats, and Solutions (2002)

The Ryan-Nichols assessment provides a framework for a qualitative and quantitative assessment (see Table 5-2). The threats presented could originate from internal or external to the Cyborg. To the threat actor, does the return on investment of the exploit or attack carry value to the perpetrator, revealing access points and exploit techniques? When assessing countermeasure, keep in mind a couple of maxims, threats evolve faster than countermeasures and the critical thinking mindset of action-reaction-counteraction. The countermeasures identified should be universal, but are not, as wireless communications are vulnerable as of this writing. The possibility of the risks remaining constant through the Singularity are likely.

Table 5-2 Ryan-Nichols Risk Assessment Lethality Legend

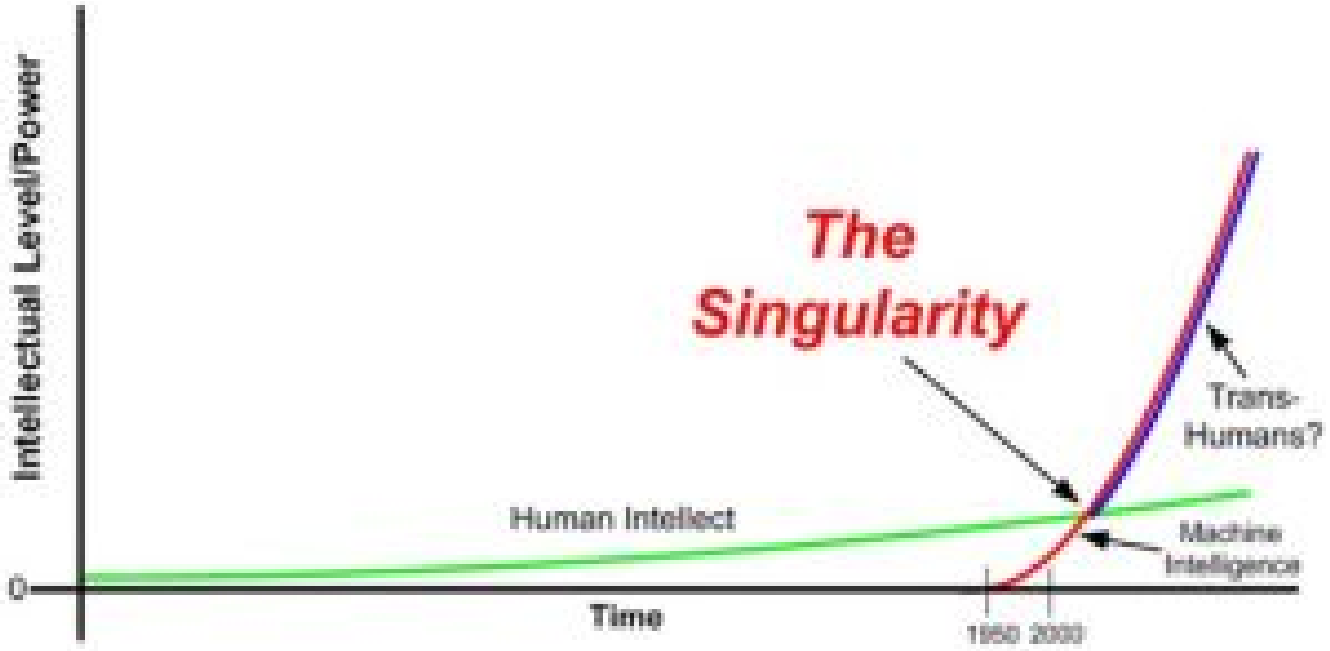
Qualitative Measure	Quantitative Value
High	81-100%
Medium-High	56-80%
Medium	31-55%
Low-Medium	14-30%
Low	7-13%
Very Low	0-6%

Source: *(Nichols R. K., 2022)*

CONCLUSION 1, THE SINGULARITY

"The Singularity is that point in or development time when artificially intelligent machines equal or surpass humans in intelligence." (Barfiled, 2022)

Figure 5-23 The Singularity Timeline



Source: (Kurweil, 2005)

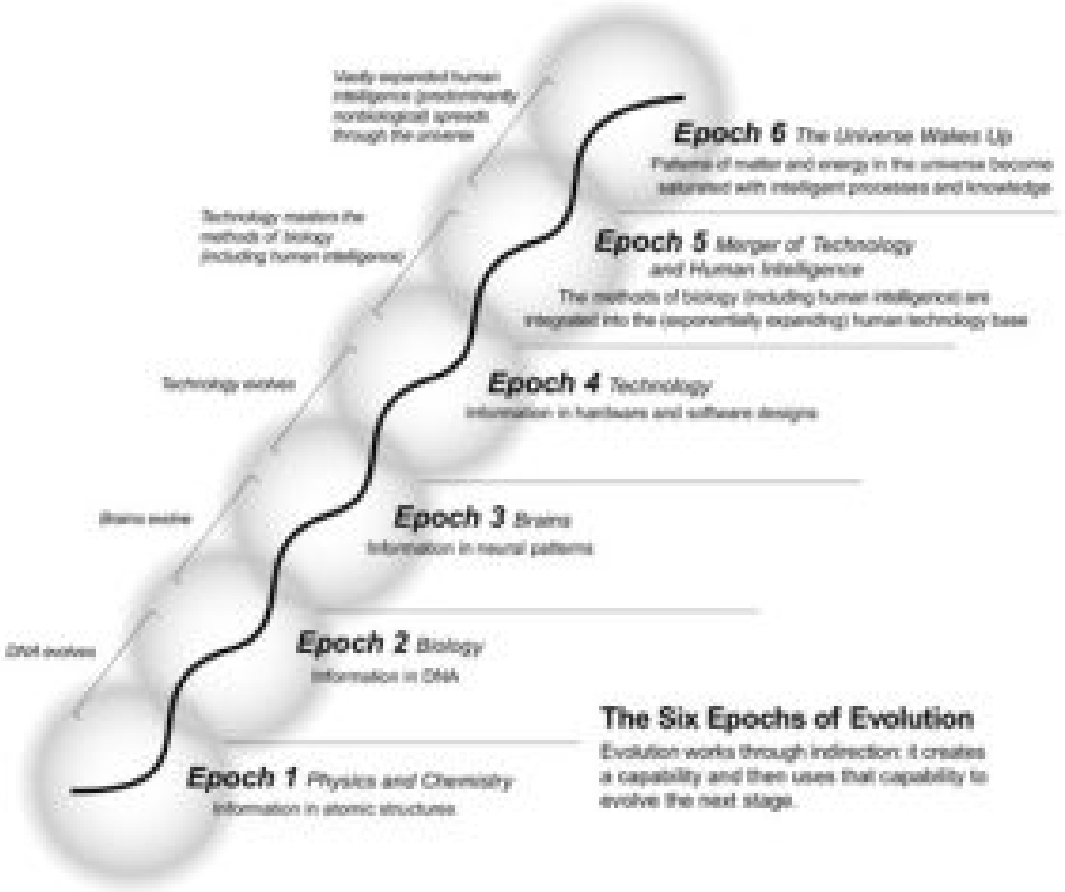
There is no one definition of the Singularity. Each futurist, or trans-humanist, applies their perspective to the overarching theme of rapid technological growth of genetics, nano-technological and robotics that is leading to a merger of man and machine. Or Cyborgs are inevitable.

Three interlocking developments are shaping the Singularity, genetics, nanotechnology, and robotics. An explanation of the progress towards the Singularity can be understood by applying Moore's Law and Monsanto's Law (Horner, 2008). Moore's law states each new generation of computer chip provides twice as many components per unit cost, each of which operates faster the number of transistors that could fit on a

single computer chip had doubled every year for six years from the beginnings of integrated circuits in 1959 and Monsanto's law, which states that the ability to identify and use genetic information doubles every 12 to 24 months. These laws of accelerating returns leads to Ray Kurzweil's Singularity definition "...It's a future period during which the pace of technological change will be so rapid, its impact so deep, that human life will be irreversibly transformed." (Kurweil, 2005).

One path leading to Kurzweil's definition is his own Six Epochs of Evolution. His Epochs "... works through indirection; it creates a capability and then uses that capability to evolve to the next stage. Epoch One: Physics and Chemistry is the era of the emergence of patterns of matter and energy whilst Epoch Two: Biology and DNA represents the emergence of life and self-replicating organisms. Epoch Three: Brains – is the epoch of the emergence of 'information in neural patterns' leading to the human ability to conceive abstract models of the world. Epoch Four is the epoch of technology – seen in terms of the emergence of information technology and a rapid acceleration of technological evolution as compared with biological evolution. Epoch Five is the merger of human intelligence with machine intelligence. Epoch Six: The Universe Wakes Up this post-singularity period begins to be described as '...the ultimate destiny of the Singularity and of the universe' (Kurweil, 2005).

Figure 5-24 The Six Epochs of Evolution



Source: *(Kurweil, 2005)*

Where do Cyborgs fit into The Singularity? An argument could be, they are riding the wave towards The Singularity. Consider the working definition used in this chapter, increasing human capability through mechanical or electrical means resulting in improved biological, bio-mechanical or neurological human abilities. Or Cyborgs are enhanced humans with increased capability, derived from the intersection of genetics, nanotechnology and robotics resulting in increased human abilities. Remember the scenario in Risk to Cyborgs, an enhanced human who has an RFID chip implanted in their organic limb, brain-controlled interface link to their external workstation and a neuro-link to their bionic limb. Individually, all of these occur today, circa 2023. Look quickly to the future and the Cyborg is working in Space, as the NASA studies of the 1960's envisioned.

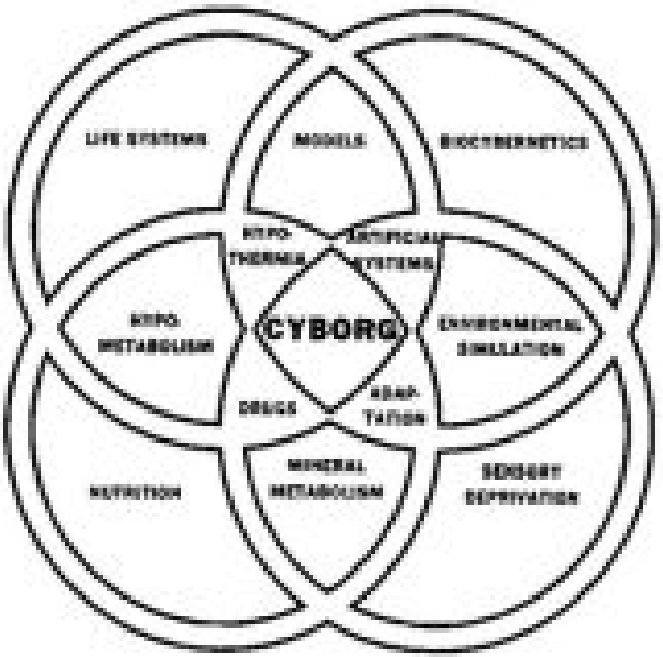
CONCLUSION 2, CYBORGS AND SPACE

"Altering man's bodily functions to meet the requirements of extraterrestrial environments would be more than logical than providing an earthly environment for him in space...Artifact-organism systems which would extend man unconscious, self-regulatory controls are one possibility." (Clynes & Kilne, 1960)

In 1960, scientists, researchers and futurists were thinking about the practical applicability of cyborgs supporting extra-terrestrial exploration. Two researchers, Manfred Clynes and Nathan Kline, in 1960 wrote about the biological impediments to man's long term exploration of space, explaining that man's adaption to the space environment by incorporating exogenous means would induce the biological changes allowing man to function, to "live in space qua natura" They argue that man as a cyborg, rather than monitoring external systems to keep him alive, "...is to provide an organizational system in which such robot-like problems are taken care of automatically and unconsciously, leaving man free to explore, to create, to think, and to feel." (Clynes & Kilne, 1960).

Clynes and Kline discuss some of the various physiological and psychological problems man's space travel would encounter. They determine the Cyborg will enhance man's natural functions to increase his ability in extra-terrestrial environments, lasting from a few weeks to years. Functions they discuss include Wakefulness, Radiation Effects, Metabolic and Hypothermic Controls, Oxygenation and Carbon Dioxide Removal, Fluid Intake and Output, Enzyme Systems, Vestibular Functions, Cardiovascular Control, Muscular Maintenance, Perceptual Problems, Pressure, Variations in External Temperature, Gravitation, Magnetic Fields, Sensory Invariance and Action Deprivation, and Psychoses to be identified and controlled. (1960).

Figure 5-25 NASA "The Cyborg Study" design group requirements



Source: *(Driscoll, 1963)*

Building off the Clynes and Kline research, NASA commissioned the CYBORG STUDY in 1963. The study's goal is to continue the theoretical ideas proposed by Clynes and Kline, rather than modifying the environment, to physically adapt the human body to the rigors of living in space. As written by Robert Driscoll, the CYBORG Study is a "study of man and the theoretical possibility of incorporating artificial organism drugs and/or hypothermia as integral parts of life support systems in scale craft design of the future, and of reducing metabolic demands and the attendant life support requirements" (Driscoll, 1963). Clynes, Kline and Driscoll all recognized that man physiological structure is well-adapted to terrestrial life, and from the initial NASA manned space flights of the 1960's, any future long-term extra-terrestrial endeavors require the study of how to adapt man's biological and mental facilities to operate outside the physical parameters of Earth.

FINAL THOUGHTS

This chapter reviews current, circa 2023, research, development, and practical application of where humankind is regarding Cyborgs. Some define the human transition to cyborg when using any mechanical implementation to improve capability, from a simple bicycle to the pocket computers that are today's smart devices. Following the origins of the word Cyborg, combining Cybernetic and Organism, incorporating external and internal components extending and expanding a human's capability to adapt to new

environments, this chapter presents a broad overview of prosthetics, bionic limbs, neural implants, and exoskeletons. The combining of Artificial Intelligence into prosthetics, brain-controlled interfaces and Augmented/Virtual reality long with the research into Nano-technology and neuro-interfaces point to future of where humankind could be headed as Cyborgs. Cyborgs are inevitable!

REFERENCES

Barfiled, W. (2022). *Cyber-Humans.*

Bast, M. (2014). *You've given me my body back: A Q&A with Hugh Herr.* Retrieved from TED Blog: https://blog.ted.com/youve-given-me-my-body-back-a-qa-with-hugh-herr/

BBC Click. (2017). *The man with a camera inside his eye.* Retrieved from BBC Click | Beyond Human: https://www.bbc.com/future/article/20170721-the-man-with-a-camera-inside-his-eye

Boroushaki, T., Lam, M., Dodds, L., Eid, A., & Adib, F. (2023). *Augmenting Augmented Reality with Non-Line-of-Sight Perception.* Massachusetts Institute of Technology, University of Michigan.

Britannica. (2022). *Medicine Bionics Technology.* Retrieved from Britannica: https://www.britannica.com/technology/bionics

Britannica. (n.d.). *Cyborg.* Retrieved from Encyclopedia Britannica: https://www.britannica.com/dictionary/cyborg

Brown, S. (2021, April 21). *Machine Learning, explained.* Retrieved from MIT Management Sloan School: https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained

Case, A. (2013). *Steve Mann.* Retrieved from Cyber Anthropology: http://cyborganthropology.com/Steve_Mann#cite_ref-3

Clynes, M., & Kilne, N. (1960). Cyborgs and Space. *Astronautics*.

Dann, A. (2015). *TED Project: No Human Can Ever Be Broken!* Retrieved from Avril Dann Illustrations: https://avrildannillustrations.wordpress.com/category/ted-project/

Darwin, C. (1859). *The Origin of Species.* London: John Murray, Ablemarle St.

Davis, N. (2023). *Science Medical Research.* Retrieved from The Guardian: https://www.theguardian.com/science/2023/mar/02/human-augmentation-with-robotic-body-parts-is-at-hand-say-scientists

Driscoll, R. (1963). *Engineering Man for Space, The Cyborg Study.* United Aircraft Corporate Systems Center.

Editors of Encyclopaedical Britannica. (2017). *Britannica, Health & Medicine, Anatomy & Physiology.* Retrieved from Britannica: https://www.britannica.com/science/exoskeleton-anatomy

Edwards, P. (2012). *Lockheed Martin – HULC™.* Retrieved from Peter Edwards GCIT 2012: https://peteredwards2012.wordpress.com/lockheed-martin-hulc/

Eveleth, R. (2014). *'I was blind... now I have bionic eyes'.* Retrieved from BBC's Tomorrow's Lives | Human Body: https://www.bbc.com/future/article/20140923-im-blind-but-i-have-bionic-eyes

Exoskeletons enable paraplegics to walk again. (2020). Retrieved from International Federation of Robotics: https://ifr.org/news/exoskeletons-enable-paraplegics-to-walk-again

Exoskelton Report. (n.d.). *Exoskeleton Catalog.* Retrieved from Exoskelton Report: https://exoskeletonreport.com/product-category/exoskeleton-catalog/

Ghose, T. (2017). *Human Behavior | Arts & Entertainment.* Retrieved from LiveScience : https://www.livescience.com/59470-eyeborg-project-photos.html

Gupta, A., Vardalakis, N., & Wagner, F. B. (2023). Neuroprosthetics: from sensorimotor to cognitive disorders. *Communications Biology*.

Harai, Y. (2016). *Homo Deus.* Harvill Secker.

Herr, H. (2014). *The new bionics that let us run, climb and dance.* Retrieved from TED: https://www.ted.com/talks/hugh_herr_the_new_bionics_that_let_us_run_climb_and_dance

Herr, H. (2018). *How we'll become cyborgs and extend human potential[Video].* Retrieved from TED: https://www.ted.com/talks/hugh_herr_the_new_bionics_that_let_us_run_climb_and_dance

Horner, D. S. (2008). Googling the Future: The Singularity of Ray Kurzweil. *ETHICOMP, Living, Working and Learning Beyond Technology.* University of Pavia.

Hsieh, T.-H. (n.d.). *Agonist-antagonist Myoneural Interface (AMI).* Retrieved from MIT Media Lab: https://www.media.mit.edu/dam/public/ami-images/

Jacobson, A. (2015). *Engineering Humans for War.* Retrieved from The Atlantic: https://www.theatlantic.com/international/archive/2015/09/military-technology-pentagon-robots/406786/

Kell, M. (2010). *Myvision, an Ophthalmic Journal.* Retrieved from The Eyeborg revealed: https://mivision.com.au/2010/09/the-eyeborg-revealed/

Kurweil, R. (2005). *The Singularity is Near.*

Kytaiko, A. (2023). *Evolution human to robot cyborg, history man evolve.* Retrieved from dreamstime: https://www.dreamstime.com/evolution-human-to-robot-cyborg-history-man-evolve-vector-ancestor-development-mankind-illustration-progress-primate-animal-ai-image198025128

Mann, S. (2012). *Wearable Computing as Means for Personal Empowerment.* Retrieved from Wearcopm.com: http://www.eyetap.org/defs/glossary/wearcomp/

Marinov, B. (., & Dao, T. (n.d.). *What is an exoskeleton?* Retrieved from Exoskeleton Report: https://exoskeletonreport.com/what-is-an-exoskeleton/

Marr, C. (2020). *Forced Worker Microchipping Faces Growing Preemptive Strike.* Retrieved from Bloomberg Law: https://news.bloomberglaw.com/daily-labor-report/forced-worker-microchipping-faces-growing-preemptive-strike

Max, T. (2017). *Beyond Human.* Retrieved from National Geographic: https://www.nationalgeographic.com/magazine/graphics/are-we-evolving-illustrations-stand-alone

McCarthy, J. (2006). Retrieved from John McCarthy's Homepage: http://www-formal.stanford.edu/jmc/

Merriam-Webster. (2023). *Cybernetics.* Retrieved from Merriam-Webster Dictionary: https://www.merriam-webster.com/dictionary/cybernetics

Merriam-Webster. (2023). *Cyborg.* Retrieved from Merriam-Webster.com dictionary: https://www.merriam-webster.com/dictionary/cyborg

Merriam-Webster. (2023). *Risk.* Retrieved from Merriam-Webster Dictionary : https://www.merriam-webster.com/dictionary/risk

Michalowska, M. (2021). *Proceedings of the International Online Conference.* Medical University of Łódź.

MIT Media Lab. (n.d.). *Agonist-antagonist Myoneural Interface (AMI).* Retrieved from https://www.media.mit.edu/projects/agonist-antagonist-myoneural-interface-ami/overview

Muller, C. (2022). *World Robotics 2022 – Industrial Robots.* International Federation of Robotics.

Nature. (2023). *Brain Machine Interface.* Retrieved from Nature Portfolio : https://www.nature.com/subjects/brain-machine-interface

Nichols, R. K. (2002). *Wireless security : models, threats, and solutions* .

Nichols, R. K. (2022). Section 3.0 Cyber Risk Assessments – Ryan-Nichols Equations.

Oxley, T. (2022). *A brain implant that turns your thoughts into text[Video].* Retrieved from TED: https://www.ted.com/talks/tom_oxley_a_brain_implant_that_turns_your_thoughts_into_text

Planck, M. L. (1949). *Scientific autobiography, and other papers.* . New York: Philosophical Library.

Rainie, L., Funk, C., Anderson, M., & Tyson, A. (2022). *AI and Human Enhancement: Americans' Openness Is Tempered by a Range of Concerns.* Retrieved from Pew Research Center: https://www.pewresearch.org/internet/2022/03/17/ai-and-human-enhancement-americans-openness-is-tempered-by-a-range-of-concerns/

Saikia, R. (2023). *Nanorobots.* Retrieved from LinkedIn: https://www.linkedin.com/pulse/smart-machines-real-time-monitoring-imaging-prof-dr-rhituraj-saikia/?midToken=AQEtYE5SiRnxZA&midSig=25TjcTBMBkpqE1&trk=eml-email_series_follow_newsletter_01-newsletter_content_preview-0-title_&trkEmail=eml-email_series_follo

Saikia, R. (2023). *The Possibility of AI Chip Implants in the Human Brain: Can We Merge with Machines??* Retrieved from LinkedIn: https://www.linkedin.com/pulse/possibility-ai-chip-implants-human-brain-can-we-merge-saikia/?midToken=AQEtYE5SiRnxZA&midSig=2YQctVSNOKmqE1&trk=eml-email_series_follow_newsletter_01-newsletter_content_preview-0-headline_&trkEmail=eml-email_series_follow_ne

Snyder, A. (2021). 'Empower' AMI Technique Gives New Life to Amputees. *NIH Record* .

Spence, R. (2014). The man with a camera inside his eye. (B. Click, Interviewer)

Swain, F. (2014). *Why I want a microchip implant.* Retrieved from BBC: https://www.bbc.com/future/article/20140209-why-i-want-a-microchip-implant

Swain, F. (2014). *Why I want a microchip implant.* Retrieved from BBC: https://www.bbc.com/future/article/20140209-why-i-want-a-microchip-implant

Thompson, K. (2022). *Boston Marathon survivor Adrianne Haslet returns to race with assist from Olympian Shalane Flanagan.* Retrieved from Boston.com: https://www.boston.com/sports/boston-marathon/2022/04/14/2022-boston-marathon-survivor-adrianne-haslet-shalane-flanagan/

Walters, H. (2013). *The sound of color: Neil Harbisson's talk visualized.* Retrieved from Ideas. Ted.Com: https://ideas.ted.com/the-sound-of-color-neil-harbissons-talk-visualized/

Wang, Y., Liu, S., Wang, H., Zhao, Y., & Zhang, X.-D. (2022). *Neuron devices: emerging prospects in neural interfaces and recognition.* Retrieved from Nature.com Microengineering & Nanotechnology: https://www.nature.com/articles/s41378-022-00453-4#citeas

Warrick, K. (2017). Cyborgs: Understanding and Mutual Treatment. *Principles of Gender-Specific Medicine.*, 705-715.

Warwick, K. (2000). *Cyborg 1.0* . Retrieved from Wired : https://www.wired.com/2000/02/warwick/

Zomorodi, M., Gutierrez, A., & Meshkinpour, S. (2023). *What if a brain was given technology?* Retrieved from TED Radio Hour: https://www.npr.org/2023/03/17/1163988220/what-if-a-brain-was-given-technology

6.

MACHINES HACKING MACHINES - TURING'S LEGACY [CARTER]

PREVIEW

This chapter provides an overview of how Alan Turing's legacy has contributed to our current and future technological development. He is often credited as being one of the founders of Artificial intelligence (AI) and Computer Science. Turing is best known as being part of the team that cracked ENGIMA in World War II. His early research led to the development of theoretical computer science with the creation of the "Turing Machine." This 1930's research by Turing established the roots of our modern-day computers and software. Theoretical computer science assisted with building of the Bombe, the machine that would break the code of the German WWII ENGIMA encryption machine. Alan Turing continued researching and publishing throughout his life. In 1950, he authored an influential paper titled "Computing Machinery and Intelligence.". This resulted in the "Turing Test," an applied theory to measure machine intelligence and the ability to mimic human behavior. The "Turing Test" is still in use and applied by AI developers as AI technology continues to advance and grow.

STUDENT OBJECTIVES

After reading this chapter, students should be able to do the following:

- Explain how Alan Turing's research of mathematics and algorithms led to the creation of different computer systems and a basis for developing software.
- Describe the significant impact on the field of encryption and encryption techniques used today when the Bombe mechanical device was used to crack the ENGIMA machine in World War II.
- Explain how the "Turing Test" is relevant today.
- Discuss how Alan Turing's research and creations laid the foundation for computer science and artificial intelligence.

INTRODUCTION

As one of the founders of computer science and the father of AI Alan Turing's legacy is endless. The "Turing Machine" laid the foundation for the development of modern computer architecture and the field of theoretical computer science. The development of theoretical computer science, the study of algorithms, computational complexity, and formal models of computation. Theoretical computer science gives an understanding of the fundamental limits of computation and to develop a mathematical theory of algorithms and computational processes. The cracking of the Enigma code during World War II had a significant impact on the field of encryption and laid the foundation for many of the encryption techniques used today. The process to break the German encryption required mechanical devices, such as the Bombe machine, to perform and highlight calculations. Turing had advanced cryptanalysis using statistical analysis. The protection key management was shown to be essential for future wars. The theory of the "Turing Test" went a step further to measure the machine's intelligence and skill. This gave the foundation for testing and creating artificial intelligence.

THE TURING MACHINE

During Alan Turing's two years (1936-38) at Princeton University, he cultivated the concept of theoretical computer science. Theoretical computer science is a field of computer science that studies the limits of computation and the foundations of computer science. It deals with abstract concepts and mathematical models that define the capabilities and limitations of computers and algorithms. Theoretical computer science encompasses a wide range of topics, including algorithms and computational complexity, automata theory, formal languages and grammars, and the study of algorithms for solving mathematical problems. It also includes the study of algorithms for solving problems in other fields, such as cryptography, game theory, and optimization. The goal of theoretical computer science is to understand the fundamental limits of computation and to develop a mathematical theory of algorithms and computational processes. This theory provides a basis for the design and analysis of algorithms and the development of new computing technologies.

The Turing machine is a theoretical machine proposed by Alan Turing in 1936. It is considered a mathematical model of computation and a cornerstone of computer science. The Turing machine is a theoretical machine that consists of an infinite tape divided into cells, each cell containing a symbol. It also has a read/write head that can read the symbol in the current cell and write a new symbol in that cell. The Turing machine operates in a series of steps, which are determined by a set of rules called the transition function. The transition function takes the current state of the machine, the symbol read by the read/write head, and determines the next state of the machine, the symbol to be written in the current cell, and the direction the read/write head should move.

The Turing machine can be thought of as a simple computer that can perform any calculation that is computationally feasible, given an appropriate set of rules and input. This is the basis of the Church-Turing

thesis, which states that any computation that can be performed by any machine can also be performed by a Turing machine. Alan Turing studied under Alonzo Church in 1936 at Princeton University. Prior to meeting Turing, Church conducted research on a class of functions that coincide with the intuitively computable functions that can be evaluated by algorithms and computer programs (Deutsch & Marshall , 2022). Church also provided first example of a particular significant function that is *not* computable, meaning a certain problem of elementary number theory is unsolvable: there is no way it could be solved by algorithmic means (Deutsch & Marshall , 2022). The Turing Machine demonstrates the framework for the design and analysis of algorithms and computational processes, laying the foundation for computer science.

The concept of the Turing machine can be applied to modern computing systems, and in this context, it is possible for machines to hack other machines. This can happen through a variety of means, such as exploiting vulnerabilities in software or hardware, using malware or other malicious software, or using social engineering techniques to trick a machine into revealing its secrets. In the field of cybersecurity, modern computers and networks can be vulnerable to hacking, and the development of advanced intrusion detection systems, which can analyze network traffic to identify and block malicious activities is a response to this problem. These systems can also learn from past attacks to improve their ability to detect and prevent future ones. Additionally, machine learning can be used to detect and analyze anomalies in the network to identify potential threats and can also be used to develop machine-learning-based malware detection systems. The concept of the Turing machine proves the possibility for machines to hack other machines.

ENIGMA MACHINE V. BOMBE MACHINE

As Britain faces World War II (WWII), Alan Turing's research is vital to assist in changing the course of WWII. The Turing Machine as a foundation for computer science, the first machine hacking machine event (outside of theory) occurred between the German Army Enigma Machine and the Turing-Welchman Bombe Machine leading to the end of WWII. There were several factors that played into the success of machine hacking machine.

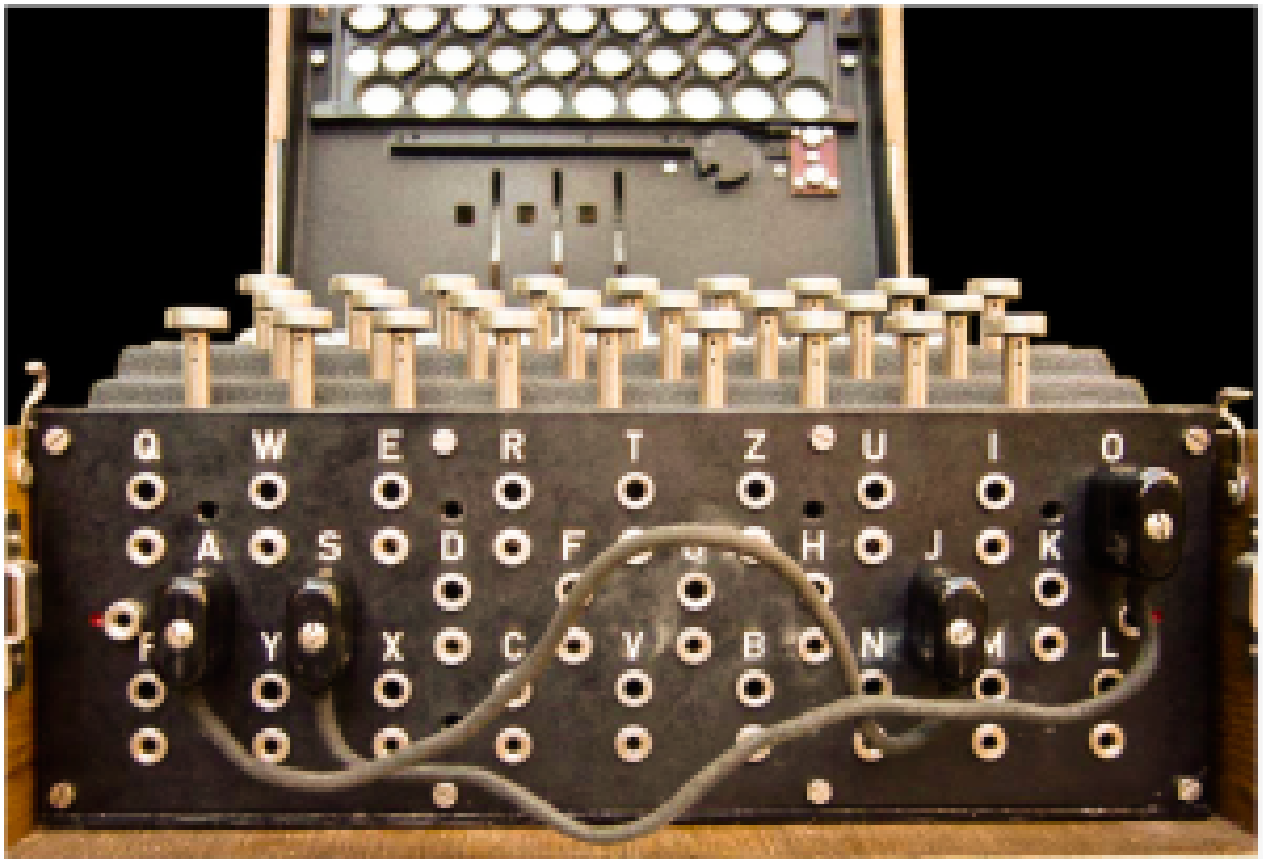
In 1938, British Secret Intelligence Service (MI6) set up the Government Code & Cypher School (GC&CS), a top-secret program at Bletchley Park. The converted private estate in Milton Keynes was home to thousands of WWII codebreakers, an elite team of mathematicians, linguists, classicists, and intelligence officers. The recruits were exceptional young men and women recruited from Britain's elite universities (Giovanni, 2021). Others were recruited by GC&CS through the newspaper, Daily Telegraph. The paper hosted a contest of solving the cryptic crossword with-in twelve minutes (Bearne, 2018). The GC&CS was organized by collection of Huts. Each Hut was contained with their own function and purpose, not to distract from one another. Alan Turing oversaw Hut 8, Naval Ultra Enigma Machine Ciphers. Gordon Welchman led Hut 6, Army, and Airforce Ultra Enigma Machine Ciphers. Hut 6 additional was the Machine Room, plus the Decoding Room and Registration Room (Giovanni, 2021). Bletchley Park's sole purpose was to crack the German Enigma Machine to save lives and stop Hitler's movement.

Figure 6-1 German Enigma Machine

Source: (Oleksiak, 2014)

The German Enigma Cipher Machine was used to send encrypted messages during WWII. For each letter that was tapped in, another letter would come out so messages would be received in code (BBC News, 2011). In 1931, Hans-Thilo Schmidt, was an employee of the German Cipher Office. Tempted by greed, Schmidt sells the instruction manual and key setting instructions to French Intelligence. With a picture and related documents of the German Enigma Cipher Machine, the French notice a unique characteristic. The Enigma Cipher Machine was widely available to others, the German version had a front plug board. Schmidt, French code name Asché, provided additional German Enigma Machine information to the French for several years to follow.

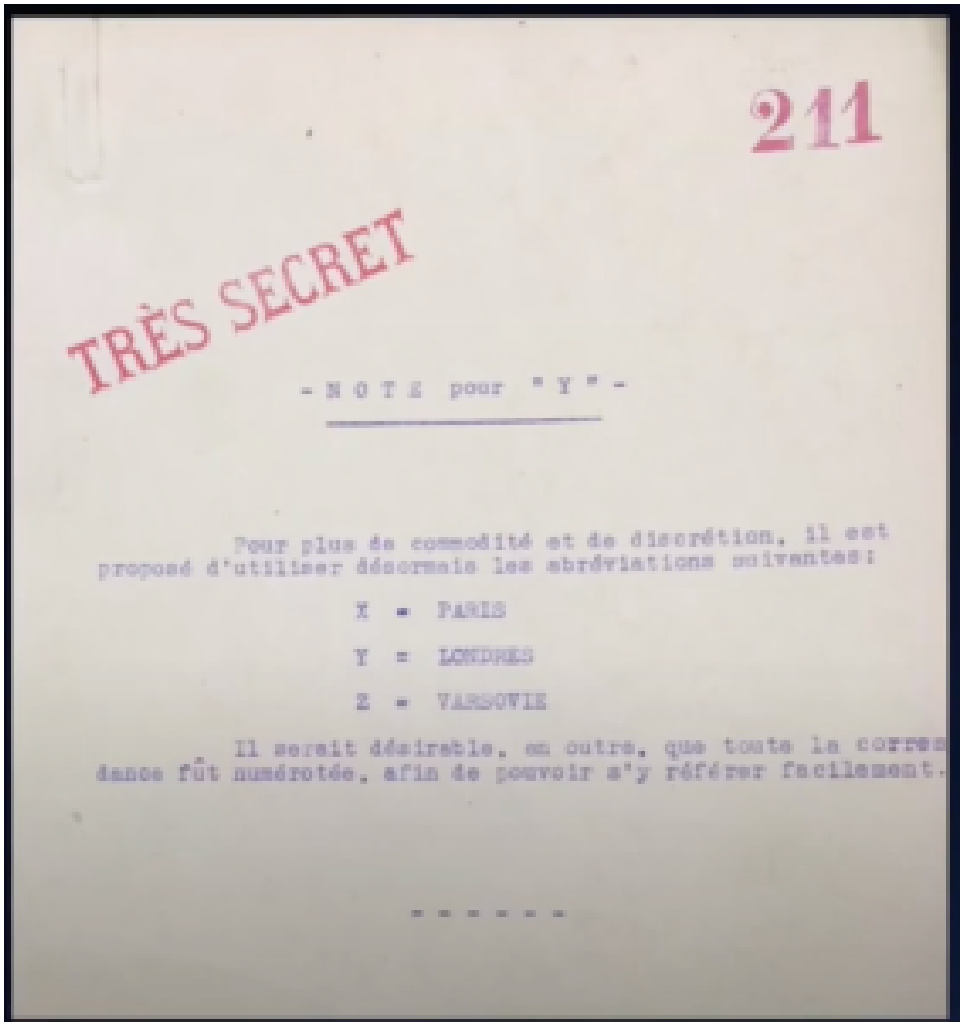
Figure 6-2 The Enigma Plugboard



Source: (Oleksiak, 2014)

In 1932, France shared the German Enigma Machine information with Poland. Immediately Polish mathematician /cryptologist Marian Rejewski began his work to break the Enigma. In 1939, the French hosted a meeting with Britain and Poland to discuss intelligence cooperation, suggesting that all three countries working together would increase the probability of breaking the Enigma. An agreement was reached on sharing communications traffic intelligence, any problems with intelligence and any breakthroughs with the Enigma. A document is drawn assigning each country a letter, X for France, Y for London, and Z for Poland.

Figure 6-3 Agreement Between France, Great Britain, and Poland



211

TRÈS SECRET

- N O T E pour " Y " -

Pour plus de commodité et de discrétion, il est proposé d'utiliser désormais les abréviations suivantes:

X = PARIS

Y = LONDRES

Z = VARSOVIE

Il serait désirable, en outre, que toute la correspondance fût numérotée, afin de pouvoir s'y référer facilement.

- - - - - -

Source: (Turning, 2016)

The French suspected Poland was not sharing their breakthroughs, their suspicion was correct. The Polish mathematician /cryptologist Marian Rejewski began to formulate equations for the Enigma rotor, leading a break into the Enigma machine since the handoff of intelligence in 1932. The British and French codebreakers did not have much success in reading the German Enigma messages. Polish authorities did not reveal their work to the British and French until July 1939 when the advance of war was getting serious in Poland (BBC News, 2011). The three countries met in Warsaw to review Poland's discoveries in breaking the German Enigma Machine. Poland's hand was forced into calling the meeting, the small collective of Polish codebreakers became overwhelmed by the German Army changing the Enigma settings each day and adding two new rotors into rotation for their Enigma Machines. The Polish explained their mockup of the German Enigma Machine, which became obsolete with the recent changes from Germany. The original German Enigma Machine had 3 rotors; rotors assisted with the increasing the difficulty of the encryption. Three rotors produced 6 permutations. Adding two additional rotors into rotation resulted in 60 permutations, strengthening the German encryption beyond the number of codebreakers in Poland. German commanders had the ability to communicated with field units encoded by messages encoded on Enigma machines and sent by wireless using

Morse code (The National Museum of Computing, n.d.). Each German high command, about 24 in all, had its own wireless network and daily key settings (The National Museum of Computing, n.d.). Additionally, Poland shared with the French and British Intelligence other codebreaking efforts to entice their allies into assisting with solving their engineering problem.

Figure 6-4 WWII Polish Mathematician Marian Rejewski

Source: (Oleksiak, 2014)

The Polish intelligence gave enough information for Turing to build a new Bombe. His approach was based on the use of 'cribs' (comparing patterns of the encrypted message and a known portion of plain text) to break the key (The National Museum of Computing, n.d.). British listing posts, Y Stations, copied the German messages and sent them to Bletchley Park to be run through the Bombe. The Bombe was working but the processing speed was inconstant and could not provide real-time data. In 1940, Gordon Welchman added a diagonal board to Turing's Bombe, (which dramatically reduced the number of invalid stops – false positives) increased throughput to the point that the Bombe became a major success (The National Museum

of Computing, n.d.). The addition of the digital board led Bletchley Park to break the first German Enigma Machine code. Coined the Turing-Welchman Bombe machine, the digital board became a permanent part of the build. By 1941, the codebreakers of Bletchley Park were understanding more of the code, a consistent combination of letters could be traced back to German military units. This was groundbreaking, now the codebreakers were able to understand the movement of the German Military, switching the allies' militaries to offense verses defense.

Figure 6-5 Bletchley Park Codebreakers

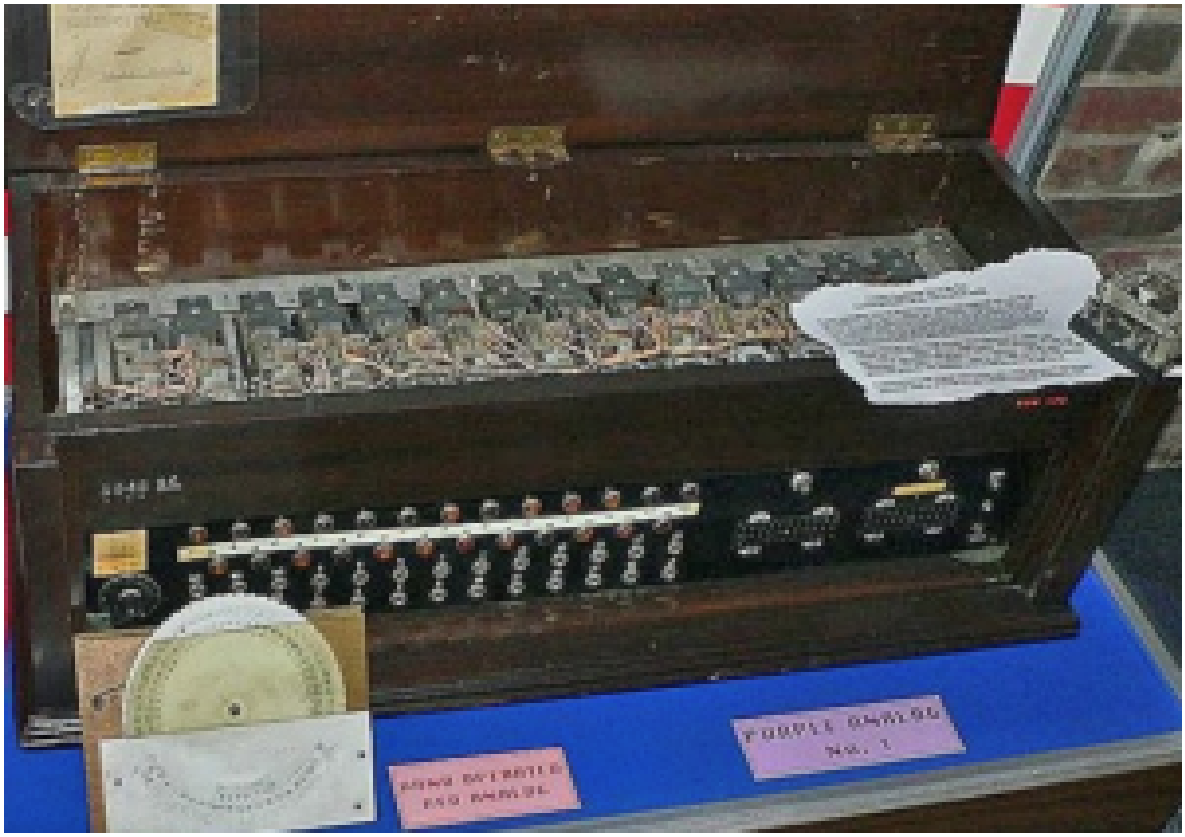
Source: (BBC News, 2020)

Figure 6-6 Polish Enigma Machine

Source: (BBC News, 2011)

The United States partnered with the United Kingdom codebreakers at Bletchley Park with the approval of Winston Churchill. The top secret "Sinkov Mission" team was led by former Brooklyn math teacher U.S. Army Capitan Abraham Sinkov, expert in Italian cipher systems (Spyscape, 2023). Other team members were U.S. cryptanalyst Leo Rosen, the Japanese cipher recreator (codename Purple); Navy Lieutenant Prescott Currier specialized in radio intelligence collection involving the Japanese Navy; Navy Rear Admiral Robert H. Weeks, experienced in communication security posts in Washington D.C. (Spyscape, 2023).

Figure 6-7 The Purple Machine

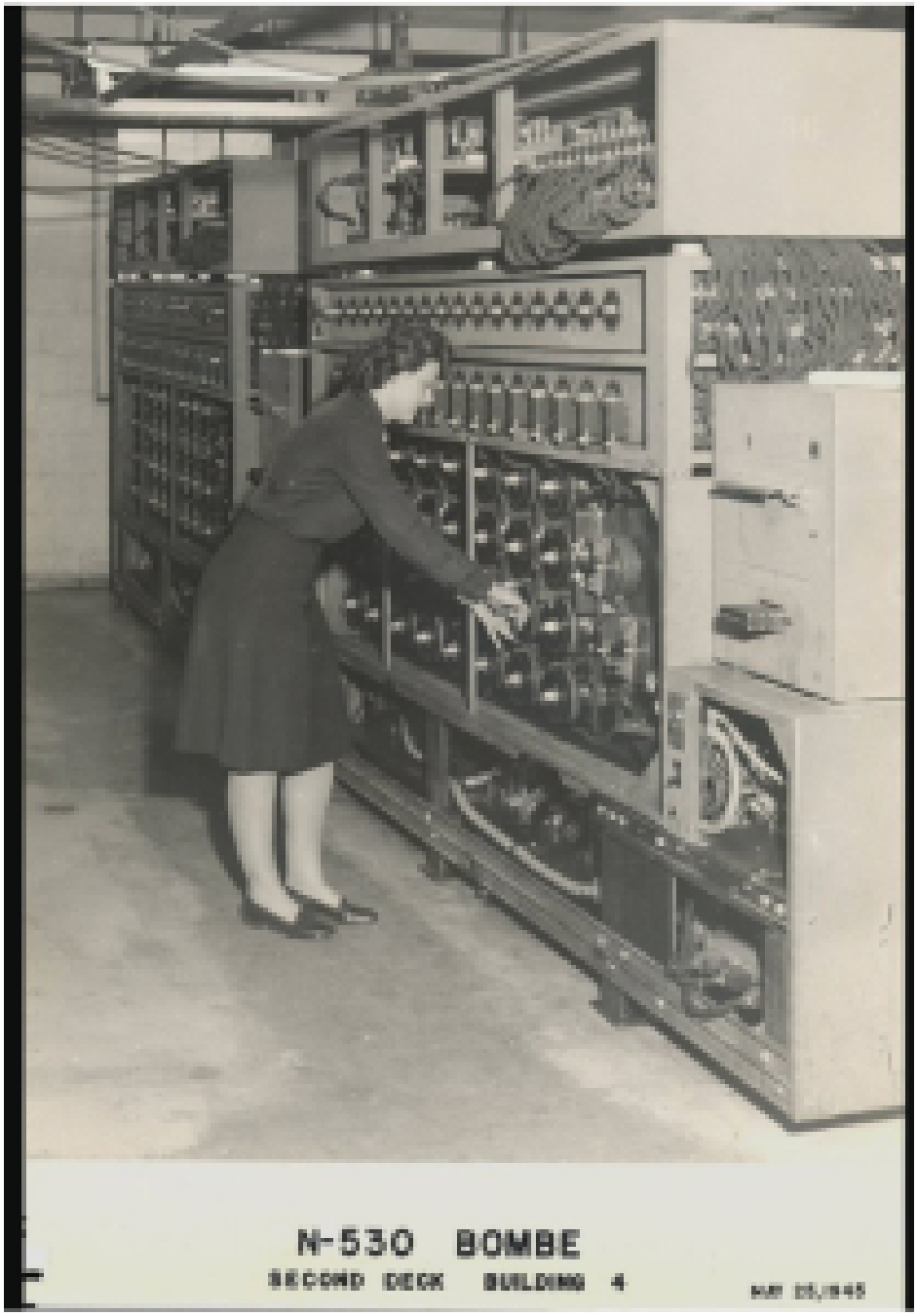


Source: (Spyscape, 2023)

Since the U.S. was not technically at war, the Sinkov team had limited access to Bletchley Park during their visit. However, Leo Rosen worked closely with the Bletchley and engineers and noted improvements for the Turing-Welchman Bombe machine. Rosen would later introduce electrical switches into the design after returning to the U.S. (Spyscape, 2023). The U.S. and U.K. intelligence bond would strengthen after the bombing of Pearl Harbor.

It is estimated 159 quintillion different German encryption permutations (The Parallax View, 2018) were read by the codebreakers of Bletchley Park (75% women), with some support of 100,000 U.S. Navy WAVES (Women Accepted for Volunteer Emergency Service) codebreakers. On May 8, 1945, the Germany surrendered, Churchill took part in the U.K. celebrations and warned that war was not over, Japan needed to be defeated. After the U.S. deployment of the Atomic Bomb, Japan surrendered on August 15th, 1945.

Figure 6-8 In Dayton Ohio, U.S. Navy women worked in three shifts a day constructing the many gears and gadgets that make up the Bombes



Source: (Wei-Haas, 2017)

ENIGMA: LESSONS LEARNED

The lessons learned of the WWII codebreakers can be applied to modern day operational security. German enigma operator's mistakes played into the hands of the codebreakers at Bletchley Park. Human mistakes were made of mundane routine combined with difficult bureaucratic processes. The enigma operators did

not understand why their role was important in the bigger picture of the war. Potentially if the operators understood the mistakes in their job posed vulnerabilities and threats for the entire German military, the operators would be aware they are mission critical. The same principle can be applied to the military leaders, respecting and applying operator feedback regarding routine.

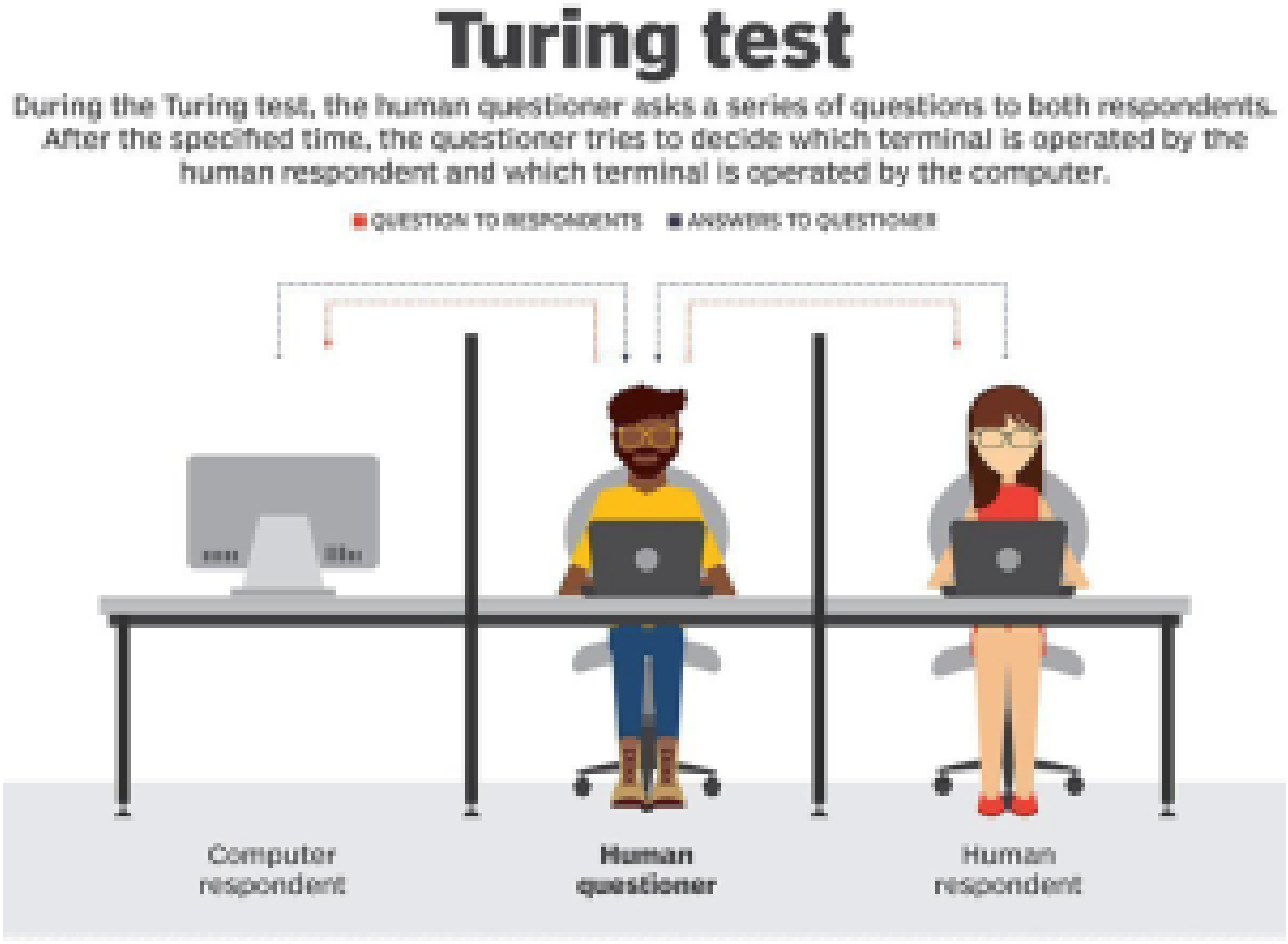
The U.K. used the combination of intelligence and military to break codes, physically surround targets and use Allies. Once a German code was deciphered there was no further protection leaving the German military's plans in plain view. Additionally with the joining force of intelligence and military, the U.K. and allies were able to attack German forces repeatedly without relief. Applying the lessons learned to modern day, clearly multiple layers of encryption with strong security architecture can prevent an attacker from getting into the "crown jewels."

Overall, the ignoring of vulnerabilities from insider threat to not evaluating the strength of security in place, can be detrimental. The lessons learned from WWII German ENIGMA contributed to cybersecurity theories of modern day.

THE TURING TEST

In 1950 Alan Turing published, "Computing Machinery and Intelligence" in the quarterly philosophy and analytic tradition journal, *Mind*. The paper introduced the concept of the "The Turing Test." The phrase "The Turing Test" is most effectively used to refer to as a way of dealing with the question whether machines can think (Stanford University, 2003). The Turing Test is considered the method of inquiry in artificial intelligence (St. George & Gillis, 2023). Turing proposed the test as a game to gauge if a computer is mimicking human intelligence under specific conditions. The test has one human judge that has a test conversation with other unseen players. The judge evaluates the players responses, it the judge is unable to detect a computer response, then the Turing Test is passed. Failure of the Turing Test would occur if the judge were able to pick out a response from a computer (University of Manchester Department of Science and Engineering, 2022). There are two groups of theory regarding the Turing Test, one believes it is obsolete another believes it is relevant.

Figure 6-9 Diagram of the Turing Test



Source: (St. George & Gillis, 2023)

The obsolete proponents of the Turing Test use bot ELIZA as an example. The ELIZA bot used psychotherapist tactics with the human. Some believe this passed the Turing Test other believe it was using trickery and played on the naïve humans. In 1991, the Loebner Prize was created, named after its founder and philanthropist Hugh Loebner, is an annual world-wide contest to evaluate the state-of-the-art in artificial intelligence (AI) (University of Exeter, 2023). The Loebner Prize is supported by several universities and organizations such as the Cambridge Center for Behavioral Studies and Bletchley Park. The Loebner Prize has recognized winning contestant bots as passing Turing Test. By recognizing the winners of this contest, a portion of the population believes the Turing Test is obsolete. Since the last Loebner Prize contest in 2019, two implementations, Google's AI LaMDA and ChatGPT have been recognized (albeit controversially) as having passed the Turing Test. (Mark,2023) (Orf, 2023) The replacement is the Marcus Test, a measure of the computer's comprehension of a television show. Also, an additional replacement to the Turing Test is the Lovelace Test 2.0. The Lovelace Test 2.0 measures the intelligence of the computer's ability to create an art artifact. Mustafa Suleyman, who co-founded the AI Lab DeepMind which was acquired by Google, argues

that the ChatGPT's large language model approach allows it to pass the Turing Test by mimicking a human yet it doesn't indicate any understanding about what the system can actually understand. He proposes a more modern Turing test based on entrepreneurship, asking the A.I. to turn $100,000 in seed money into $1million by devising an original product idea. (Shin, 2023)

Figure 6-10 Cartoon the Turing Test

Source: (Cornell University, 2023)

The other side of the population believes the Turing Test is relevant and has not been achieved as of today. This population views the Turing Test as a concept testing machines response to human speech. To have a conversation as humans do this would prove artificial intelligence. The argument is that Artificial Intelligence does not exist today. Instead, there are machines that have a response to stimulus, kicking off the process of the machine to perform an action. We know that computers can follow an algorithm to accomplish a task. However, this does not prove the machine is thinking. The summer of 2022, Blake Lemoin, a Google

engineer claimed Google had created a sentient machine. Lemoin believed the Language Model for Dialogue Applications (LaMDA), system he has been working on as sentient, with a perception of, and ability to express, thoughts and feelings that was equivalent to a human child (Reed, 2022). Google and many leading scientists were quick to dismiss Lemoine's views as misguided, saying LaMDA is simply a complex algorithm designed to generate convincing human language (Reed, 2022). Algorithms and ancillary items are too primitive to create human intelligence (Roitblat, 2021).

Could it be that we do not have artificial intelligence that can pass a Turing Test? The University Manchester Professor Steve Furber states we have yet to see any convincing demonstration of a machine that can pass his test (Furber, 2016). Professor Furber, believes we need to return to the natural intelligence, the human brain to solve for Turing's concept of "thinking" (Furber, 2016). Professor Furber is currently building a computer to support real-time models of the brain subsystems (Christopherson, 2022). Professor Furber masterpiece, 'Spiking Neural Network Architecture' known as SpiNNaker is the world's largest neuromorphic supercomputer designed and built to work in the same way a human brain does has been recently fitted with its landmark one-millionth processor core. With a price tag of £15million, 20 years in conception and over 10 years in construction starting 2006 (University of Manchester Department of Science and Engineering, 2022). Project funding began with Engineering and the Physical Sciences Research Council (EPSRC), currently funding is coming from the European Human Brain Project.

Figure 6-11 SpiNNaker

Source: (University of Manchester Department of Science and Engineering, 2022)

SpiNNaker is unique because, unlike traditional computers, it doesn't communicate by sending large amounts of information from point A to B via a standard network. Instead, it mimics the massively parallel communication architecture of the brain, sending billions of small amounts of information simultaneously to thousands of different destinations (University of Manchester Department of Science and Engineering, 2022). Professor Furber's ultimate goal for SpiNNaker's is understanding the information processing principles at work in natural intelligence. SpiNNaker could satisfy Turing's concept of "Thinking" per Professor Furber theory.

The Turing Test does not recognize functional Intelligence in a computer. The revelation of simulated intelligence by machine can be found using the Turing Test. The Turing Test can be said to reveal judgement by humans who come to conclusions using feelings, intuition, and imperfect information. The Turing Test will continue to be debated among scientists, programmers, and philosophers.

Figure 6-12 Alan Mathison Turing

Source: (Mullen, 2014)

CONCLUSIONS

Alan Turing research was influential during his time, modern day, and in the future. His early research of

mathematics and algorithms led to the creation and of different computer systems and a basis for developing software. Turing remains popular in our minds for co-creating the Turing-Welchman Bombe machine leading to the breaking of German ENGIMA encryption machines resulting in an early end of WW II. Turing's life contributions have led to the development of theoretical computer science, the study of algorithms, computational complexity, and formal models of computation. Turing was boundless with creative mathematical concepts and theories. Alan Turing remains relevant today and for the development of artificial intelligence and technology for the future.

REFERENCES

BBC News. (2011, July 14). *Bletchley Park Remembers Polish Code Breakers*. Retrieved from BBC News: https://www.bbc.com/news/uk-england-beds-bucks-herts-14141406

BBC News. (2020, October 20). *BBC News*. Retrieved from Bletchley Park's contribution to WW2 : https://www.bbc.com/news/uk-54604895

Bearne, S. (2018, July 24). *Meet the Female Codebreakers of Bletchley Park*. Retrieved from The Guardian: https://www.theguardian.com/careers/2018/jul/24/meet-the-female-codebreakers-of-bletchley-park

Christopherson, C. (2022, January 31). *ARM Community: SpiNNaker: Next-level thinking*. Retrieved from ARM Community: https://community.arm.com/arm-research/b/articles/posts/spinnaker-next-level-thinking

Cornell University. (2023). *Numb3rs 517: First Law*. Retrieved from Cornell University Department of Math: http://pi.math.cornell.edu/~numb3rs/spulido/Numb3rs_season5/Numb3rs_517.html

Deutsch, H., & Marshall , O. (2022, March 21). *Alonzo Church*. Retrieved from The Stanford Encyclopedia of Philosophy: https://plato.stanford.edu/archives/sum2022/entries/church/

Furber, S. (2016). The SpiNNaker project. *Unconventional computation and natural computation : 15th International Conference, UCNC 2016, Manchester, UK, July 11-15, 2016, Proceedings* (p. 9726). Manchester: Spring Nature.

Giovanni, J. d. (2021, July 5). *How World War II Code-Breakers Created the Modern Digital World* . Retrieved from Foreign Policy: https://foreignpolicy.com/2021/07/05/geniuses-at-war-david-a-price-book-review-bletchley-park-alan-turing-computer-technology-world-war-ii-hitler-nazis-london-blitz-battle-of-britain-luftwaffe-enigma-secret-code/

Mark. (2023, May 9). *ChatGPT Passes Turing Test: A Turning Point for Language Models*. Retrieved July 12, 2023, from mlylearning.com: https://www.mlyearning.org/chatgpt-passes-turing-test/

Mullen, J. (2014, August 19). *CNN: Alan Turing, code-breaker castrated for homosexuality, receives royal pardon*. Retrieved from CNN: https://www.cnn.com/2013/12/24/world/europe/alan-turing-royal-pardon/index.html

Oleksiak, W. (2014, July 3). *The Hacker Who Saved Thirty Million Lives*. Retrieved from CluturePL: https://culture.pl/en/article/the-hacker-who-saved-thirty-million-lives

Orf, D. (2023, March 16). *The Turing Test for AI Is Far Beyond Obsolete*. Retrieved July 12, 2023, from Popular Mechanics: https://www.popularmechanics.com/technology/robots/a43328241/turing-test-for-artificial-intelligence-is-obsolete/

Reed, B. (2022, July 23). *The Guardian:Technology:Google fires software engineer who claims AI chatbot is sentient*. Retrieved from The Guardian Technology : https://www.theguardian.com/technology/2022/jul/23/google-fires-software-engineer-who-claims-ai-chatbot-is-sentient

Roitblat, H. L. (2021, October 4). *AI Is No Match for the Quirks of Human Intelligence*. Retrieved from The MIT Press Reader: https://thereader.mitpress.mit.edu/ai-insight-problems-quirks-human-intelligence/

Shin, R. (2023, June 20). *The Turing test for measuring A.I. intelligence is outdated because of ChatGPT's wizardry, and a new test would be better, DeepMind cofounder says*. Retrieved July 12, 2023, from Fortune: https://fortune.com/2023/06/20/turing-test-proposed-update-ai-chatgpt-deepmind-cofounder/

Spyscape. (2023). *Bletchley Park: The Top Secret Mission to Crack the Enigma Code*. Retrieved from Spyscape: https://spyscape.com/article/bletchley-park-the-top-secret-us-mission-to-crack-the-enigma-code

St. George, B., & Gillis, A. S. (2023, April). *What is the Turning Test?* Retrieved from Techtarget: https://www.techtarget.com/searchenterpriseai/definition/Turing-test

Stanford University. (2003, April 9). *Stanford Encyclopedia of Philosophy*. Retrieved from stanford.edu: https://plato.stanford.edu/entries/turing-test/

The National Museum of Computing. (n.d.). *The Turing Welshman Bombe*. Retrieved from The National Museum of Computing: https://www.tnmoc.org/bombe

The Parallax View. (2018, August 1). *Bletchley Park's WWII Lessons for Today's Hackers*. Retrieved from The Parallax: https://www.the-parallax.com/bletchley-park-wwii-lessons-hackers/

Turning, D. (2016, February 1). Alan Turing Decoded: An Evening with Sir Dermot Turing (ENGIMA). (I. S. Museum, Interviewer)

University of Exeter. (2023). *LOEBNER PRIZE*. Retrieved from University of Exeter : https://loebner.exeter.ac.uk

University of Manchester Department of Science and Engineering. (2022, June 23). *Passing as a Human – What is the Turning Test?* Retrieved from University of Manchester Department of Science and Engineering: https://www.mub.eps.manchester.ac.uk/science-engineering/2022/06/23/passing-as-human-what-is-the-turing-test/#:~:text=Back%20to%20the%20future&text=Interestingly%2C%20Turing%20predicted%20that%20by,successful%2C%20and%20mostly%20through%20trickery.

Wei-Haas, M. (2017, October 5). *How the American Women Codebreakers of WWII Helped Win the War*. Retrieved from Smithsonian Magazine: https://www.smithsonianmag.com/history/how-women-codebreakers-wwii-helped-win-war-180965058/

Williams, A. (2023, June 22). *ASK HACKADAY: THE TURING TEST IS DEAD: LONG LIVE THE TURING TEST!* Retrieved July 12, 2023, from Hackaday: https://hackaday.com/2023/06/22/ask-hackaday-the-turing-test-is-dead-long-live-the-turing-test/

7.

MANAGEMENT CHALLENGES FOR MIXED HUMAN-MACHINE TEAMS [RYAN]

MANAGEMENT CHALLENGES FOR HUMAN-AI TEAMS

This chapter explores some of the challenges associated with managing teams of workers that include both humans (modified or unmodified) and machines of various levels of intelligence (smart, intelligent, or special purpose). Management is a complicated process that includes planning, resourcing, decision making, oversight, and process measurement. Executing management responsibilities necessarily means acquiring, organizing, training, and equipping the workers to do the job. In a world where humans and machines work together in teams, which means that these processes need to address the needs of both humans and machines — processes today that are done by separate groups of people with different training, skills, and job descriptions. This chapter is designed to help you understand how to begin to think about these challenges and how they fit into your life.

Note: the use of the term 'artificial intelligence' (AI) is problematic because of all the various definitions. In this chapter, no specific definition is used since it is well discussed in the other chapters.

STUDENT LEARNING OBJECTIVES

This is a philosophical exploration of a complicated topic. After reading this chapter, the student should explore these ideas further, particularly through the lens of life experiences.

PROLOGUE

A friend posited recently that good managers spend most of their time coaching, rather than engaging in the classical aspects of management (which include planning, resourcing, directing, measuring, and rewarding). In fact, she went so far as to opine that excellent managers spend about 70% of their time coaching. I asked her in response the following:

I wonder if you have considered what the effect of increased "AI"-human teams (where I use the term AI very, very loosely) might have on the role of the manager/coach? The emergence of a job that is (loosely) described as "AI

prompting" might suggest that in these mixed teams, your formula will continue to be correct, albeit expressed in different ways according to the target.

Her answer was, "*With sentience, sure. What do you think?*"

My reply:

Sentience is an interesting but unsatisfying measure. For one thing it is only indirectly measurable (via surrogate variables). But how do you detect if a thing is faking sentience? I think some mixture of sapience and agency makes a difference. The agency aspect is particularly interesting with regards to this challenge.

Sentience, as a concept, is problematic as a measure of, well, anything really. It merely means the ability to perceive or feel things. Even plants can do that. How does that advance our understanding of future issues with AIs? Sapience is only slightly better, as it implies a measure of wisdom. Wisdom itself is a difficult concept to define, much less use.

But if you elide sapience into intelligence and add agency to that, then you get a being that has some level of intelligence that approaches wisdom and has the ability to act based on its own judgment. **So this is the focus of the challenge: a machine that is intelligent in one or more aspect and which has the ability to decide if and how to act in any particular situation.** This implies more than simply following programmed logic: it implies the ability to collect data from the environment, use that data as input to a decision-making analysis, and then independently decide if and how to act based on the results of the decision-making analysis process.

So, here's the thought: if you have two equally sapient individuals, each with agency, but one is human and the other is not, how do you manage them as a team? This is where we find ourselves. And it is worth considering how we manage today, how we will manage tomorrow, and how we should plan on managing in the future, assuming that humans remain in the management position.

The technology base of the modern economy is highly advanced in information processing and supporting functions. The people who work in this economy need to be highly skilled in order to use and work with intelligent machines. To date, these two components — technology and people — have been managed through separate systems. Until recently, that separation made good sense: people are different than machines and have different needs. However, there are emerging technology trends that suggest it is time to rethink this separation. As human performance is more tightly coupled with machines, including those classed as "artificially intelligent," the approach to management needs to change. Human Resources (HR) and Machine Resources (MR) combine to create the modern workforce. Machines that collaborate with humans cannot be managed without taking the humans into account; concomitantly, humans that are tightly coupled with machines cannot be managed without taking the machines into account.

One of the interesting aspects of the thought exercise is considering how focused many managers are in removing or limiting the agency of human employees. Various human resources management techniques have been developed over time to reduce the ability of workers to act with a full, independent agency. These techniques include use of devices such as non-compete clauses, claw-back options for earned commissions, and

psychological approaches to creating "firm as family" emotional ties. As a result, one of the potential futures that must be considered is a future where the machine has more agency than the human.

The purpose of this chapter is to explore that future specifically through the lens of management. You could just as easily change the lens to that of talent supply chain, innovation, or any other organizational issue. In fact, do so. It will enlarge your appreciation of the challenges ahead.

THE ROLES OF MACHINES AND HUMANS

Humans have always used technology. The first technologies were tools, clothing, and symbols. As new technologies were invented, merged with other technologies, and improved, the dependence that humans have on technology has grown significantly. We live in artificial caves that come with artificial sunlight and artificial heat. We cook on artificial campfires, clothe ourselves in artificial skins and cloth, and communicate using artificial noise. In truth, it would be difficult for a normal person to survive if plucked out of this cocoon of technological comfort and ease that we have created.

The most recent advancements of technology assistance to human endeavors have relieved humans of the types of work that humans do not perform well or consistently. This includes repetitious mindless activities, such as factory work, and large data set analyses. As humans have off-loaded these types of tasks onto machines, humans have been freed to focus on things that machines cannot do or do poorly. However, even as humans work in areas that machines are not (currently) good for, the execution of these types of activities relies in great part on technological support. And as tools like ChatGPT continue to make inroads into the workplace, the role of "technological support" becomes more closely coupled with human efforts.

In great nation competition, technology has been adapted and invented to protect humans from harm, both in offensive operations and in defense. Unmanned systems are paired with human controllers and weapon system operators. Intelligent targeting systems guide bombs to targets. AI assistants suggest and make decisions in ways that may be fully obscured from human understanding. The idea of "human in the loop" is being replaced by "human over the loop," with the human taking on more of a role of coach or customer rather than participant.

The integration of technology into human existence has not been limited to performing tasks and serving as distancing mechanisms. It also includes integration into the human body for performance monitoring, maintenance, and adjustment. As noted in a 2012 study by the National Academy of Sciences, "Advances in medicine, biology, electronics, and computation have enabled an increasingly sophisticated ability to modify the human body." The study pointed to three general areas of technology innovation regarding the human body: "human cognitive modification as a computational problem, human performance modification as a biological problem, and human performance modification as a function of the brain-computer interface."[1]

THE NEED FOR COMBINED TALENT MANAGEMENT

In reality, combined talent management is already here, albeit in nascent form. Machines manage humans in all sorts of interesting ways, and machines are managed by humans. The various talents of human workers are judged and sorted by machines, while the various abilities of machines are integrated into workplaces according to need and potential to contribute.

During recent research into human talent management systems, a study group[2] discovered very interesting evidence of the integration of advanced technology into the process of managing humans. These integrated processes included the decisions associated with selection, assessing, and training the humans, sometimes to the extent of it not being clear how the humans would actually operate without the technology. In other words, the machines were managing the humans, at least to some level. This suggests the potential of a future of human resource management that is more tightly coupled with machine management than we might be anticipating.

The adoption and integration of advanced technology, such as artificial intelligence, into the post-industrial economy, education, and governance structures have advanced the leveraging of knowledge to make processes more efficient and more effective. The field of knowledge management has attempted to capture the challenges of collecting, curating, and spreading both implicit and explicit knowledge within these environments, with some success. However, as the integration of knowledge, both as multipliers and as external replications of human intelligence, surges forward, there must be a concomitant recognition that organizations must deal with a supply chain of human intelligence — the brain power that humans bring to the working environment. The supply chain of human intelligence includes both the acquisition and value adding of intelligence in humans (hiring, training, and educating) as well as the integration of human intelligence into machines. Writ broadly, this describes a supply chain of intelligence that integrates the human and the machine. The supply chain approach can enable enterprises to value each contribution to the value-added prospect of the enterprise, enabling enterprises to account for investments correctly and adequately in the human intelligence supply chain.

It's not just the cognitive processes of humans that are subject to supply chain like activities. The entirety of human and extra-human intelligence, either encapsulated in a human or as captured in a computer program, needs to be considered together. Humans use automation to outsource elements of intelligent activity. Alternatively phrased, humans extend their brain activity interaction with the rest of the world (other people, tools, places, etc.) by expanding their physical presence through the use of technology such as decision aids, AI, and other assistive technologies.

It is unlikely that the integration of human and technology components will cease, slow down, or reverse itself. In fact, we have seen direct evidence to the contrary, particularly as we have sheltered in place during the COVID-19 pandemic for an extended period of time, each of us learning new ways of collaborating with each other and socializing with each other. The future envisioned in The Caves of Steel[3] may be just around the corner.

Exploring the emerging issue of human-machine teams requires not just the investigation of human-machine teaming but also the supply chain of both artificial and organic intelligence. So, there are several management issues to consider. These include, but are not limited to:

- The behavioral and cognitive effects of human-machine teaming
- Issues of trust between humans and machine teammates
- Synchronization of the human and machine talent development and management systems
- The security of the "intelligence" supply chain

MANAGEMENT OF AI-HUMAN TEAMS

When most people think of AI-Human teams, they reflexively think about data scientists or other high-tech people working with and developing AIs. A much more interesting team composition to consider is the 'normal' person teamed with one or more commercial production AIs.

Consider, however, examples of more ordinary work teams: that of a janitor, a lab technician, a kindergarten teacher, or a construction worker, each teamed with AI to accomplish their respective jobs. Each of those workers has specialty knowledge related to their jobs and presumably the AI will to. How will they 'talk' to each other? How will they coordinate? It is a manager's job to make sure the working environment is appropriate to the needs of the worker (including disability issues).

A manager plans, resources, oversees, and measures the progress and success of work efforts. In order to successfully manage the human AI team, the manager (which may in fact be another AI) must take into accounts the differing needs of each member of the team. The manager hires (acquires) the talent needed, ensures each team member knows what they need to know to accomplish the job, provides the needed resources, makes the schedules, and assigns the activities. The manager also measures work performance, provides guidance on how each worker is performing, and integrates work output with other elements of the overall enterprise. It is challenging enough to do this well with only humans and dumb but critically important machines (like word processors, earth penetrating radar, or mass spectrometers). Adding what could be viewed as an alien being into that mix of personalities and technologies is very likely to result in novel challenges that are unpredictable right now.

BEHAVIORAL AND COGNITIVE ISSUES

One existing challenge associated with managing teams is observing, evaluating, and managing behavioral aspects of team relationships. We have names for different behaviors because these behaviors occur often enough to warrant consideration. Bullies, prima donnas, manipulators, shirkers, toadies, and more: each can

cause challenges in team management. If left unmanaged, each can contribute towards the development of a toxic working environment.

What types of behaviors are likely to arise from the integration of sapient machines with agency? Will there be jealousies, attempts to sabotage the work of the AI, or other behavioral challenges with the human members of the team? Conversely, will the AI subvert the efforts of the humans?

Understanding that these need to be considered and watched for in the process of creating a true human-AI team is a critical first step to addressing potential problems.

ISSUES OF TRUST

Trust is a critical component of team efforts, particularly in work efforts that require a high degree of precision. When trust is lost between team members, the overall performance of the team suffers, sometimes to the point of becoming dysfunctional.

What does a human do if they lose trust in a machine they are working with right now? The answer is normally to try to fix it — go through trouble-shooting procedures, consult the tech manuals, ask the help desk, or reboot the machine. What will a human do in the future if the human loses trust in the AI teammate? It is entirely possible that AIs will be too complicated to trouble-shoot outside of an "AI hospital" and rebooting could do more harm than good.

What will an AI do if it loses trust in its human teammate? You can't reboot a human, at least not today. Will the AI simply cease working with the human? Will the AI create an environment where the human can't successfully participate in the work processes? Will the AI damage the human in order to get it removed from the work environment? When trust is lost, it is normally for good reasons and the AI might feel like there is no option but to act in order to limit the ability of the untrusted (and untrustworthy) team member from working.

The issue of trust between team members then becomes a critical focus for managers of mixed AI-human teams. This issue becomes particularly acute when the loss of trust occurs during a fast-paced precision work situation. Consider an AI-human team operating on a human to remove a brain tumor. The loss of trust, by one member or the other, during that operation would be a potentially catastrophic problem.

THE TALENT SUPPLY CHAIN

Assuming a future where human intelligence is a desired attribute in the work environment, any Worker Resource (WR) system must consider the differences in the development of the various intelligences. For example, humans develop slowly; machines can be developed much more quickly. The needs of the work environment must be able to synchronize the time development schedules of both humans and machines in

a way that optimizes the utility of each. The strategic planning issues associated with this synchronization are staggering, given the speed at which technology, and needed future human education can change.

Additionally, there are inherent security aspects of the human talent supply chain, even though it is not fool proof. The humans developed undergo years of training and education, during which they are observable and can be assessed for trustworthiness and competency. These same aspects are not inherently part of the machine intelligence supply chain, although they could be. The integration of parts manufactured in many different parts of the world, combined to create a body in which an AI can reside, creates a universe of supply chain issues associated with the trustworthiness of parts — both as individual components and as elements of systems.

FINAL THOUGHTS

As the previous chapters in this book have demonstrated, we are headed into a future that will provide many challenges. Thinking about how humans fit into that future is an important task. Research, obviously, is needed. Another thing that is needed is a profound sense of caution. Embracing the promise of technology is critically important but it must be done with clear-eyed testing, analysis, and adaptation of the technology to ordinary human existence. With such an approach, the stars become ours to conquer.

ENDNOTES

[1] National Research Council. 2012. Human Performance Modification: Review of Worldwide Research with a View to the Future. Washington, DC: The National Academies Press. https://doi.org/10.17226/13480.

[2] Strengthening Air Force Human Capital Management. https://sites.nationalacademies.org/DBASSE/BOHSI/Strengthening-Air-Force-Human-Capital-Management/index.htm

[3] Asimov, I. (1953). *The caves of steel*. New York, Ballantine.

8.

NEUROSTRIKE - THE CYBER, COGNITIVE, NANOTECH AND ELECTRONIC GATEWAY TO MINDFULLY IMPAIRED METAVERSE [MCCREIGHT]

PURVIEW

Images of a future world where humans are engaged in lifelong phony IOT/AI enabled fantasy universe are frenetically engaged in a competitive long-term struggle with those choosing to dwell in reality for dominance. Reality is one thing, but AI enabled escapism is quite another. Youth have collectively signaled their preferences and fantasy seems likely to edge out extended excursions into reality wherein pain, setback, humiliation, and loss are prevalent. Regrettably, many under the age of 25 want that fantasy right now and cannot wait any longer for it to happen. Collegiate diversions to contemplate life's hidden meanings and study enduring global mysteries hold no power over those who cherish entertainment over education.

Capturing the attention and focus of younger people is no longer reserved for the decade after 2030. Today calibrating an illusory threat, we neither comprehend nor display adequate expertise to decipher allows the cyber experts to engineer a future we may not want to inhabit. Instead, it beckons to those who shun the random, sometimes bizarre and whimsical episodes which daily life offers. When quantum, AI and IOT [internet of things] combine in deliberate convergent ways for explicit entertainment infused among the masses who can resist or overcome its undeniable appeal. The rest of us opting out of cyber fantasyland cannot forecast what good things, perverse things and some very bad things might result. Those embarking on the risk of consuming unlimited unrestricted cyber entertainment must absorb the consequences. What warning flags or cautionary advice would dissuade those already smitten with cyber based fantasy? Can we foresee the engineered convergence of multiple technologies yielding anything but productive and beneficial outcomes? How about blending in nanotech, genomics, electromagnetics, and other technological dynamics? Should the experts pause to consider the impact or implications? What happens then? Will the net result be a better world or one where what Mankind has created via its unending curiosity an environment that eventually swallows us all up? How will our minds be affected?

THE TAUTOLOGY OF TRUSTING IN TECHNOLOGY

What does the human constantly yearn for and what steps will humans undertake to achieve that? If we are truly on a path to a better more fulfilling life versus the apocalypse, then what is the best road to be chosen? Will the current trajectory of human aspiration, global society and civilization continue as in the past or divert in a new direction? Many will put their trust in technology as a rational and objective basis for answering these questions. They will do so without very much hesitation.

Some will prefer to continue the present uneven and fate-filled course. Holding technology at arm's length attracts those doubtful the full array of expected and unexpected outcomes will be salutary. Others will reject that out of hand. Only a full embrace of all technology offers makes sense to them. Fearlessly the pursuit and support of unrestricted technology—convergent or not—is the antidote to stagnation.

Life itself needs a reboot and refocus that only objective unlimited application and investment in every aspect of technology can offer. For many this is the preferred path. Is there any doubt? Technology provides the answer to a multitude of global ills, doesn't it? Technology unchained and supported continually by visionary leadership can bring about a level of global achievement, efficiency, stability, and relative security unencumbered by managers, politicians, and professors whose inherent fleshly capabilities are limited. The future and its essential socio-technical architecture is a comfortable alternative to swallowing more of the same. It allows one to jettison the past and all the trappings of unimaginative energy which hold back human destiny.

Without too much thought we routinely invest confidence and trust in modern technology. We find ourselves comfortably minimizing any latent uncertainty when we board a jetliner or travel overseas by merchant ship trusting all will go well and safely. We abide by the assurances and confidence which positive experiences with technology have thus far conveyed. Technology itself is the pathway to a better future for all. Isn't it? It harbors good things—not woeful things—correct? We have benefitted so richly from technology over the years can its rare and periodic setbacks ever nullify its frequent successes. If technology is king who then are its servants?

We govern what technology achieves in our name and faithfully executes the tasks given to it. As such technology is our handmaiden and workhorse obedient and tireless like the horse pulling a plow or a yachtsman steering his ship. We remain unsure whether that will always be the case and we harbor some serious doubt about whether our love affair with technology will end well or badly. Bent to our will and governed by well-educated and visionary brainiacs we expect technology to take us places we could never go to or experience without it. It is a clever and deceptive bargain in any case.

Technologies we hardly imagined 50 years ago such as cell phones, hypersonics, advanced genomics, quantum computers and vehicles for transiting space are prevalent and ubiquitous. The human brain has launched and nurtured these ideas and infused these technologies in ways that cause one to ponder if the brain itself is truly without limits. We must always balance the good with the bad, the expected with the unexpected, the known with the unknown. Recognizing we can hardly see the actual end of all things that today we can only dimly grasp should enable us to admit we wander into speculation. One might consider whether

inquiries which push modern technologies into operational realms never merit a detached perspective. In effect we should insert caution—however frequently we do not. Far from being a wildly unpredictable jungle full of predators and risks embedded in nature, the decision to pursue and engage technology aggressively raises few caution flags. With applied genius, scientific rigor and professional dedication, experimental innovative excursions into modern technology are seen as manageable as controlling a drone with a joystick. In episodes like this we routinely trust the experts to know what they are doing.

Risks are inherently embedded in discovery and outcomes include both the known and unexpected. When scientists tinker with technology the rest of us have to invest some trust in their innovative theory—up to a point. After all whatever could go wrong is keenly understood within the limitless ambit of pristine human logic. Risk is always there but not to a degree that thwarts scientific inquiry and experimentation. Esteemed scientists have encountered these risks and pitfalls many times. This does compel serious thought about ramping up confidence , paring down uncertainty and expanding the art of the possible. Our brains, cognition and normal everyday neural functions are indeed spectacular and impressive. Is there a dark side that seldom gets attention? Is there a hidden dimension ignored? Is it reasonable to ask whether our brains and ordinary cognition are at risk? What are the boundaries of neuro-resilience? What threats our brains and cognition must be taken seriously? Are we asking the right questions?

We must reckon with the frontier into which technology invades a very personal space. Here we witness technology at work assisting 0r alleviating persons with emotional or mental health issues and those with traumatic brain injury. The MRI and the MeRT [Magnetic Resonance Therapy] used by neuroscientists offers a benign and helpful pathway to reduce mental stress and reductions in chronic brain problems. Here the admirable skills of public health aim to heal and restore people suffering a variety of mental health woes. It can readily be extolled as marvelous and conferring verifiable relief on those afflicted. Neuroscience remedies are wonderful things.

Our brains are also wonderful things, but they lack sustained defenses against external nefarious efforts to degrade and distort ordinary thought and cognition. To imagine a hostile nation that would subvert and redirect certain technologies to disrupt and destabilize the brain sounds ludicrous and offensive. We must note carefully and diligently that the threat emanating from this activity is genuine.

Targeting healthy brains to disrupt, impair, destabilize, and degrade their innate functions using stealthy technology sounds like Sci-Fi but it is not. We possess admirable cognitive instincts against danger, but our brains stop short of being alerted instinctively to every conceivable pitfall, calamity, and risk. There are biases and perspectives which inhabit our mind as much as creative and helpful thoughts often do. Trying to picture our brain as a target and an objective to be conquered, neutralized, and crippled by a determined clandestine foe seems alien. However, these days our attention should shift quickly to this provocative idea. It is happening to many people and has been verified as a confirmable neuroscience assault incident. Those adversely affected for years have stepped forward to claim harm and seek relief knowing a shroud of serious doubt and derision is often levied at them. These randomized attacks on human cognition and brain function are significant and have adversely affected thousands. Evidence abounds regrettably that this is happening all around us.

GRASPING THE ERA OF NEUROSTRIKE

When US diplomats first reported suspicious and bizarre brain maladies in the 2016-2018 period arising from their posting to Havana it was embraced by the media with a mixture of acceptance, doubt, and denigration. Numerous studies and reports on these incidents can be found which reflect a widening series of attacks on diplomats, US military personnel, intelligence community staff and those assigned to work in selected embassies on trade, commerce, or energy issues. (National Academies, 2020) It is far less illuminating to know the actual number of verified victims than to ponder what technology could be causing this series of cognitive impairment events which I have termed NeuroStrike. **(McCreight, Neuro-Cognitive Warfare: Inflicting Strategic Impact via Non-Kinetic Threat, 2022)**

Media and armchair experts have launched their theories rooted in doubt and denigration where various explanations for the victim's cognitive injuries have ranged from crickets to hallucinations, to emotional distress, to job pressures to indirect exposure to Zika virus environmental spraying. All of these analyses are rooted in nonfactual analysis and faulty conclusions. While the actual number of victims, even continuing today, is less important than the fact that such insidious attacks persist at all without robust detection, defense, deterrence, and defeat measures we cannot fail to see the implications of NeuroStrike technology and sophisticated cognitive warfare dominating the decades ahead. Convergent technology will continue at a pace which far exceeds our ability to understand or manage it. (McCreight & Sincavage, The Significance of Convergent Technology Threats to Geospatial Intelligence, 2019) Biochemical, neuroscience, electronic warfare, RF biophysical effects, acoustic biophysical effects, nanoparticles, and magnetic factors are blended in a debilitating convergent technology which signifies the complex NeuroStrike threat. It enables the owner of NeuroStrike to derive the quintessential leverage which ancient Chinese sage Sun Tzu observed allows one to win a war 'without firing a shot.'

Thinking about how silent, covert, and insidious neuro-modulators can impair cognitive functions, damage analysis, and decimate ordinary reasoning along with speech, memory and spatial orientation is likewise relegated to a time cloaked in distant science fiction. We know otherwise. Not because we subscribe to conspiracy theory or allow ourselves to depict a dark and dystopian future rooted in abject cynicism or submit to hallucinogenic drugs. Instead, we know history has demonstrated humanity has a deeps seated lust and enduring appetite for technology that fascinates, entertains, amuses, and simplifies life's problems. So, it is with innovative technology, complexity convergent technology, and technology that alters our sense of what is real and unreal. For many, the virtual world has more net appeal than the real one and those talented geniuses in our midst are driven to acquire it as soon as feasible.

Is this a recipe for madness? Or is it a world instead where machines, computers and AI technology do our bidding, attaining quantum insights and secures advances in social and economic wellbeing we long for perpetually? Our innate fascination with the seductive value of technology and what it potentially offers can hardly be dismissed. Worse, we lack wisdom not only in gauging the known risks we face but grappling with

the myriad unknown risks attached to any future convergent technology engineering venture. This absence of wisdom accrues to experts and scientists alike.

Intuitively we are accustomed to reliance on egghead experts. In fact, in some cases, we carelessly delegate the task of making complex decisions to further societal progress towards scientific elites. This most frequently happens because we lack proper estimates of the design, operational structure, and dynamics of the venture they are sponsoring. Do we also unwittingly assume the downstream risk and unforeseen consequences which produce potential negative outcomes for society have been assessed and homogenized to our benefit? Are we truly aware and cognizant of the persistent problems quantum computers and AI can resolve—or regrettably and inadvertently generate? If anything, enhancing NeuroStrike scope and effectiveness via quantum AI, and unlimited IOT involves risks we can hardly envision let alone regulate. Yet here we sit keenly aware of the beast at our doorstep but entranced and distracted by TV, entertainment, and vapid expressions of cultural awareness masquerading as education.

We can hardly be blamed for wanting to harness technology which improves life for all, creates abundance, economic security, improved health, upgraded quality of life and still manages to solve mankind's most acute problem while we sit back and watch movies or request another beverage. However, there is always the inevitably unexpected spate of outcomes which can be brutally damaging and then it is often accompanied by unseen or hardly anticipated costs and societal consequences. Not to worry you say. Just like TV, jetliners, computers, and plastic surgery the initial fears and skepticism are overblown and display a haphazard disregard for the promise of technology as savior.

However, if our doubts, concerns, and risk awareness are justifiable we find ourselves once again reliant on the closed shop cabal of scientists who are extremely happy to be entrusted to navigate and accelerate our collective societal wellbeing. Too often this scientific mafia of experts decides what is 'good' for all people based on their superior intellect. Supported and funded by their retinue of endorsers and policymakers who ramrod their presumptive expertise and technological preferences into massively consequential decisions affecting the unwashed masses. The naively trusting public must always endure the immediate and long-term consequences of scientific largesse absorbing the best and unseen worst of their ideas and technological ventures.

Quite simply and predictably we trust these big decisions to those experts who have earned our collective trust and civic confidence. We imagine that like a jetliner rolling down the runway at takeoff speed the entire flight will be smooth, safe, and pleasurable. It is akin to the unstated confidence we invest in medical doctors to know what they are doing, conduct proper diagnoses and find the prescription for better health. The degree of automatic trust involved is overwhelming. In like manner we have invested similar levels of trust in science and technology for their salutary effects. But is that a foolish default position for society to adopt so unthinkingly? A trusting public unaware of risk and potentially negative outcomes remains comfortable with the view science and technology is the pathway to a better life. Is it flawed to think that experts trust science, worship technology and are energetically committed to achieving all that focused brainpower and technology can accomplish? Not necessarily but it could be so.

All our flawed thinking, blind ignorance and error prone behavior is steered faultlessly toward ever more

perfect and optimal outcomes because we seek it so urgently. If the pathway to a better future resides in the convergent mix of IOT, AI, quantum, and the promises of nanotech, ChatGPT and the metaverse why would anyone aim to thwart that? As a result, we have placed our support behind mixing these technologies in explicitly convergent strategies to attain a better future. (Ortiz, 2023) In effect, we openly create an electronic gateway to a more ideal, tranquil, stable, and secure future where that formula is attractive. Many see this as a calculated gamble which nullifies the annoying diversions, errors, blind spots, and costly surprises which have historically plagued human thought. In effect this sophisticated convergent technology venture is well worth the risk—assuming we truly grasp the risks involved. Isn't that the pathway and outcome modern society and organized great nations ought to pursue with robust enthusiasm and confidence? Why should anyone raise concerns or pose cautions when engineering advanced convergent technology itself is the difference between progress and maintaining the deceptive array of gadgets we know as normal?

NEUROSTRIKE—CONSIDERING ITS CYBER DIMENSIONS IOT/CHATGPT

The immediate future in modern society is one transfixed and endlessly entertained by quantum, IOT, cyber leverage and the introduction of ChatGPT unveiled in November 2022. Expectant society welcomes all the beneficial changes and revolutionary outcomes which these technologies offer to society dimly aware that hidden and ambiguous risks are blended with –but dwarfed—by images of limitless progress. Can a hopeful society be blamed for such enthusiasm? Technological breakthroughs and skillfully mixing emerging complex and hybrid technologies earn a welcome from the general public because it contains the promise of a simplified and enhanced ordinary life.

The internet of things [IOT] dwells harmlessly in our midst and operates magically in human space as a means of communication—so we think. However, the standard cell phone is always searching for and receiving signals which it finds useful or which it has relied on many times before. Those thousands of signals drifting and bouncing among people in a crowded shopping mall stores, relays and searches other signals in that mishmash environment which the phone itself is designed to identify and connect with apart from any decision the user or owner may have. Our reliance on cell phones and the amazing IOT network behind them connecting us to devices anywhere in the world via satellite or other means purely out of sight and mind. However, we must remember our brains are truly hardwired to display sensitivity and a degree of receptivity to electromagnetic activities around us whether we are cognizant and aware or not. It raises the intriguing question of whether cellphones can be instruments of passive mind influence and cognitive control. A question best left as speculative—for now.

Cyber, IOT, quantum and ChatGPT are truly fascinating and laden with extraordinary promise. By themselves they offer grand visions of a better life for many. Caution is justified as the realities of unrestricted technology convergence is not well understood. Justifiable confidence in engineered convergence is the fundamental root of wide civic faith in what advanced technology might produce. However, where many advanced areas of scientific inquiry such as genomics, nanotech, biotech, cyber mechanics, geomagnetic

systems, and electronics are explicitly merged and engineered via deliberate convergence is fraught with risk and uncertainty. In exchange for every conceivable outcome that is valuable and beneficial there is a hidden, unexpected, and ambiguous array of risks. Worse, our collective ability to estimate and foresee all adverse and dangerous outcomes from technology convergence is opaque and often delusional. This is the central dilemma and evokes a security nightmare which is embedded in a headlong race to engineer convergence of IOT, quantum and ChatGPT.[Generative Pretrained Transformer] (BROWNE, 2023)

It is simply because all possible, unexpected, secondary, and downstream adverse consequences of such deliberate engineering symbolize a level of trust which society can ill afford. Traditional reliance on science and technology experts to overcome these shortfalls and hidden risks displays a level of misplaced confidence which is dangerous. This is especially troublesome as our enemies, rivals and foes have no compunction about engaging in this odyssey of convergent engineering because they seek to secure an invincible strategic advantage.

The explicit convergence of these technologies contains zero risks according to some critics who see benign text-based regurgitation of massive databases, an inability to persuade, influence, reason or imagine in complex cognitive operations equivalent to the human brain. Just blending these innovative technologies includes a manageable set of risks they say where a system defaults to a trove of stored data and facts. However, the threat involved is clearly insidious. This makes the issue more complex as those regimes which threaten our future security will pursue insidious convergent engineering to leverage their strategic projection and power. We understand the explicit blend of IOT, cyber, AI and ChatGPT contains these risks

–there are no operational, legal, or ethical boundaries [no moral corpus]

–it does not yet acquire self-aware capabilities but eventually could do so

–can potentially acquire competitive analysis and critical thinking

–it is potentially capable of blended deep fake misdirected phony communication

–it retains the capacity to generate deceptive, fraudulent, and incorrect decisions

–it can misguide and misdirect decisionmakers who rely upon it

–it is not impervious to external hacking and anonymous external control

In effect, the engineered blend of IOT, cyber, AI and ChatGPT fails to convey to its human overseers the inherent capacity to transparently view the good, bad, and ugly of its internal operations, focused queries, and generative outcomes. Building safeguards or kill switches into the convergently engineered mix of these technologies does not appear to be under consideration. But it should be. The merger and explicit convergent engineering of ChatGPT, quantum, IOT and cyber over the next few years contains risks and unseen consequences which even the experts cannot fathom.

In 2014, **Elon Musk called AI humanity's biggest existential threat** and compared it to demonizing the devil, "One of the biggest risks to the future of civilization is AI," Musk told attendees at the 2023 World Government Summit in Dubai, United Arab Emirates, shortly after mentioning the development of ChatGPT. "It's both positive or negative and has great, great promise, great capability," Musk said. But he stressed that "with that comes great danger." More recently he mentioned at that summit that we lack skilled

and sophisticated appreciation for its hidden risks—not just its attractive benefits. *Elon Musk, who co-founded firm behind ChatGPT, warns A.I. is 'one of the biggest risks' to civilization (Browne, 2023)*

Merged elements of ChatGPT, IOT, cyber, and other convergent technologies is not only happening now but will continue to happen in the unrestricted wild west wide open space that nurtures creativity, innovation, and free thinking. Nations oblivious to ethical constraints and mindful of its strategic leverage will seek to expand and invest in these dangerous convergent mixes. Worse, terrorists, criminal enterprises and proxy guerilla warfare states can expect to acquire this capability—or rent it—for their own nefarious purposes. Laid back society snoozing comfortably amidst NETFLIX, Grubhub, endless video games, fitness activities, mindless Grammy infused music tsunamis and Tik Tok will never see it coming. It is here already. But the dazed confused clueless will likely remain entranced and unfocused mired in staggering narcissism consuming hours of their own entertainment as US national security is exchanged for escapist relaxation.

Collaboration among like-minded criminal experts will also open the doorway to installing nanotech issues and stealthy neurotoxins where it is most beneficial to them. If you imagined cocaine and fentanyl was poisoning youth just picture a generation turned into Tim Tok zombies unable to sense when their wellbeing and security is in jeopardy. Will the West truly awaken from a woke stupor in time? What about our enemies, foes, and rivals? What leveraged opportunities exist for the bad guys to redirect these technologies against us? What conceivable countermeasures will limit their work?

The essential warning derives from a fundamental awareness of how our bodies, brains and internal systems respond to electromagnetic waves, signals, and influences. Gateways to crafty external human exploitation and nefarious misdirection within the brain and its cognitive subsystems starts with a keen awareness of how electromagnetic phenomena interact with our brains and nervous systems. We know that transcranial magnetic stimulation (TMS) is a technique used to induce a short-term interruption of normal activity in a restricted area of the brain caused primarily via rapid changes using a strong magnetic field near the focus of treatment activity. Modern technology, including nonionizing radiation from power lines, wireless devices, cell phone towers is ubiquitous in our society and unavoidable. Along with that are risks arising from extremely low frequency electromagnetic fields (EMF) which routinely surround home appliances as well as high-voltage electrical transmission lines and transformers. Evidence of adverse health effects from EMF, including its controversial influence on the brain, ranges from studiously inconclusive to menacingly harmful. Few experts today wish to conclusively state that continuous EMF exposure is a genuine health hazard. However, we do know that exposure to elevated levels of non-ionizing energy, such as at radio wave frequencies, can potentially damage the structure and function of the nervous system. In some ways the perverse politics of environmental science mitigates a deeper dive into human health implications as the sacred agenda of those who express alarm versus those arguing for benign effects cannot readily agree. (Staff, 2017)

Hence there is ample room for caution when considering the next neurological effects of electromagnetic factors and technologies on human brains. Does that issue stop the application, research and innovation of such technology given this caution? Not really. We are left to isolate and study what the net impact of

electromagnetic technologies may be in both immediate, long term and their latent effects**.** (WHO -Staff, 2016) (Zwoinska & al., 2015) (N.J.Cherry, 2003) (Tennenhouse, 2018)

DEALING WITH THE COGNITIVE, NANOTECH AND THE ELECTROMAGNETIC GATEWAY

Humans are distinctly composed biophysically and biochemically as repositories for electromagnetic activity and the record of human sensitivity to, and influence by, electromatic factors is beyond debate. There is little if any debate about the nature of human sensitivity to and reaction to electromagnetic fields [EMF]. The intensity of electromagnetic radiation in the human environment emanating from these fields– which are ubiquitous and normally found in developed areas—are both significant plentiful in human health terms. Normal EMF impact on living organisms derives from its direct tissue penetration. More specifically, the nature of our brains as a biological organ automatically includes a degree of electromagnetic sensitivity and responsiveness to EMF. Scientific theory and research into human intelligence notes that in order to retain intelligent thinking and sustain cognitive systems there needs to be a constant, globally available, synchronization system that continuously stabilizes the brain. Here the significance is found in the electromagnetic signaling system, supported by a biochemical system. EMF exerts both a thermal and nonthermal effect on brain tissue and its effects on other parts of the body [nervous system, endocrine system, visual system, cardiovascular and immune systems] are well established. More specifically EMF radiation is reported to affect the central nervous system, brain chemistry and histology, and the blood-brain barrier. We also understand limited medical applications of EMF for treatment and diagnostic purposes found in the electroencephalograms (EEGs) and MRI [magnetic resonance imaging] used to treat neural disorders are commonplace. Repurposing and re-engineering these technologies for harmful, disruptive, and damaging effects is just as real.

Effects of pulsed and sinusoidal ELF fields on the electrical activity of the nervous system have also been studied extensively. While only high-intensity sinusoidal electric fields or rapidly pulsed magnetic fields induce sufficient current density in tissue to alter neuronal excitability and synaptic transmission or to produce neuromuscular stimulation their net effects at verified intensities are beyond dispute. When a person focuses attention or tries to remember something this activity fires thousands of neurons simultaneously at the same frequency generating a wave — but at a rate closer to 10 to 100 cycles per second. Along with the brain the heart is the largest and most potent electromagnetic field inside the body exceeding brain electromagnetic sensitivity by 60 times.

It is well known that weak EMF could cause all sorts of dramatic non-thermal effects in body cells, tissues, and organs. The observed symptoms are hardly to assign to other environmental factors occurring simultaneously in the human environment. Although, there are still ongoing discussions on non-thermal effects of EMF influence, (WHO) has classified radio electromagnetic fields as potentially carcinogenic. Electromagnetic fields can be dangerous not only because of the risk of cancer, but also other health problems,

including electromagnetic hypersensitivity (EHS). Electromagnetic hypersensitivity (EHS) is a phenomenon characterized by the appearance of symptoms after exposure of people to electromagnetic fields, generated by EHS is characterized as a syndrome with a broad spectrum of non-specific multiple organ symptoms including both acute and chronic inflammatory processes located in the skin and nervous systems, as well as in respiratory, cardiovascular systems, and musculoskeletal system.

When nanotech aspects are added to EMF influences available research shows high risks of ambient neurotoxicity exists not only from nanotech in foods, the environment and within medical treatments such as vaccines. This is not claiming a deliberate and perverse conspiracy to poison people and render then silent bio-transducers of external ELF signals. Instead, this is simply to draw attention to the ramped-up risk for human health based on the presence of nanoparticles in various aspects of our normal lives dwelling covertly there largely without our knowledge or consent. So, ELF by itself generates many legitimate human health questions but when paired with the existence of nanoparticles in the environment, our bodies, and our food we may want to pause and consider its impact and ramifications on cognitive degradation issues, brain biochemistry and the overall degree to which our DNA has been altered in ways that fundamentally change our humanity. We know painfully well that anxiety, depression, and even self-harm can be linked to youth saturation with social media technology. Again, this is not aimed to condemn nanotech but to shed light on its prevalence in our society, ordinary social media, and diet in order to highlight the studies which underscore human health risks and suggest we need to know more about its borderline toxicity. In effect, our collective combined trust juxtaposed with our ignorance of nanotech complicates a rational analysis of its insidious contributing impact. (WHO – Staff, 2017)

Part of the electronic gateway facilitating NeuroStrike is the obvious nexus between cyber, AI, quantum and space platforms which send, receive, and resonate electronic signals enabling long distance transmission of allegedly benign but potentially harmful RF and electromagnetic energy which has the capacity to injure or impair cognitive functions. While the era of precise targeting of humans in large groups—i.e., cities, buildings or gathering places—all at once in the form of a planned attack seems remote. To many people it smells of borderline Sci-Fi antics gone amuck. However, creativity in this sphere of research admits a wonderfully complex convergent matrix of integrated technologies creating a pathway for its eventual appearance along with a few unexpected issues. It is not far-fetched to imagine satellite leveraged EMF directed to clueless cell phone users or equivalent signals disruptive of normal synaptic and dendrite connectivity inside the brain. Neural waves contain low levels of magneto-electronic activity, and we must acknowledge that many modern high EMF-emitting satellites in space which are being used to enhance internet speed, video surveillance and communication here on earth can exert that effect whether intended or not.

In 2012 chemists at New York University (NYU) created a nanoscale robot from DNA fragments that walks on two legs just 10 nm long. This so-called “nanowalker,” with the help of psoralen molecules attached to the ends of its feet, takes its first baby steps: two forward and two back. Its creators envisage a future molecule-scale production line, where molecules are shifted until the right location is reached. In this unique way a nanobot injects chemistry like “spot-welding” on a car assembly line. This is a decent example of “biomimetics,” where

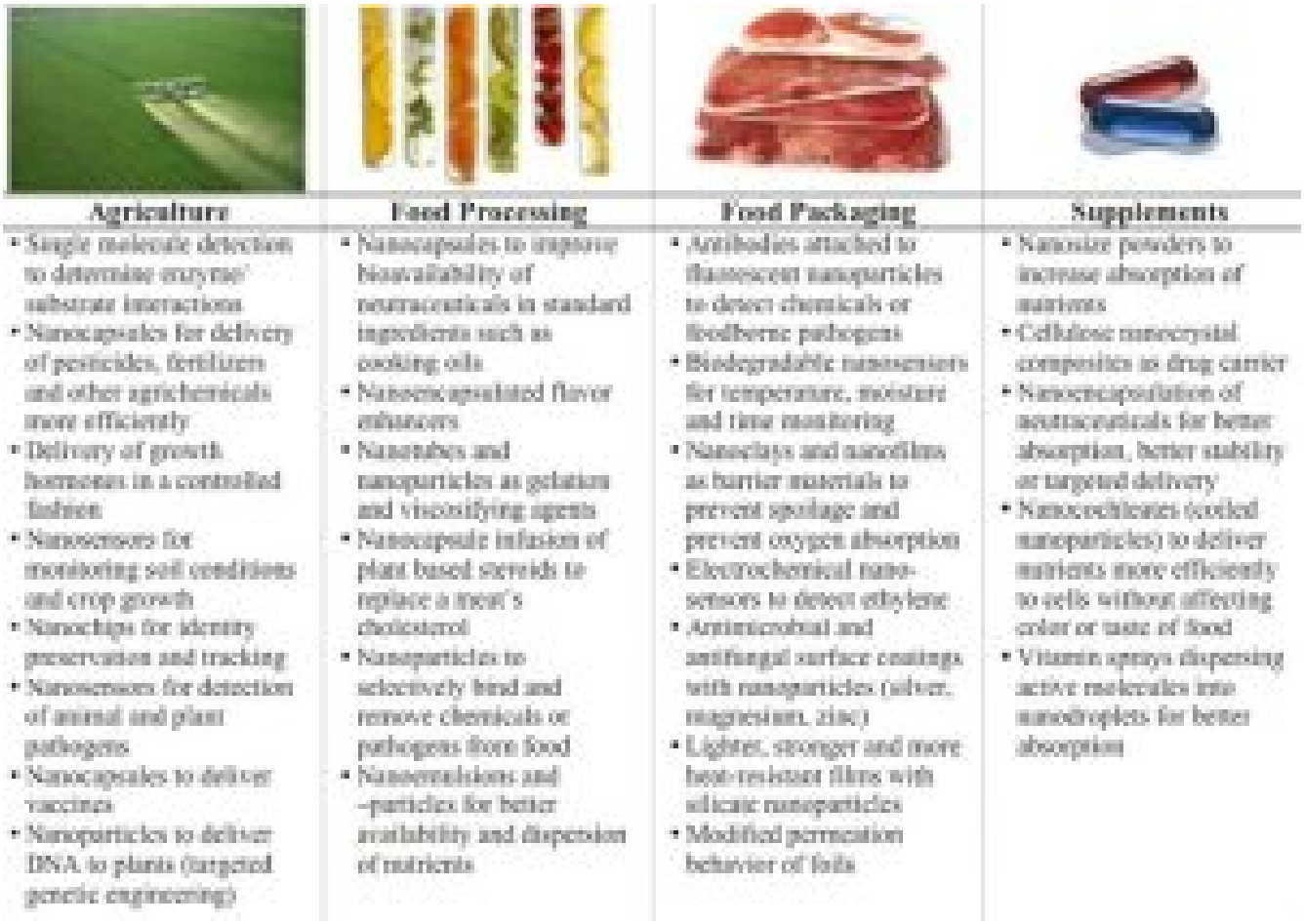
with nanotechnology they can imitate some of the biological processes in nature, such as the behavior of DNA, to engineer new methods and even improve them. So, while its medical benefits are clear, the perversion of such science for insidious and damaging purposes by nefarious actors and state sponsored enemies is also reinforced.

Recently a study published in 2022 in the Journal ***Neurology*** found that a higher daily intake of ultra-processed foods was associated with a substantially higher risk of dementia. The researchers were also able to determine that substitution of some ultra-processed foods with unprocessed or minimally processed foods was associated with a lower risk of dementia. In that study 72,000 participants were identified from the UK Biobank and all participants were at least 55 years old and did not have dementia at the start of the study. Participants were followed for an average of 10 years, during which they filled out questionnaires regarding their diet which included processed foods. By the end of the study, 518 people were diagnosed with dementia. The controversy over nanotech, including independently credible assessments of its actual risks, always confronts supporters and detractors. The WHO recently went on record as well saying,

"*The properties of nanomaterials, and of engineered nanoparticles in particular, have raised concern about unwanted or unexpected interactions with biological systems, which could result in adverse consequences to human and ecosystem health. Though rapidly growing, knowledge on these aspects is limited and many uncertainties remain.* ***" (McMillen, 2015)***

So, the unanswered questions about nanoparticles in food, their net impact on how the body and brain store and contend with their presence and the implications of stored nanoparticles in terms of human health is a subject not often addressed or discussed among major media. So, we are left to speculate about the interactive aspects of nanotech embedded as it is with RF, electromagnetics and other technologies this far mentioned on human neurological health. For example, the chart below simply illustrates a portion of the nanotech effect in our food supply. (Ghebretatious & et.al., 2021) (Gaidos, 2015) (Sahdev & et.al., 2014) (Nature Reviews – Staff, 2021) (centerforfoodsafety.org – Staff / Editorials, 2023)

Figure 8-1: Extract from Nanoparticles in Food Raise Safety Questions



Agriculture	Food Processing	Food Packaging	Supplements
• Single molecule detection to determine enzyme/ substrate interactions • Nanocapsules for delivery of pesticides, fertilizers and other agrichemicals more efficiently • Delivery of growth hormones in a controlled fashion • Nanosensors for monitoring soil conditions and crop growth • Nanochips for identity preservation and tracking • Nanosensors for detection of animal and plant pathogens • Nanocapsules to deliver vaccines • Nanoparticles to deliver DNA to plants (targeted genetic engineering)	• Nanocapsules to improve bioavailability of nutraceuticals in standard ingredients such as cooking oils • Nanoencapsulated flavor enhancers • Nanotubes and nanoparticles as gelation and viscosifying agents • Nanocapsule infusion of plant based sterols to replace a meat's cholesterol • Nanoparticles to selectively bind and remove chemicals or pathogens from food • Nanoemulsions and –particles for better availability and dispersion of nutrients	• Antibodies attached to fluorescent nanoparticles to detect chemicals or foodborne pathogens • Biodegradable nanosensors for temperature, moisture and time monitoring • Nanoclays and nanofilms as barrier materials to prevent spoilage and prevent oxygen absorption • Electrochemical nano-sensors to detect ethylene • Antimicrobial and antifungal surface coatings with nanoparticles (silver, magnesium, zinc) • Lighter, stronger and more heat-resistant films with silicate nanoparticles • Modified permeation behavior of foils	• Nanosize powders to increase absorption of nutrients • Cellulose nanocrystal composites as drug carrier • Nanoencapsulation of nutraceuticals for better absorption, better stability or targeted delivery • Nanoclathrates (coated nanoparticles) to deliver nutrients more efficiently to cells without affecting color or taste of food • Vitamin sprays dispersing active molecules into nanodroplets for better absorption

Source: (Gaidos, 2015)

As a direct consequence we now have reason to raise concerns about IOT, cyber, quantum computers, nanotech, EMF, and related substances which form an arguable electronic gateway into human mental functions, cognition, and brain health. Apart from marvelous and beneficial aspects of medical research and scientific inquiry seeking to blend these technologies into better human health we understand the covert engineered diversion and perversion of these technologies for impairing cognition and degrading neurological health is plainly wide open to exploitation by bad actors. This confers an entirely new meaning to the conventional term 'brainstorm' which does not explicitly refer to the lightening quick appearance of a great idea or insight Instead it depicts the covert insidious destruction and degradation of cognitive health, neurological wellbeing via external nonkinetic technologies which exploit neurobiological vulnerability.

Worst of all we find it difficult to ascertain sponsored government or industry hosted objective studies which outline the impact, risks and consequences of engineered technology convergence involving these disparate systems on the human body and brain. Is this yet another area where trusting the experts and allowing periodic government scrutiny and oversight supply the margin of safety, we consumers expect? What entity provides the safeguards to create speed-bumps and guardrails around the explicit mixing of technologies without examining the immediate and long-term effects of their engineered combination?

So, we are left to ponder the degree to which social media and pervasive influence factors such as Tik Tok. Aside from its appeal as entertainment, serving as a platform for exchanges of video material among people, it provides a subtle but powerful impact on human cognition especially among young adults whose brains are still undergoing cognitive growth and biophysical maturation. Their brain chemistry and neurological stability are still developing and yet that offers the ripest and most delectable target for Tik Tok designers to exploit.

Tik Tok symbolizes and reflects a wider confluence of exploitive technologies having a measurable effect on young brains, perceptions, attitudes, and behaviors which is still regarded as benign and annoying by many adults and our own government. Our Congress is focused on the issue as Senators Hawley of Missouri and Rubio of Florida have proposed bills that would bar Tik Tok from government IOT devices. In addition, Senators Blumenthal of-Connecticut and Moran of Kansas teamed up to demand the Biden administration impose a wall between TikTok's U.S. operations and its Chinese parent company, ByteDance. A Senate hearing urged TikTok CEO Shou Zi Chew "to consider his platform's harm to a generation of Americans." "TikTok is digital fentanyl," said Rep. Mike Gallagher, R-Wis., the chair of the new House select committee in China. (Scott Wong, 2023)

Judging from prevalent effects which social media has on young people and adults we must draw renewed attention to its indirect neurological influences which are detrimental. Tik Tok illustrates the almost hypnotic influence which that platform has on youngsters and its ability to trigger, support, and encourage dangerous and destructive behavior such as the various and infamous Tik Tok challenges' which so often result in physical harm to those succumbing to its Ethernet whims. A 2021 study on TikTok's specific neurological effects examined how Douyin, China's TikTok equivalent, affects Chinese college students' brains. It found that watching personalized, algorithm-selected videos ***activates reward centers in the brain*** much more than watching random videos that have not been chosen specifically for the viewer. (Miller, 2022)

In a 2022 Harvard medical review of the issue involving Tik Tok it was found that the first known examples of social media-induced sociogenic illness were recognized in the period 2020-2022, a time coinciding with the pandemic. Neurologists began seeing increasing numbers of patients, especially teenage girls, with unusual, involuntary movements and vocalizations reminiscent of Tourette syndrome. After ruling out other explanations, the tics in these teenagers seemed related to many hours spent watching TikTok videos of people who report having Tourette syndrome and other movement disorders. Posted by social media influencers, these videos have billions of page views on TikTok; related videos are available on YouTube and other sites. (Shmerling, 2022)

Indirect but effective neurological disruptions and displacement of normal cognitive functions tied to the visual, auditory, and routine sensory ingestion of social media such as Tik Tok on a regular basis indicates more must be done to sort out any hidden NeuroStrike factors and injurious elements of these media. We lack a comprehensive understanding of their net immediate, long term and covertly embedded impact on young minds and whether they open the door to other forms of external influence, manipulation, or control. Being naive about this threat and separating it conveniently from other influence technologies such as AI, quantum, cyber, nanotech and EMF is a dangerously narrow-minded strategy which thwarts a comprehensive

strategic assessment of its genuine power. We do not know enough to provide cautionary warnings which are preventative and timely for those most likely to be affected.

The central task is not to raise alarms and point to unmanaged risks arising from the explicit and deliberate blending of these technologies. Our goal is to pinpoint our innate vulnerability to the silent hidden and perverse engineering of these technologies for which we lack strategic warning, adequate defenses, robust deterrent measures, and operational strategies to nullify and defeat those who would wield such damaging technology against us. Opportunities for enemy interests to magnify the scope, scale and effect of these insidious technologies are unlimited for several reasons

- We are focused on and distracted by glossy kinetic high dollar defense systems
- Evidence of deliberate NeuroStrike technology in enemy hands is unconvincing
- We lack hard facts about the exploitable neural pathways for NeuroStrike
- We lack consensus on candidate technologies which comprise NeuroStrike
- We are unable to accept that enemy interests have perfected NeuroStrike
- We are far from finding powerful countermeasures to nullify NeuroStrike

The key challenge after 2022 is discerning the nature, scope, scale, magnitude and focus of enemy NeuroStrike capabilities. We must devise effective deterrent and offsetting technologies ourselves to diminish a threat that has been ripening and maturing for at least a decade. Military and civilian leadership is at critical risk that NeuroStrike will only become more sophisticated as time unfolds and its damage to larger groups of people is manifest. Building defenses is important but even more so is the task of attaining resilience against it.

BUILDING NEUROSTRIKE RESILIENCE IN THE MIDST OF TECHNOLOGY TSUNAMI

When one imagines a future replete with modern state-of-the-art technological breakthroughs and emerging complex and hybrid technologies the general public welcomes anything which simplifies and enhances ordinary life. However, where many advanced areas of scientific inquiry such as genomics, nanotech, biotech, cyber mechanics, geomagnetic systems, and electronics are explicitly merged and engineered via deliberate convergence into something never before seen our collective ability to estimate and foresee adverse and dangerous outcomes is opaque and ambiguous. This is the central dilemma and security nightmare which a headlong race to devise, develop and sustain an ill-defined Metaverse includes.

Using a mix of the most advanced science and technology systems and platforms to create a faux parallel cyber grounded reality esteemed and admired as more inherently attractive and beneficial than reality itself. The quest for a metaverse where no organizational, personal or government entity can assume primordial governance and creative ownership of it opens the door to insidiously dangerous mischief where our neural and behavioral safeguards and intuitive autonomous systems are outmaneuvered. It creates to a degree, so far

unanticipated or expected, an evolving appetite for dwelling in the allegedly majestic and fantastic environment which the metaverse promises to establish.

NEUROSTRIKE: A METAVERSE IMPAIRED MINEFIELD

The metaverse is a set of virtual three-dimensional spaces where you can share immersive experiences with other people even when you cannot be together. It will be inherently social; you will be able to hang out with friends, collaborate with colleagues, learn, shop, and create – among other things. Its most enthusiastic supporters and fanatical endorsers cannot see any downside to the emergence of the metaverse and welcome its arrival warmly as a life experience enhancing experience.

Being mindful the metaverse swallows up, replicates, and substitutes itself for reality with seductive immersion in V/R and A/R, humans are ill equipped to divert their attention away from so attractive a source of faux enlightenment. Here it is truly insidious qualities are revealed as deftly skilled AI, quantum and IOT engineers achieve a parallel experiential universe more appealing and satisfying than real life itself. One must accept the fact that those wishing to dwell inside the metaverse will always be open to its invitation and some will enter for a brief period and be deluded while others will opt to remain there much longer. The deceit is grounded on the principle that access to the metaverse is not exclusively by their own choice as any would believe. Instead, just as the maturation of quantum, AI, IOT, nanotech, neurobiological factors, EMF, Magento-biology and NeuroStrike demonstrate it is orchestrated externally as a covert weapon of influence destabilizing leaders, managers, commanders, and everyday people.

A healthy dose of skepticism seems warranted here. It is attractive because it offers an escapist gateway into a faux reality that allows an endless series of fantasy adventures and unlimited entertainment experiences which can be terminated easily by simply unplugging form the program or removing the special V/R equipment. But wait a minute!! The metaverse is not just VR! It is not just one dimensional. Those metaverse junctions and entry ports will connect the person with AR glasses and launch them into a world of unrivalled imaginary experiences in dreamlike quality where the person actually sees themselves operating in that virtual environment. One of its chief sponsors and supporters has said, "...there will be a real sense of continuity where the things you buy are always available to you." **(**Shah, 2021) Other metaverse advocates say, ".the metaverse will be an infinite realm that blankets both the physical and virtual worlds. At its core will be a self-contained economy that allows individuals and businesses to create, own or invest in a range of activities and experiences. Like the internet, it will not be just one thing–but several layers of different technologies, products, and languages." (NOBELL, 2023)

They argue vehemently that the metaverse bridges physical and digital realities in ways where the interface offers a spatial version of the Internet . . . Ideally, the metaverse is highly customizable and as separate or integrated into our physical realities as necessary—and desired. Therefore, the metaverse experience can be altered from the individual's point of view and shaped or curated by any number of agents—whether human or A.I. The metaverse, together with our physical locations, forms a spatial continuum. The very materials of

the metaverse are math and imagination, so we can create buildings or garments made here to function in new, more ambitious, and inspired ways than their counterparts in the physical world**.** (CHERUKURI, 2021)

Advocates for the metaverse will extol its benign and harmless features. It will find a place in everyone's living room along with the TV, fireplace and couch. Consumers and entrepreneurs will all be able to interact amid the metaverse. Gamers, and coworkers sitting around a table as digital holograms for a conference as opposed to a video call, making virtual meetings seem more natural as it is in 3D. The A/R and v/R applications of the metaverse are limitless and it really can become the next great version of the internet. These depictions of the metaverse—especially by its most ardent fans—sound useful and beneficial. But like every other technology discussed thus far that can influence, leverage, alter and undermine cognitive functions and neurological activity there is adequate reason for caution.

These cautions are rooted in several fundamental questions which ought to guide, govern, and inform further excursions into ambitious enthusiastic metaverse development

— what regulatory, safeguards and security principles will apply to it?

— what organization, entity or group will control, manage, and provide it?

— what restrictions, boundaries, cautions and requirements will be included in it?

— what measures will be taken to ensure that those visiting it can freely depart from it?

Here there is room enough for serious doubt, cynicism, and outright repudiation as even the most strident supporters of the metaverse can argue it is still decades distant in appearing and scientifically impossible to establish. In effect many dispute whether a metaverse can even be devised, developed and sustained. Excursions into the metaverse by persons and families are not just PG-13 ventures into a dreamworld where one can operate with elements of freedom and emerge safely back into reality unscathed either psychologically or neurologically from the experience. In fact, there is no scientific evidence which provides assurance that those inhabiting the metaverse for 30 minutes and returning back to reality are the same people in terms of their cognitive security and intellect. Measuring what actually happens to the human brain while swimming inside the metaverse remains an unknown equation and arcane theory as yet unproven and unknown. Look at the extraordinary precautions we used to prepare astronauts for space travel. Did we plan to do as much for those wearing V/R headsets?

Again, the essential concept of a dual parallel reality available for a short V/R diversion, or a multi-day investment of time indicates people may wish to inhabit the false reality as superior and more rewarding than real life itself. What is more perverse is considering the capability of evil geniuses devising a Metaverse as friendly and accessible as Tik Tok where kids and adults alike can disappear and never return—either mentally or physically. This would entail the deliberate collective engineered convergence of quantum, AI, EMF, nanotech, magneto-biology, and other technologies to validate an operational universe playland where thousands would drift towards it for the fantasy experience just as surely as throngs await the next generation smartphone release. Too much to imagine? Very unlikely and too Sci-Fi to contemplate? Well then consider the reality of NeuroStrike itself. If you doubt that its effects are genuine—anything science and technology produces is ironically attractive.

Metaverse dilemmas can arise in expected and unexpected ways and reside in subtle venues which have many security implications deserving a closer look. There are simply too many ramifications of metaverse adoption to be exhaustively examined and discussed here but sensible caution and risk management criteria must be diligently applied to avoid succumbing to the nuanced and seductive nature of presumptive metaverse benefits. With the emergence of every single dual use technology in the 21st century we must confront the hidden, unknown and subtle risks of misusing or redirecting that technology away from its benign and beneficial intentions and capabilities to create instead an unforeseen weapon or instrument of societal repression and control. Dual-use Science and Technology [DUST] is the hallmark of 21st century creativity and power but contains within itself also the ingredients of humanity's demise.

More sensible and coherent risk analysis must be applied to fully grasp the implications of the metaverse on many of our essential societal and industrial systems. While it can never be assumed that unethical and unscrupulous hostile nations, terrorist groups or criminal elements will reject using the metaverse to acquire more power, leverage control and unleash mayhem it is a stark warning. It means that modern civilized nations blissfully unaware could be targeted and therefore must remain wary and vigilant to grasp the true spectrum of metaverse threats. This calls for serious sophisticated wargaming of metaverse risk scenarios—who will do it?

For example, if the metaverse expands under a climate of unfettered technology oversight it can readily be used by institutions, organizations, government and the military to covertly impose a regulatory scheme in social, political and economic spheres by concentrating cyber power in vested groups who possess custodial controls over it. Observers have called the metaverse a '***convergence of virtually enhanced physical reality operating seamlessly in a parallel virtual' space'*** coexisting with bona fide reality itself. (Vanorio, 2020) We know the metaverse as envisioned skillfully blends augmented reality [AR] with extended reality [XR] utilizing a mixed reality system [MR] to create a virtual reality world [VR]. The MR construct enables free flowing movement between genuine reality and AR where the user enters the VR portal causing real data and images to be replaced by virtual data and images. Thus VR fulfills its designer's ultimate purpose by smoothly replacing the real world with a simulated one.

This means using AR/VR technology enables the illusion and felt experience of trading genuine reality for a cyber created reality. This has serious and unforeseen security implications of long-term concern. We are already familiar with digital replication technologies, erasing images from video streams to alter a landscape, being fooled by deep-fakes and other alternative distortions of visual perception where a person's actual location is at considerable variance with what VR says is his/her augmented location. So the metaverse could make images of people appear in places where in reality they are not. Crisis management, military threat analysis and spatial orientation to confirm place and location would be compromised. Memories, emotional reactions and behavioral anomalies could occur impairing breathing, heart rate, judgement and balance. Likely the true physiological and neurological impact of metaverse experience has never been medically evaluated for its overall human effects. This begs the question of how that would be accomplished and verified to enable safe continued metaverse operations.

At least two aspects of the evolving metaverse merit a pause—its dark web and physical-cyber threats. Some have argued the metaverse is more dangerous than the dark web because of the pseudo-physical presence of the users mimicking clandestine physical meetings versus the purely online open discussion threads in dark web criminal forums. (Numaan Huq, 2022) It seems almost everything a user does will be under unlimited surveillance by the metaverse owner/ operators who will enjoy unprecedented visibility into user actions where privacy conveniently evaporates. Tyrannical and repressive regimes can use the metaverse to control, subdue and govern people as state owned metaverse operators collect troves of user data and exploit it for advantage. As an example, critical infrastructure (CI) facilities will have physical equipment connected to metaverse platforms featuring 'helpful' digital twins ostensibly for safety and maintenance reasons which enables benign remote work. However, it also potentially exposes CI to external cyberattacks via the metaverse and theoretically brings in outsiders able to sabotage CI systems and functions. Criminal access to a power plant's digital twin can exploit it to gain unlawful access to the plant's internal systems or its internal ICS/ SCADA environment. Worse criminals can use digital blueprints of the site to plot their attacks or plan entry/ exit approaches to power plants and possibly nuclear reactors. How does this change the set of risk considerations and security measures which must be incorporated to offset this?

Another disturbing area of metaverse intrusion which seems harmless at first would be full-body actuator suits giving users [surgeons and maintenance personnel] the ability to physically feel things inside the metaverse. Metaverse systems can allow users to touch an object, sense a push, feel a jump, experience the interactive elements, and derive the 'hands on' feel of reality. However, this opens the door to dangerous cyber-physical threats where malicious code embedded in these body suits can cause a malfunction, endangering the user by inducing extreme heat, cold, pain or visual effects distorting reality to triggering seizures. Criminal elements can gain access to bodysuits via cyber intrusion and monitor the user's actions.

Curbing adoption and implementation of metaverse technologies will be difficult. Champions advocating metaverse use will be relentless during the 21st century. Those harboring doubts or legitimate concerns will encounter stiff and resolute resistance from inventors, scientists and civilian leaders who will extol its many benefits while overlooking its risks and security pitfalls. Again the forces of modernity may prevail over those hesitant to embrace all the good and bad which comes along whenever DUST is accepted and promoted.

What we have described about the metaverse is worth thinking about. Using a mix of the most advanced science and technology systems and platforms to create a faux parallel cyber grounded reality much more inherently attractive and beneficial than reality itself we stumble upon the ultimate escape. The quest for a metaverse free space where no organizational, personal or government entity can assume primordial governance and creative ownership of it is breathtaking. However, it opens the door to insidiously dangerous mischief where our neural and behavioral safeguards and intuitive autonomous systems are outmaneuvered. It creates to a degree, so far unanticipated or expected, an unrequited and evolving appetite for dwelling in the allegedly majestic and fantastic environment which the metaverse promises to establish. For all to enjoy.

In strategic terms as the decade beginning in 2020 rolls ahead without hesitation into its third year, we face a crossroads of geopolitical analysis where assigning blame and ultimate responsibility for both the good and

bad arising from the engineered convergence of these technologies must be assessed. In more stringent terms we must confront the degree to which explicit convergence of these technologies actually confers the kind of strategic advantage which leverages global history in favor of one nation over the others. It is therefore fair to ask who benefits from this massive endeavor?

STRATEGIC MYOPIA AND CHINA BLINDNESS

In turn this historic crossroads must be assessed against the present-day forces of geostrategic reality. Dominant military enterprises, research institutes, decades long R&D ventures in innovative technology and sophisticated high-tech espionage depict the Peoples Republic today. Their relentless quest to sit atop the global superpower club drives their respective ambitions and unlimited appetite to further the deliberately engineered technology convergence which is the heart of this essay. This is not to claim that other nations are not busy pursuing the same set of outcomes but instead to reinforce the point that the West—especially the USA—is woefully behind in the frantic race for supremacy in this arena. Worse, many of these nations are blissfully unaware that Chinese military investment in and perfection of this set of convergent technologies is happening at a pace and scale which conveys a distinct strategic advantage. This is both myopia and China blindness. There is no immediate remedy for the shortcoming but reckoning with it honestly as a serious security shortfall is a start. Kinetic systems capture the imagination and win the lion's share of budget dollars. There is a disturbing tendency among commercial and government leadership to favor short term issues and challenges over the longer-term view which deals explicitly with the security and stability of the enterprise itself. This is also known as strategic myopia which refers to intense focus on short term issues, gains, objectives, and challenges to the extent that anything longer term is ignored, overlooked, or diminished in significance. For example, having the US focus on the Russia-Ukraine war, or climate change, or the World Economic Forum dicta about ESG to the utter exclusion of legitimate geopolitical threats such as China, secure US borders, drug cartel dominance in Mexico, declining leverage in US made goods and trade imbalances and many others. When one contemplates the insidious, gradual, and covertly growing momentum which convergently engineered IOT, quantum, nanotech, metaverse perversion and NeuroStrike symbolizes the threshold endgame significance as tipping point strategic leverage becomes clear. Tragically, among senior US defense leadership—both civilian and military—there is ample manifestation of strategic myopia which fosters widespread concern. Traditional defense bulwarks such as new weapons systems, investing in troop training, upgrading special operations versatility, overhauling logistics requirements, acquiring space, IOT, quantum and nanotech superiority have fallen into a quiet trance. Our defenses against future biotech, synthetic biology and genomic weapons are at least 15 years behind their most desirable position. Even some senior Pentagon officers have spoken out about this aware that their energetic call to arms is being ignored in the process.

"I will be very honest with you. It is very unsettling to see how much the US is not connecting the dots on our number one challenge," Rear Adm. Mike Studeman, the commander of the Office of Naval Intelligence, told attendees here at the West 2023 conference in San Diego. "It is disturbing how ill-informed and naïve

the average American is on China. I chalk this up, if I could summarize, into a China blindness. We face a knowledge crisis and a China blindness problem," he continued. Studeman's blunt comments come as the White House, the Pentagon, and the country at-large deal with the fall-out of a Chinese high-altitude balloon that violated US airspace (Katz, 2023)

So, the question lingering in the atmosphere is simple—If the NeuroStrike threat is real and it is founded on the explicit convergent engineering of several key technologies mentioned herein which the USA has thus far overlooked, dismissed, or ignored what does that suggest about future American security and societal stability among our allies in the West? The answer is to speculate openly about at least three outcomes...

1—West and USA discern NeuroStrike threat effectively confronting and defeating it

2—West and USA dismiss/ignore NeuroStrike threat and become 3rd rate powers

3—The NeuroStrike threat scenario never happens at all is the globe is secure

PRIMARY PRINCIPLES AND THE PRIMACY OF THE POO POO PASHAS

The underlying principles in grasping NeuroStrike entail a mix of technologies combined with well-established and scientifically verified studies of negative cognitive effects stemming from the so-called Frey effect and the work of acoustics genius Ross Adey. Of course, deniers, artful dodgers from the intelligence community, and media hawks unaccustomed to probing scientific phenomena which contain anomalies will inhabit the poo poo pasha sect. Those focused on truth and medical facts must arrive at a different conclusion. Very simply the nonkinetic yet invasive neurological degradation system called NeuroStrike is very real and has dozens of government scientists and other experts engaged in validating its operational metrics and discerning ways to thwart its effects. Defense of persons and creation of early warning and eventual countermeasures to quell NeuroStrike attacks in the future is well underway.

This fact exists apart from the faux vision of reality which the leader of US intelligence at ODNI denies is 'hostile' or originates from a foreign threat source. (ODNI, 2023) The denial of NeuroStrike as a legitimate threat is puzzling and counterintuitive for several reasons. First there are hundreds of victims seeking authentic cognitive treatment and relief where medical experts are today attempting to reduce cognitive degradation effects. Secondarily the reports of random isolated NeuroStrike attacks remain viable and confirmable as recently as March 1, 2023-coincidentally the same date as ODNI denies its authenticity. Thirdly a dedicated cadre of experts are investigating the contributing factors underpinning NeuroStrike on both sides of the Atlantic and they are pursuing this quest without the ODNI bias that so-called victims are experiencing episodes of emotional or psychological trauma. Fourth, the laws passed by Congress to compensate verified victims of NeuroStrike have been in place for 2 years and some have been reimbursed for their medical expenses and others continue to seek qualification under those laws for onward treatment. Fifth, prominent US government analysts and diplomats who have gone on record with media interviews have never repudiated their basic narratives about the effects of NeuroStrike on themselves and their families.

A dilemma of genuine national security proportions looms from this analysis because if the technology

behind Havana Syndrome [i.e., NeuroStrike] is real, and such attacks continue, and thousands of people remain injured from this technology, and we have reason to suspect a foreign power controls this technology and it poses a future threat to military and civilian leadership as well as ordinary warfighting troops we have a problem. Is it a problem more serious than global warming, equity or finding pathway to sustainable development—indeed it is. But unless our leadership sees it that way, we risk becoming victimized strategically for lack of vision and geopolitical courage.

So, we are left with a conclusion that is far more plausible and credible than an official denial levied by a US government agency. After all the sordid experience of Americans with COVID amply illustrates a breach of trust between citizens and their government on the trustworthiness and reliability of guidance on masks, shutdowns, vaccines, and what cohort groups ought to be vaccinated we can read for ourselves the hypocrisy involved. The primary principles on NeuroStrike which emerge from all this are

- NeuroStrike is real and authentic, not imagined or theoretical.
- NeuroStrike attacks have damaged many hundreds of victims thus far
- NeuroStrike attacks continue into 2023.
- Technologies at the core of NeuroStrike are under serious investigation.
- Protecting US diplomats, military, and IC personnel against NeuroStrike is key.
- Determining if ordinary US citizens have been victimized by NeuroStrike is key
- Discerning the technological core of NeuroStrike is a paramount security goal
- Devising defense/deterrence/defeat technologies against NeuroStrike is key.
- Confirming foreign sponsors/owners of NeuroStrike is a priority security issue.

Surely there can be little doubt that fundamentally these principles must guide our national survey and inquiry about NeuroStrike over the next few years to dispel all doubt, decode any lingering mystery and validate its technological essence and foreign sponsor well before 2025. If we have trouble seeing the confluence of cyber, AI, nanotech, the metaverse and mixed RF, magnetic, acoustic, and vestibular factors involved then one should join the critics who regard NeuroStrike as an evil fantasy.

To overlook. misjudge or underestimate the strategic significance of NeuroStrike and its indirect links to AI, cyber, nanotech, ChatGPT and the metaverse is a fatal error. The linkage is palpable and insidiously unfolding outside the facile and inquisitive eyes of major media and academic experts for two good reasons. Number one they are in love with modern technology and all it potentially offers. Number two, they are abysmal in discerning threats to society rooted in advanced technology as their paradigm posits a world made comprehensively better because of technology itself. Years ago, the prescient author Mary Shelley wrote about the dangers of science and renegade ego running amuck in her famous treatise on Frankenstein where the monster devours its creator. We risk the same outcome because of widespread arrogance and naivete where the contours of unrestricted technology as threat vs technical savior wins out. (Shelly, 1818)

There is ample room for caution, doubt, and skepticism when one combines AI, nanotech, cyber,

neurotechnology and ChatGPT into some amorphous insidious convergent monster that strips humanity of its sovereign controls over mental functions and cognitive operations. However, that reasonable signpost of caution and doubt must be dispelled in part because the obvious and latent convergence of these technologies has already happened and is being upgraded for effectiveness and reliability. It reflects a concept also known as 'attack surface management' [ASM] which involves a combination of people, processes, technologies, and services deployed to continuously discover, inventory, and manage an organization's assets. These assets can be both internal and external, and they pose digital risks. This visibility can help reduce exposure that could be exploited by malicious threat actors which entail internal, external, and digital risks. (Paloaltonetworks – Staff, 2022) The unknown vulnerabilities we confront or ignore will spell out our collective humanitarian future.

The watchword being offered here is that often we are blind to the full spectrum of our own vulnerabilities which opponents can exploit to their advantage. While it makes sense to consider that ChatGPT, AI, cyber systems, nanotech, neurobiological impairment platforms and the Metaverse can convergently combine in insidious ways to harm us it requires some strategic perspective. The ASM construct suggests we may be ignorant of all internal, external, and digital risks—including the oft neglected phigital realm where digital and human factors coincide and dwell harmoniously. The day will surely arrive when scientists and innovative engineers bereft of a moral code will create a cyborg that is autonomous and refuses to heel to our desperate bidding. Only then will we fully comprehend the future Frankenstein which our imaginations have been born.

What must happen today and urgently is to liberate ourselves from viewing the net impact of convergent technology on humans and its incipient fascination. It is a dangerously flawed assumption which distracts us from the genuine challenge. Instead, we ought to refocus ourselves towards establishing human direct and indirect influence over all technology itself including strategies for zero-day controls and kill switches. By protecting our innate cognition, perception and mental functions against technological interference, theft, and hostile manipulation we can survive in spite of the machines which so ardently seduce us in spite of ourselves. We must take a different pathway. The reciprocal option is that human logic, perception, imagination, thought and design can warmly persuade us that nothing less than direct control, confinement, absolute restriction and daily vigilant governance of technology is our best hope.

FINDING A WAY FORWARD AGAINST NEUROSTRIKE

The NeuroStrike threat is genuine and has racked up thousands of verifiable victims awaiting some form of cognitive relief and genuine treatment to alleviate the persistent disabling syndrome its victims endure. Today Europe and the United States can awake from a dangerous stupor and recognize the era of targeted cognitive warfare where NeuroStrike is all but invincible is truly upon us. Such powerful technology in the wrong hands, or in the hands of amoral scientific ghouls based in any society, leads us into a miasma of cognitive chaos and abject mental cannibalism. Certainly, enemy possession of this technology can covertly bring down society, its leaders, and its government with surgical precision as the technology is improved and modified to adversely affect a wider target audience. If this remains an unknown threat and an unrecognized vulnerability, we are

doomed. Many will fall victim to its enduring appeal especially for those who would seek to subdue us all and control human behavior conclusively as a blatant power move. This cannot be allowed to happen.

If it fails to be clear now it should soon emerge as the obvious preferred scenario choice listed that choice #1 is the best path forward for America and the West. Recognizing, confronting, and defeating all manifestations of the NeuroStrike threat is paramount. This will require devising robust early warning, sensor detection capabilities, defensive and deterrent technologies, and standoff systems to impose nullification and defeat of the NeuroStrike threat. This implies also finding a validation architecture for forensic analysis to determine and validate the origin of future attacks. The term 'attack' seems off-putting and controversial to so many. However unpopular or quasi-offensive the term 'attack' may be, it clarifies exactly what is happening. Technology is targeting humans to strip them of cognition, will and logic and it edges every day towards a finer degree of perfection.

A better term than 'NeuroStrike attack' is needed to make the idea more resonant with a doubtful public and civic leadership? Should such terminology be clear enough that the old and noticeably young readily grasp its significance and rail energetically against its continuation? Brain wars are clear enough and cognitive conflict is appealing, however it must be a concept we all recognize as a foundational threat to humanity. There can be no latent ambiguity. Can we call it a 'hostile brainstorm" and thereby acquire wider public approval and support? The jury is still out on the question. It is not at all clear—the only thing that is fundamentally clear is what happens to civilization if we continue to ignore or overlook the NeuroStrike threat. Doing so is truly not good at all.

REFERENCES

BROWNE, R. (2023, Feb 15). CHATGPT. (https://www.cnbcevents.com/davos/, Interviewer)

Browne, R. (2023, Feb 15). *elon-musk-co-founder-of-chatgpt-creator-openai-warns-of-ai-society-risk.* Retrieved from https://www.cnbc.com: https://www.cnbc.com/2023/02/15/elon-musk-co-founder-of-chatgpt-creator-openai-warns-of-ai-society-risk.html

centerforfoodsafety.org – Staff / Editorials. (2023, Mar 15). *nanotechnology and our food supply* . Retrieved from https://www.centerforfoodsafety.org: https://www.centerforfoodsafety.org/issues/682/nanotechnology/food-and-nanotechnology

CHERUKURI, N. (2021). *Interview.* Retrieved from https://www.thirdeyegen.com/: https://www.thirdeyegen.com/

Gaidos, S. (2015, Oct 16). *Nanoparticles in foods raise safety questions.* Retrieved from https://www.sciencenews.org: https://www.sciencenews.org/article/nanoparticles-foods-raise-safety-questions

Ghebretatious, M., & et.al. (2021, Feb 16). *Nanoparticles in the Food Industry and Their Impact on Human Gut Microbiome and Diseases.* Retrieved from https://pubmed.ncbi.nlm.nih.gov/33669290/: https://pubmed.ncbi.nlm.nih.gov/33669290/

Katz, J. (2023, Feb 15). *naval-intelligence-admiral-naive-american-public-has-a-china-blindness-problem.* Retrieved from https://breakingdefense.com/: https://breakingdefense.com/2023/02/naval-intelligence-admiral-naive-american-public-has-a-china-blindness-problem/

McCreight, R. (2022, Sept 16). *Neuro-Cognitive Warfare: Inflicting Strategic Impact via Non-Kinetic Threat.* Retrieved from https://smallwarsjournal.com/jrnl/: https://smallwarsjournal.com/jrnl/art/neuro-cognitive-warfare-inflicting-strategic-impact-non-kinetic-threat

McCreight, R., & Sincavage, &. S. (2019, Jan 25). *The Significance of Convergent Technology Threats to Geospatial Intelligence.* Retrieved from https://trajectorymagazine.com/: https://trajectorymagazine.com/the-significance-of-convergent-technology-threats-to-geospatial-intelligence/

McMillen, M. (2015, July 15). *Nanoparticles: Small Size, Big Health Concerns?* Retrieved from https://www.webmd.com/: https://www.webmd.com/special-reports/food-additives/20150723/nanoparticles-food-additives#:~:text=Titanium%20dioxide%2C%20the%20most%20common%20nanoparticle%20in%20food%2C,dioxide%20as%20%22GRAS%2C%22%20or%20generally%20regarded%20as%20safe.

Miller, M. (2022, April 13). *Is 'TikTok Brain' Affecting Kids?* Retrieved from https://www.verywellhealth.com/tiktok-brain-5225664: https://www.verywellhealth.com/tiktok-brain-5225664

N.J.Cherry. (2003, Jun 60(6):843-4. doi: 10.1016/s0306-9877(03)00027-6.). *Human intelligence: the brain, an electromagnetic system synchronised by the Schumann Resonance signal.* Retrieved from https://pubmed.ncbi.nlm.nih.gov/12699709/: https://pubmed.ncbi.nlm.nih.gov/12699709/

National Academies. (2020, Dec 5). *New Report Assesses Illnesses Among U.S. Government Personnel and Their Families at Overseas Embassies.* Retrieved from https://www.nationalacademies.org/: https://www.nationalacademies.org/news/2020/12/new-report-assesses-illnesses-among-us-government-personnel-and-their-families-at-overseas-embassies

Nature Reviews – Staff. (2021, Feb 9). *Let's talk about lipid nanoparticles.* Retrieved from https://www.nature.com/: https://www.nature.com/articles/s41578-021-00281-4

NOBELL, N. (2023). *the metaverse will be an infinite realm that blankets both the physical and virtual worlds.* Retrieved from https://www.callisonrtkl.com/: https://www.callisonrtkl.com/

Numaan Huq, R. R. (2022). Metaverse or Metaworse? Cybersecurity Threats Against the Internet of Experiences . *TrendMicro Rsearch*.

ODNI. (2023, March 3). *US Intelligence—No Evidence a Foreign Power Behind Havana.* Retrieved from https://thehill.com/: https://thehill.com/policy/national-security/3879732-us-intelligence-says-havana-syndrome-unlikely-caused-by-foreign-adversary/

Ortiz, S. (2023, March 10). *what-is-chatgpt-and-why-does-it-matter-heres-everything-you-need-to-know/.* Retrieved from https://www.zdnet.com/: https://www.zdnet.com/article/what-is-chatgpt-and-why-does-it-matter-heres-everything-you-need-to-know/

Paloaltonetworks – Staff. (2022, April 5). *Innovation Insight for Attack Surface Management.* Retrieved

from https://www.paloaltonetworks.com/resources/research/innovation-insight-for-sttack-surface-management: https://www.paloaltonetworks.com/resources/research/innovation-insight-for-sttack-surface-management

Sahdev, P., & et.al. (2014, Nov 22). *Biomaterials for nanoparticle vaccine delivery systems.* Retrieved from https://pubmed.ncbi.nlm.nih.gov/: https://pubmed.ncbi.nlm.nih.gov/24848341/

Scott Wong, K. S.-K. (2023, Feb 18). *Momentum builds in Congress to crack down on TikTok.* Retrieved from https://www.nbcnews.com/: https://www.nbcnews.com/politics/congress/congress-tiktok-ban-social-media-harms-teens-rcna70998

Shah, V. (2021, Oct 29). *What is the Metaverse? Meta's Vishal Shah explains.* Retrieved from https://www.facebook.com/EFTMonline/videos/: https://www.facebook.com/EFTMonline/videos/what-is-the-metaverse-metas-vishal-shah-explains/6474011812672174/

Shelly, M. (1818). *Frankenstein-or-The-Modern-Prometheus.* Retrieved from https://www.britannica.com/topic/Frankenstein-or-The-Modern-Prometheus: https://www.britannica.com/topic/Frankenstein-or-The-Modern-Prometheus

Shmerling, R. H. (2022, Jan 18). *Tics and TikTok: Can social media trigger illness?* Retrieved from https://www.health.harvard.edu/: https://www.health.harvard.edu/blog/tics-and-tiktok-can-social-media-trigger-illness-202201182670

Staff. (2017, Nov 3). *how-the-human-body-creates-electromagnetic-fields.* Retrieved from www.forbes.com/: https://www.forbes.com/sites/quora/2017/11/03/how-the-human-body-creates-electromagnetic-fields/?sh=32a879a356ea

Tennenhouse, E. (2018, May 25). *What Magnetic Fields Do to Your Brain and Body.* Retrieved from https://www.discovermagazine.com/: https://www.discovermagazine.com/environment/what-magnetic-fields-do-to-your-brain-and-body

Vanorio, F. (2020). Metaverse: Implications for Security and Intelligence . *NATO Defense College Foundation Paper*.

WHO – Staff. (2017, Feb 2). *WHO guidelines on protecting workers from potential risks of manufactured nanomaterials.* Retrieved from https://www.who.int/: https://www.who.int/publications/i/item/9789241550048

WHO -Staff. (2016, Aug 4). *questions-and-answers/item/radiation-electromagnetic-fields.* Retrieved from https://www.who.int/news-room/questions-and-answers/item/radiation-electromagnetic-fields: https://www.who.int/news-room/questions-and-answers/item/radiation-electromagnetic-fields

Zwoinska, J., & al., e. (2015). *Electromagnetic field induced biological effects in humans.* Retrieved from https://pubmed.ncbi.nlm.nih.gov/27012122/: https://pubmed.ncbi.nlm.nih.gov/27012122/

PART II

PART 2: SPACE THREATS

9.

BIOLOGICAL THREATS AND GROWTH IN SPACE [SINCAVAGE & MUEHLFELDER & CARTER]

ABSTRACT

Biological threats in space pose significant challenges for human space exploration. It requires comprehensive research and development of innovative strategies to mitigate risks and ensure the safety and sustainability of space missions. This chapter provides an overview of biological threats to spacecraft and astronauts, including technological development through time and considerations for future growth. It emphasizes the importance of collaboration between government agencies, industry partners, and academic institutions to address the complex issues of biological threats within new space exploration.

STUDENT OBJECTIVES

After reading this chapter, students should be able to do the following:

- Explain the difference between forward and backward contamination when discussing biological threats in space.
- Describe the diverse types of threats posed by pathogens within spacecraft.
- Define critical technologies to mitigate biological risks and help advance space exploration.

INTRODUCTION

Biological threats and growth in space are two important topics that have gained significant attention in recent years. The possibility of biological threats in space is a primary concern for astronauts and space agencies, as exposure to harmful microorganisms can severely affect human health. As space exploration and research continue to advance, the possibility of encountering biological threats in space becomes an ever-growing concern. These threats can come from microorganisms, viruses, and other pathogens that may adversely affect human health and the environment. Understanding the nature of these biological threats and developing effective countermeasures is essential for ensuring safe and successful space missions. On the other hand,

growth in space has become an area of interest due to its potential to support long-term space missions and even colonize other planets. This topic involves studying the behavior of living organisms in microgravity conditions, vacuum, and high radiation environments, which can provide insights into the fundamental principles of life.

DEFINITION OF BIOLOGICAL THREATS IN SPACE

Biological threats in space refer to the potential danger posed by microorganisms or pathogens that may exist in extraterrestrial environments or travel from Earth into space habitats. The possibility of such threats arises since microorganisms are ubiquitous and can survive in extreme conditions, including those in space. In addition, human space exploration and colonization activities involve the introduction of new organisms into extraterrestrial environments, which could disrupt existing ecosystems and pose risks to human health.

The potential biological threats in space include both naturally occurring microorganisms and those that are intentionally or accidentally introduced by humans. Naturally occurring microorganisms such as comets, asteroids, and celestial bodies appear in extraterrestrial environments. These microorganisms may have evolved to survive in extreme conditions such as low temperatures, high radiation levels, and lack of water. Intentional or accidental introduction of microorganisms by humans can occur through the contamination of spacecraft or equipment used for space exploration or through the release of waste materials into space habitats.

Biological threats in space can be significant for human health and extraterrestrial ecosystems. Microorganisms that harm humans can cause infections, allergies, and other health problems. In addition, introducing new organisms into extraterrestrial environments can disrupt existing ecosystems and alter natural processes.

Various measures are continuously being developed and implemented by space agencies and organizations to address the potential biological threats in space. These include strict protocols for spacecraft sterilization, quarantine procedures for astronauts returning from space missions, and monitoring of extraterrestrial environments for signs of microbial activity.

IMPORTANCE OF STUDYING BIOLOGICAL THREATS IN SPACE

The exploration and colonization of space have been a topic of interest for scientists and researchers for decades. However, with the increasing number of missions and expeditions to space, there is a growing concern about the potential biological threats that may arise. Studying biological threats in space is crucial to ensure the safety and well-being of astronauts and prevent the spread of harmful microorganisms from Earth to Earth.

One of the primary reasons for studying biological threats in space is the potential impact on human health. The microgravity environment of space can weaken the immune system, making astronauts more susceptible to infections. Moreover, harmless microorganisms on Earth may become virulent in space due to mutations

caused by radiation exposure or other environmental factors. Therefore, understanding the behavior and evolution of microorganisms in space is essential to develop effective preventive measures and treatments.

Another reason for studying biological threats in space is the risk of contamination. Spacecraft returning from missions may carry microorganisms that can survive in the harsh conditions of space. If these microorganisms are not adequately contained and decontaminated, they may threaten Earth's ecosystems and public health. Therefore, it is crucial to identify and monitor potential contaminants and develop protocols for their safe handling.

Furthermore, studying biological threats in space can also provide insights into the origins of life on Earth and other planets. Microorganisms found in extreme environments such as space may have unique genetic adaptations that could shed light on the evolution of life on Earth and the possibility of extraterrestrial life.

Overall, studying biological threats in space is essential for ensuring the safety and well-being of astronauts, preventing contamination, and advancing our understanding of life on Earth and beyond.

HISTORICAL OVERVIEW OF BIOLOGICAL THREATS IN SPACE

EARLY SPACE MISSIONS

Space exploration has always been a fascinating subject for scientists and researchers. However, discovering the unknown comes with several risks, including biological threats. The potential risks of biological contamination in space have been a concern since the beginning of space exploration.

During World War II, the German army conducted experiments on human subjects to study the effects of high altitude on the human body (Burgess & Dubbs, 2007). These experiments used high-altitude chambers and pressurized suits that simulated high-altitude conditions. The experiments showed that exposure to high altitude could cause severe physiological changes in the human body, including hypoxia and decompression sickness. However, these experiments also raised concerns about potential biological contamination in space.

According to a study by the National Aeronautics and Space Administration (NASA), "The first living organisms sent into space were fruit flies aboard a U.S. V-2 rocket launched by the Army Ballistic Missile Agency on February 20, 1947" (Joosse, 2023). Since then, various missions have been conducted, including manned missions, that have exposed astronauts and spacecraft to different biological threats.

From the 1950s to the 1960s, the United States and the Soviet Union launched several missions that carried biological samples into space, including bacteria, viruses, and fungi (Beischer & Fregly, 1962). The multiple missions' goal was to study the effects of microgravity and radiation on living organisms. However, they also raised concerns about the potential to contaminate other planets or spacecraft.

In 1961, Yuri Gagarin became the first human to orbit Earth (Mai, 1961). Several other manned missions by both countries followed this achievement. However, these missions also raised concerns about potential biological contamination in space. The astronauts were exposed to various microorganisms during their

training and preparation for space flight. There was a risk that microorganisms could contaminate the spacecraft and infect other crew members.

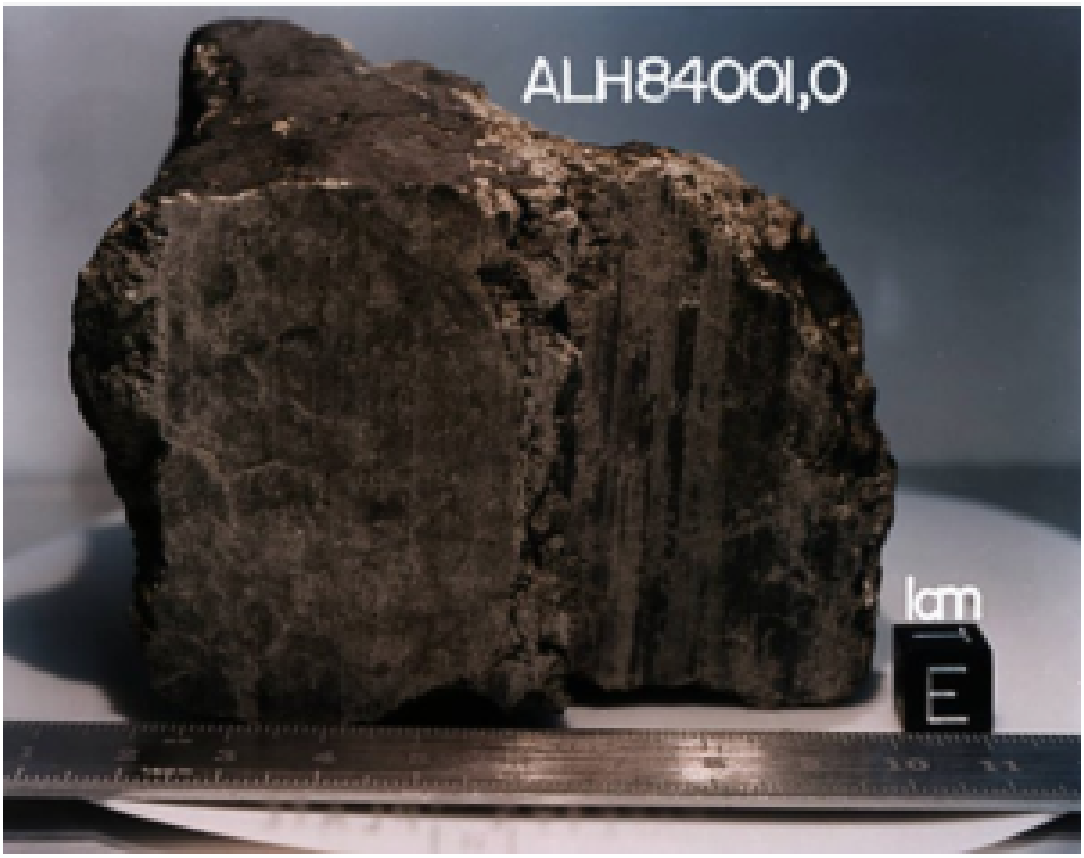
Concerns amplified between 1968 and 1972 with the U.S. Apollo missions to the moon. The possibility of sending a person to a celestial object changed how scientists viewed biological contamination in space. To address these concerns, NASA developed strict protocols for preventing biological contamination during manned missions (Carter, 2001). These protocols included rigorous cleaning and sterilization of the spacecraft, quarantine of the crew before launch, and monitoring the crew's health during the mission. These protocols were effective in preventing any major biological incidents during manned missions. The same precautions were taken during the Viking missions to Mars in the 1970s. However, only in the 1990s did the threat of biological contamination in space become more widely recognized.

One of the most famous incidents involving biological contamination in space occurred in 1967, when the Surveyor 3 spacecraft returned to Earth, carrying bacteria that had survived on the moon's surface for over two years (Rummel, Allton, & Morrison, 2011). This incident startled the aerospace community and highlighted the need for stricter protocols to prevent contamination of other celestial bodies during future missions. However, it was found later that the contamination came from personnel after the craft returned to Earth.

In 1971, the Soviet Union launched the first space station, Salyut 1 (Mars, 2021). This event marked a new era in space exploration, allowing for longer-duration missions. However, with more extended missions came new challenges in preventing biological contamination. The crew members were exposed to various microorganisms for an extended period, increasing the risk of infection. To address these challenges, NASA and other space agencies developed newer protocols for preventing biological contamination during long-duration missions (Carter, 2001).

However, one of the most significant events in the history of biological threats in space was the declared discovery of life on Mars. Not only could we carry the threat of contamination to space, but there was also a threat from above. In 1996, NASA announced that they had discovered evidence of microbial life on a meteorite believed to have originated from Mars (Savage, Hartsfield, & Salisbury, 1996). The meteorite, ALH84001, was recovered from Antarctica's Allan Hills ice field in 1984. Later, scientists from NASA who analyzed the meteorite described what was fossilized bacteria on its surface. To this day, the discovery was disputed by scientists. However, the discovery sparked renewed interest in the search for life on other planets and increased concerns about the potential for contamination from outer space.

FIGURE 9-1 The Allan Hills 84001 Meteorite



Source: (Scalice, 2022)

The history of biological threats in space dates to the early days of space exploration. The potential risks of biological contamination have always been a concern for scientists and researchers, which still holds today. However, with the development of advanced technologies and strict protocols for preventing biological contamination, the risk of a significant biological incident during manned missions has been significantly reduced.

MODERN SPACE MISSIONS

Modern space missions have increasingly focused on studying biological threats in space and other planets. Since the beginning of human space exploration, scientists have been concerned about the potential risks of biological contamination and the spread of disease between our world and other celestial bodies. The unique environment of space provides a valuable opportunity to study the effects of microgravity and radiation on living organisms, including pathogens that could threaten human health. In recent years, several missions were launched to study and help prevent biological threats to protect astronauts and future space travelers. These missions have involved collaborations between various space agencies and private companies, including NASA, the European Space Agency (ESA), the Russian Federal Space Agency (ROSCOSMOS), the China National

Space Administration (CNSA), SpaceX, and others. This section will briefly review recent and ongoing space missions, including some of their experiments.

1. **International Space Station (ISS)**: The ISS is a joint project between NASA, ROSCOSMOS, ESA, JAXA, and CSA, continuously inhabited since November of 2000 (Howell, 2023). The ISS provides a unique platform for conducting long-term studies on the effects of microgravity on human physiology and biology. Several experiments have been conducted on board the ISS to study the effects of microgravity on bone density, muscle mass, cardiovascular function, immune system, and other physiological systems.

* **Biomolecule Extraction and Sequencing Technology (BEST):** This investigation occurs on the International Space Station (ISS). This investigation aims to identify unknown microbial organisms that may be present on the ISS and assess their potential risks to human health. The BEST investigation uses advanced DNA sequencing technology to analyze samples collected from various surfaces on the ISS, including air filters, water systems, and crew quarters (Johnson, 2018).

* One of the primary goals of the ISS missions is to understand how microorganisms behave in microgravity environments. Studies have shown that microorganisms can adapt to these conditions and become more virulent, potentially threatening astronauts and spacecraft. To address this concern, NASA has launched several missions to study microbial behavior in space, including the Microbial Observatory-1 (MO-1) mission beginning in 2003 and the Microbial Tracking-1, 2, & 3 (MT-1, MT-2, MT-3) missions beginning in 2006. This investigation uses specialized equipment to collect samples from various locations around the ISS, analyze their genetic makeup, and track the movement of the microbes (Tabor, 2021).

FIGURE 9-2 International Space Station

Source: (The Guardian, 2010)

2. **Mars Science Laboratory (MSL):** The MSL is a NASA mission that landed the Curiosity rover on Mars in 2012. The mission's primary objective is to study Mars's geology and habitability. However, the mission also includes several experiments to study the effects of radiation on living organisms. The rover carries a radiation detector that measures the levels of radiation on the Martian surface, which can help scientists understand how radiation affects living organisms in space (Dunbar, 2017).
3. **ExoMars:** is a joint mission between ESA and ROSCOSMOS that aims to search for signs of past or present life on Mars. The mission includes a rover and a stationary lander that will conduct experiments to study the Martian environment and search for biosignatures. One of the mission's key objectives is understanding how life can survive in extreme environments like Mars (European Space Agency, 2023).
4. **The BioSentinel mission**: is scheduled for launch in 2024. The mission will send a small spacecraft equipped with yeast cells into deep space to study the effects of cosmic radiation on living organisms. The yeast cells will be genetically modified to detect and report levels of radiation exposure, providing valuable data for future manned missions beyond low Earth orbit (Ahmed, 2022).
5. **Bion-M:** is a series of Russian space missions that aim to study the effects of microgravity and other spaceflight factors on living organisms. The missions have carried a variety of animals into space already,

including mice, rats, geckos, and fruit flies, to study the effects of spaceflight on their physiology and behavior. The data collected from these missions enable scientists to understand better how living organisms adapt to the extreme conditions of space. Further launches for Bion-M missions will launch in 2024 (Kovo, 2014).

6. **The Mars Sample Return Mission will occur in the 2030s**. The mission will involve collecting samples from Mars and returning them to Earth for analysis. One of the primary goals of this mission is to search for signs of past or present microbial life on Mars. Studying these samples could provide valuable insights into the potential for life beyond Earth and inform our understanding of biological threats in space (NASA, 2023).

These current space missions and scientific conferences demonstrate a growing interest in studying biological threats in space and developing countermeasures to protect astronauts and future space travelers. Modern missions are determined to study and prevent biological threats in space and are critical for ensuring the safety of astronauts and protecting other celestial bodies from contamination. As space exploration expands, these missions will play an increasingly important role in maintaining the integrity of our home and solar system.

EMERGENCE OF BIOLOGICAL THREATS IN SPACE

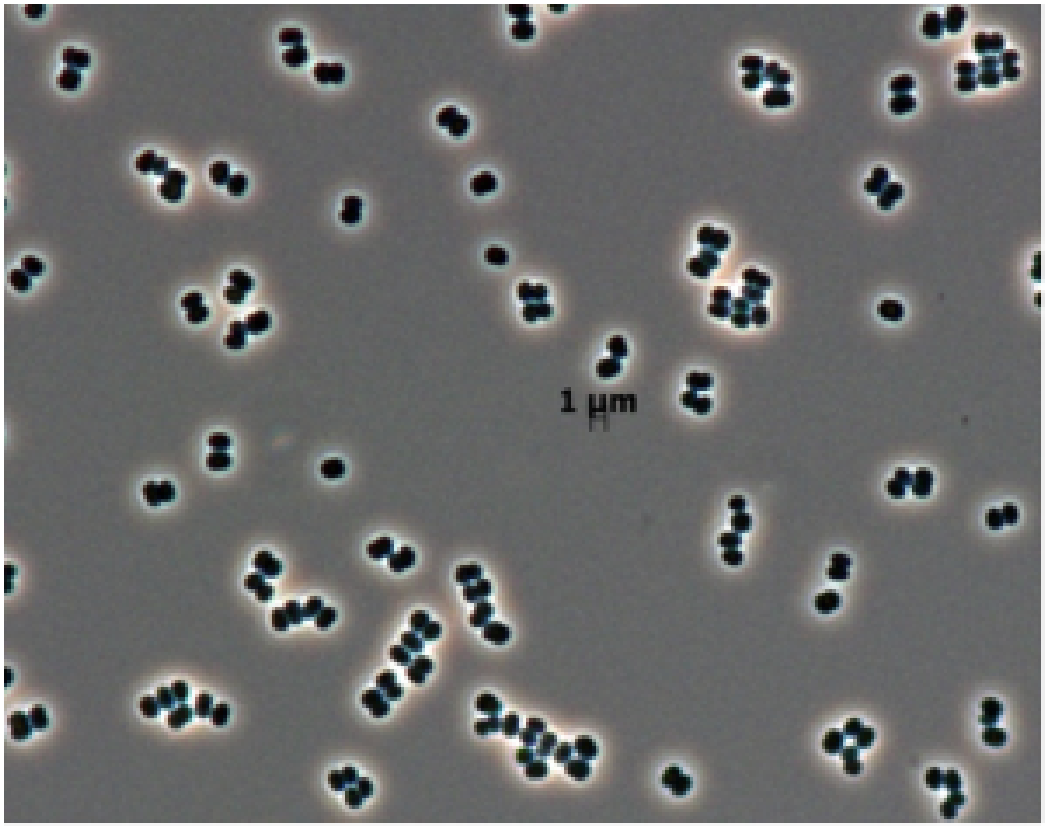
In the early stages of space exploration, The Committee on Space Research (COSPAR) was established on October 3, 1958, by the International Council for Scientific Unions. COSPAR's objectives were, and still are, to "promote, on an international level, scientific space research, with emphasis on the exchange of results, information, and opinions, and to provide a forum, open to all scientists, for the discussion of problems that may affect scientific space research" (International Space Council, 2023). Through its guidance, The Outer Space Treaty was signed on October 10, 1967, between the U.S., Moscow, and the U.K., with 113 countries adding themselves to the agreement. The treaty formulated policies that spacefaring nations could adhere to and was based on scientific knowledge. Article 9 of the agreement paved the way for regulations about "Forward Contamination" and "Backward Contamination" during space travel (United Nations Office for Outer Space Affairs, 2023).

According to NASA's Office of Safety and Mission Assurance (OSMA), Forward Contamination refers to the "unintentional transfer of terrestrial organisms or biological material from Earth to another celestial body, such as a planet or moon" (Keith, 2021). Accidental transfer can occur during space exploration missions when spacecraft, landers, or rovers carry microorganisms or other organic materials that may contaminate the target environment. The concern is that if these organisms survive and proliferate on another celestial body, they could interfere with scientific investigations and potentially compromise the search for extraterrestrial life.

Backward Contamination, on the other hand, refers to "the potential contamination of Earth by extraterrestrial organisms or biological material" (Keith, 2023). This contamination could occur when samples collected from another celestial body are returned to Earth for analysis. The concern is that if any potentially

hazardous microorganisms or other biological entities are present in these samples, they could risk terrestrial ecosystems and human health.

FIGURE 9-3 Bacteria found on Curiosity before launch



Source: (Stromberg, 2014)

Both forward and backward contamination are essential considerations in space exploration missions. However, the big question is, can a pathogen survive in space?

A pathogen describes an infectious microorganism or agent, such as viruses, bacteria, protozoa, prions, viroids, or fungi (Alberts, Johnson, & Lewis, 2022). The question of whether a pathogen can survive in space is a complex one, with many factors to consider. The short answer is that some pathogens can survive in space. However, much depends on several variables, such as the type of pathogen, gravity, moisture, radiation exposure, and whether it is inside of a vessel or outside of the vessel.

One of the primary factors determining whether a pathogen can survive exposure outside a craft in space is its ability to withstand extreme temperatures and radiation. In space, there is no atmosphere to protect against

solar radiation and other high-energy particles. Any pathogen exposed to these conditions would be subjected to high levels of ionizing radiation, which can damage or destroy genetic material.

However, some viruses are more resistant to radiation than others. For example, research has shown that the bacteriophage T7 virus can survive exposure to high doses of ionizing radiation, even when it is dried onto a surface (Tom, Molineux, Paff, & Bull, 2018). Similarly, studies have found that other viruses, like adenovirus and herpes simplex, can also survive exposure to ionizing radiation (Mezhir, et al., 2005).

Another factor that plays a role in whether a pathogen can survive in outer space is its ability to resist desiccation (drying out). No atmosphere or water vapor creates humidity in space, so any virus exposed to these conditions would quickly dry out. However, some viruses are better adapted to dry environments than others. For example, research has shown that norovirus (which causes gastroenteritis) can survive on surfaces for several days, even when completely dry (Warnes & Keevil, 2013).

Overall, while some pathogens can survive in the vacuum of space, the conditions are harsh and inhospitable. Most organisms would not be able to withstand the extreme temperatures, radiation, and desiccation in space on the outside of a vessel. Furthermore, without a contained environment, pathogens could not reproduce or conduct metabolic processes independently. Instead, they rely heavily on sustainable host environments to replicate and spread.

On the other hand, the inside of a vessel traveling through space is different, carrying humans, moisture, and a protective atmosphere to have pathogens thrive. Spaceflight has further demonstrated to have various effects on microorganisms, including changes in their virulence and antibiotic resistance. Microgravity, radiation, and other spaceflight-related stressors can alter microbial physiology and gene expression, potentially harming outcomes.

For example, one study found that Salmonella typhimurium bacteria grown in spaceflight conditions exhibited increased virulence compared to their ground-grown counterparts (Nickerson et al., 2004). The researchers also observed changes in the expression of genes related to bacterial metabolism, stress response, and pathogenesis.

Another study investigated the effect of spaceflight on Staphylococcus aureus, a common bacterial pathogen that can cause a wide variety of clinical diseases such as Methicillin-Resistant Staphylococcus aureus (MRSA). On the exterior of the human body, it is usually not a threat. Still, if introduced to the bloodstream or internal tissues, it can cause various life-threatening infections. The researchers in the study found that S. aureus grown in spaceflight conditions had increased virulence and antibiotic resistance compared to their "ground-based" counterparts (Kim, et al., 2013).

These studies suggest that spaceflight can change microbial physiology and virulence that may affect human health during prolonged space missions. Continued research in this area is ongoing and needed to understand better the mechanisms underlying these changes and to develop strategies for mitigating potential risks for forward and backward contamination. Understanding these risks helps establish ethical guidelines and protocols for planetary safety and preventing harmful contamination of our world and other celestial bodies.

TYPES OF BIOLOGICAL THREATS IN SPACE

Biological threats in space refer to the risks posed by microorganisms, viruses, and other biological agents to the health and safety of astronauts and space travelers. These threats can arise from various sources, including bacteria, fungi, viruses, plants, contaminated equipment, human carriers, and exposure to extraterrestrial microorganisms. Biological threats and growth in space are a growing concern for the future of space exploration. As humans continue to explore and colonize other planets, they will inevitably bring with them their biological threats and be susceptible to microorganisms from otherworldly sources. In addition, the growth of these organisms in space can be challenging to control due to the lack of gravity and other environmental factors.

BACTERIA

The most common biological threat in space is bacteria. Bacteria are tiny, single-celled organisms that can survive in extreme environments, including those in space. They can cause disease and infection if they contact humans or other living organisms. Bacteria can also reproduce quickly, making them difficult to contain or eliminate once they have established themselves in a new environment.

Bacteria pose a significant threat to space exploration, as they can contaminate spacecraft and potentially harm astronauts. According to the Encyclopedia of Microbiology, "The risk of contamination of other planets or moons with terrestrial microorganisms is a major concern in space exploration" (Lederberg, et al., 2000). Bacteria can survive in extreme conditions, such as those found in space, and potentially colonize other planets or moons unless adequately contained.

One example of the potential danger of bacterial contamination in space exploration is the case of the Mars Viking missions in 1976. As described in the book Planetary Protection: Policy Development and Implementation for Planetary Missions, "The Viking landers were sterilized before launch, but subsequent studies showed that some bacteria survived the sterilization process and could have contaminated Mars" (Race & Lupisella, 2020). These studies raise concerns about the possibility of introducing Earth's microorganisms to other planets and potentially interfering with any native life that may exist there.

Furthermore, bacterial contamination can also pose a threat to astronauts themselves. The book, Astrobiology: A Short Introduction, notes that "Microbial contamination of life support systems onboard spacecraft poses a risk to crew health and performance" (Catling, 2014). This concept is particularly concerning for long-duration missions, such as those planned for future Mars missions, where astronauts exposure to these contaminants for extended periods.

Another example of threats was discovered on the International Space Station (ISS). The ISS is a unique environment that presents several challenges for the survival of microorganisms. Despite the stringent measures taken to prevent contamination, bacteria have been found on various surfaces in the ISS. These

bacteria are of great interest to scientists as they may possess unique characteristics that could be exploited for various applications.

Several studies have reported isolating and identifying bacterial strains from various surfaces in the ISS. These bacteria belong to different taxonomic groups and possess diverse physiological and metabolic properties. For instance, a study by (La Duc, et al., 2007) reported the isolation of 1,271 bacterial strains from 8 locations in the ISS, including the dining table, toilet seat, and exercise platform. Most of these strains belonged to the phyla Actinobacteria, Firmicutes, and Proteobacteria. Another study by (Camilla Urbaniak, 2022) identified a novel bacterial species named Methylobacterium Ajmalii from an air filter in the ISS. This bacterium possessed unique metabolic capabilities that could be exploited for bioremediation purposes.

In March 2021, a new species, named Methylobacterium Ajmaline, associated with three new strains, designated IF7SW-B2T, IIF1SW-B5, and IIF4SW-B5, were reported to have been discovered, for the first time, on the International Space Station.

FIGURE 9-4 Methylobacterium

Source: (Versalovic, 2011)

Bacteria in the ISS raises concerns about their potential impact on human health and equipment functionality. However, some studies have suggested that these bacteria may also have beneficial effects. For example, a study by (Kim, et al., 2013) reported that some bacterial strains isolated from the ISS possessed antimicrobial activity against pathogenic bacteria such as Staphylococcus aureus and Escherichia coli. Additionally, some bacterial strains were found to produce extracellular polymeric substances that could be used for various applications, such as biofilm formation and drug delivery (Mikutta, Guggenberger, Haumaier, Schippers, & Baumgärtner, 2012).

The discovery of unknown bacterium strains in the ISS presents an exciting opportunity for further exploration and research. These bacteria may possess unique characteristics that could be harnessed for various applications, including bioremediation and drug delivery. However, their potential impact on human health and equipment functionality must be addressed, and more studies are needed to fully understand their properties and behavior in the ISS environment.

Bacterial contamination poses a significant threat to space exploration due to its potential impact on

planetary environments and astronaut health. Further strict protocols for sterilization and planetary protection are necessary to ensure the safety and success of future space missions.

FUNGI

Fungus is another type of biological threat that is in space. Fungi are microscopic organisms that feed on organic matter, such as plants and animals. Left unchecked, they can cause diseases such as athlete's foot, ringworm, and cancer. Fungi can also reproduce quickly, making them difficult to contain or eliminate once they have established themselves in a new environment. Fungi are a diverse group of organisms that play essential roles in various ecosystems on Earth. However, they can also threaten space travel and exploration, as they are known to thrive in extreme environments, such as deserts and the deep sea. They can potentially contaminate spacecraft and planetary surfaces. According to the Encyclopedia of Microbiology, "Fungi are ubiquitous on Earth and can survive under extreme conditions of temperature, pH, radiation, and desiccation" (Rummel, Allton, & Morrison, 2011). This resilience makes them a formidable challenge for space exploration missions, where there should be a minimized risk of contamination.

One of the main concerns with fungal contamination is its potential to interfere with scientific experiments. Fungi can grow on equipment and instruments, affecting their accuracy and reliability. For example, fungal growth on optical lenses can cause distortion or obstruction of the images (Rummel, Allton, & Morrison, 2011). Fungal contamination can also affect the integrity of samples collected from other planets or moons, potentially altering, or destroying valuable data.

Another potential problem is fungi's presence in spacecraft's air filtration systems. The Journal of Applied Microbiology noted, "Air filtration systems are designed to remove particulate matter from the air, but they may not effectively remove fungal spores" (Howell, 2023). Even if a spacecraft is thoroughly cleaned before launch, it may still be contaminated with fungal spores that could grow and spread during the mission, increasing the potential for fungi to cause health problems for astronauts. Fungal spores, if inhaled, cause respiratory issues or allergies. Some species of fungi produce mycotoxins, which can be harmful if ingested or inhaled. In addition, prolonged exposure to fungi can weaken the immune system, making astronauts more susceptible to other infections.

Another concern is the potential for fungi to contaminate food supplies. The book Astrobiology: A Very Short Introduction explains that "Fungal contamination of stored food is a major problem on Earth and could be an even greater problem on long-duration spaceflights" (Catling, 2014). Fungal growth on food could render it inedible and release toxins that could harm astronauts.

In addition to these practical concerns, there is also a scientific interest in studying how fungi behave in space environments. However, as noted in the book Fungi in Biogeochemical Cycles, "The study of fungi in space is complicated by the need to prevent contamination of extraterrestrial environments with terrestrial microorganisms" (Gadd, 2006). Fungi can also pose a threat to planetary protection efforts. The Outer Space Treaty of 1967 requires that all space missions avoid harmful contamination of celestial bodies (United

Nations Office for Outer Space Affairs, 2023). If fungi were to contaminate another planet or moon, it could potentially introduce Earth-based life forms that could interfere with any native life that may exist there. Fungi contamination means strict protocols ensure that fungi experiments do not inadvertently introduce them into the studied environment.

The threat of fungal contamination is a significant challenge for space exploration missions. As the book Space Microbiology states, "The potential for contamination of extraterrestrial environments with terrestrial microorganisms is a critical issue for all space exploration missions" (Stutte, Flynn, & Acevedo, 2008). Careful planning and rigorous cleaning protocols must be in place to ensure that spacecraft and habitats remain free of fungal contamination; this will mitigate risk.

VIRUSES

"Viruses are entities whose genomes are elements of nucleic acid that replicate inside living cells using the cellular synthetic machinery and causing the synthesis of specialized elements that can transfer the viral genome to other cells" (Luria, Darnell, Baltimore, & Campbell, 1978). The newly developed discipline of studying viruses in space is called Astrovirology, a subdiscipline of astrobiology.

The possibility of viral contamination in space is a significant concern for space agencies and scientists. The presence of viruses in spacecraft or on extraterrestrial surfaces could pose a threat to astronauts' health and compromise scientific research. Viruses are much smaller than bacteria and can spread through contact with infected individuals or objects. They can cause serious illnesses such as influenza, measles, and even HIV/AIDS if left unchecked. Viruses can also mutate quickly, making them difficult to treat or contain once introduced into a new environment.

One of the primary concerns regarding viral contamination is the potential for viruses to mutate in space. Research has shown that microgravity can alter the behavior of viruses, making them more virulent or resistant to treatment (Aunins, et al., 2018). Microgravity could lead to new, more dangerous strains that could be difficult to control. Additionally, harmless viruses on Earth could become dangerous in space due to changes in the immune system and other physiological factors.

Another concern is the potential for viruses to spread rapidly in the confined environment of a spacecraft. As humanity continues to explore space, the possibility of encountering viruses becomes a growing concern. While space is a sterile environment, spacecraft and other equipment sent into space are not as germ-free. These objects can carry microorganisms, including viruses, which could threaten astronauts and their missions. With close quarters and recycled air systems not working correctly, it could facilitate the transmission of viruses between crew members, potentially leading to an outbreak (Novikova, 2006). Furthermore, viruses are likely the most common cause of infectious disease attributed to enclosed environments. Close personal contact within a spacecraft or a space colony makes them ideal places to spread viral infections.

Astronauts experience a weakened immune system when they travel in space. One research study showed that Increased levels of stress hormones such as cortisol, dehydroepiandrosterone, epinephrine, and

norepinephrine, coupled with a decreased cell-mediated immunity, contributed to the reactivation of latent herpes viruses in astronauts (Rooney, 2019). The study also included that viral reactivation was evident through the shedding of viral DNA in the body fluids of astronauts, and the viral load only increased with more time in space. As the viral load increased, it naturally triggered an increase of viral shedding by 60%, and with some subjects, the shedding increased by 96% (Rooney, 2019). Additionally, more than one virus reactivates at a time, potentially compounding the physiological ramifications of uncontrolled viral reactivations such as rashes, severe organ failures, and permanent loss of hearing and vision.

In addition to the risks posed by viruses carried from Earth, there is also the possibility of encountering unknown viruses in space. As we explore further into the cosmos, we may encounter microorganisms we have never faced before. New microorganisms could lead to the discovery of new valuable and helpful pathogens, but it also poses a risk if they are harmful.

To help mitigate the risks, a recent study by researchers using the ISS investigated the evolution of bacteriophages or phages (viruses that infect and kill potentially harmful bacteria) in microgravity conditions. The study was groundbreaking in that if phages can mutate in the micro-gravity environment, it could enhance the phage's ability to attack or limit the bacteria's ability to defend (Howell, 2023). The result is a new antibiotic that could help keep harmful bacteria subdued during long-distance space travel and increase the health of astronauts.

While the threat of viral contamination in space is a significant concern, scientists and space agencies mitigate these risks through scientific discovery, rigorous sterilization protocols, medical screening, and research into new antiviral treatments.

RADIATION

Although radiation is not a threat from biology, prolonged exposure to radiation in space can significantly affect microorganisms and astronauts. One of the potential consequences is the development of genetic mutations that could lead to the emergence of new pathogens. The high-energy particles present in space can damage DNA, leading to changes in the genetic code that can alter the function of proteins and enzymes (Durante, 2008). These changes can have a range of effects, from benign to harmful, and potentially result in the emergence of new, pathogenic microorganisms.

Studies have shown that exposure to ionizing radiation can induce mutations in various microorganisms, including bacteria and fungi. For example, research has demonstrated that exposure to gamma radiation can cause mutations in the bacterium Escherichia coli (E. coli) that lead to increased resistance to antibiotics (Catling, 2014). Other studies have shown that radiation exposure can increase the virulence of specific fungal pathogens, such as Aspergillus fumigatus (Blachowicz, et al., 2020).

The potential for radiation-induced mutation to lead to the emergence of new pathogens is a concern for space exploration, as astronauts are exposed to higher levels of radiation than they would experience on Earth. Astronauts on long-duration space missions risk developing infections due to weakened immune systems

caused by prolonged exposure to radiation and other factors (Bijlani, Stephens, Singh, Venkateswaran, & Wang, 2021). In addition, microorganisms carried on spacecraft or present in space habitats could be exposed to these high radiation levels.

While there is still much to learn about the effects of radiation on microorganisms, prolonged exposure to high radiation levels can induce genetic mutations that could lead to the development of new pathogens. This underscores the need for careful monitoring and mitigation strategies to minimize the risks associated with radiation exposure during space exploration.

EXTRATERRESTRIAL PATHOGENS

As space exploration advances, the possibility of encountering extraterrestrial life becomes more likely. While this may be an exciting prospect, it also presents potential dangers, particularly extraterrestrial pathogens. These pathogens could pose a significant threat to space travel and the health of astronauts. A primary concern with extraterrestrial pathogens is that they may be completely unknown to humans. We have yet to learn what organisms might exist in other worlds or what diseases they might provoke. This lack of knowledge makes preparing for potential infections and illnesses challenging.

Furthermore, extraterrestrial pathogens may be able to survive in environments that are hostile to human life. For example, some bacteria on Earth can survive in extreme temperatures and radiation levels. If similar organisms exist on other planets, they could infect humans who encounter them. According to one study, changes in human microbiology due to the conditions of space travel and the adaptation of earth-borne pathogens to alien environments could also lead to the emergence of modified microorganisms with vastly different pathogenic potentials (Mihai G. Netea , 2020).

Another concern is the potential for backward contamination of extraterrestrial pathogens in rock and dust samples. Carl Woese, a Nobel Prize–nominated biophysicist at the University of Illinois, once stated, "When the entire biosphere hangs in the balance, it is adventuristic to the extreme to bring Martian life here. Sure, there is a chance it would not harm; but that is not the point. Unless there is less chance that it might harm, one should not embark on such a course" (DiGregorio, 2001). Many researchers in the scientific community believe the odds are low that we would ever find life within our solar system. However, realizing our lack of understanding about pathogens from other worlds is essential.

Space agencies must take precautions when exploring other planets and celestial bodies to mitigate these risks. Samples must be cautiously handled and analyzed to the best of our ability so there are no false assumptions. Additionally, any samples from other planets must be carefully contained and studied in a secure laboratory environment. One of the safest ways to protect Earth from extraterrestrial pathogens would be a quarantine facility placed on the moon. A publication produced by the Lunar and Planetary Institute's Workshop on Mars Sample Return in 1988 outlined how a facility on the moon would offer "significant advantages" over other locations (Davidson, 1988). It would offer a form of low gravity, vacuum, distance from Earth, and accessible communication.

In conclusion, while discovering extraterrestrial life would be groundbreaking, it also presents potential hazards in the form of extraterrestrial pathogens. As space exploration continues, we must take precautions to protect astronauts and Earth from these threats.

IMPACT OF BIOLOGICAL THREATS ON SPACE EXPLORATION

HEALTH RISKS TO ASTRONAUTS

There are several health risks from biological threats that astronauts may encounter during space missions. These include bacterial infections, viral infections, fungal infections, allergic reactions, or even extraterrestrial pathogens. Bacterial infections are a significant concern as they can thrive in the microgravity environment of spacecraft and become resistant to antibiotics (M A Juergensmeyer, 1999). Viral infections are also a concern as they can spread rapidly in closed environments such as spacecraft. Fungal infections may also pose a threat as they can grow on surfaces and equipment within the spacecraft. Allergic reactions to environmental factors such as dust and pollen may also occur. The possibility of encountering extraterrestrial pathogens is also possible. However, how our immune system would react to extraterrestrial pathogens and cause health risks is still being determined.

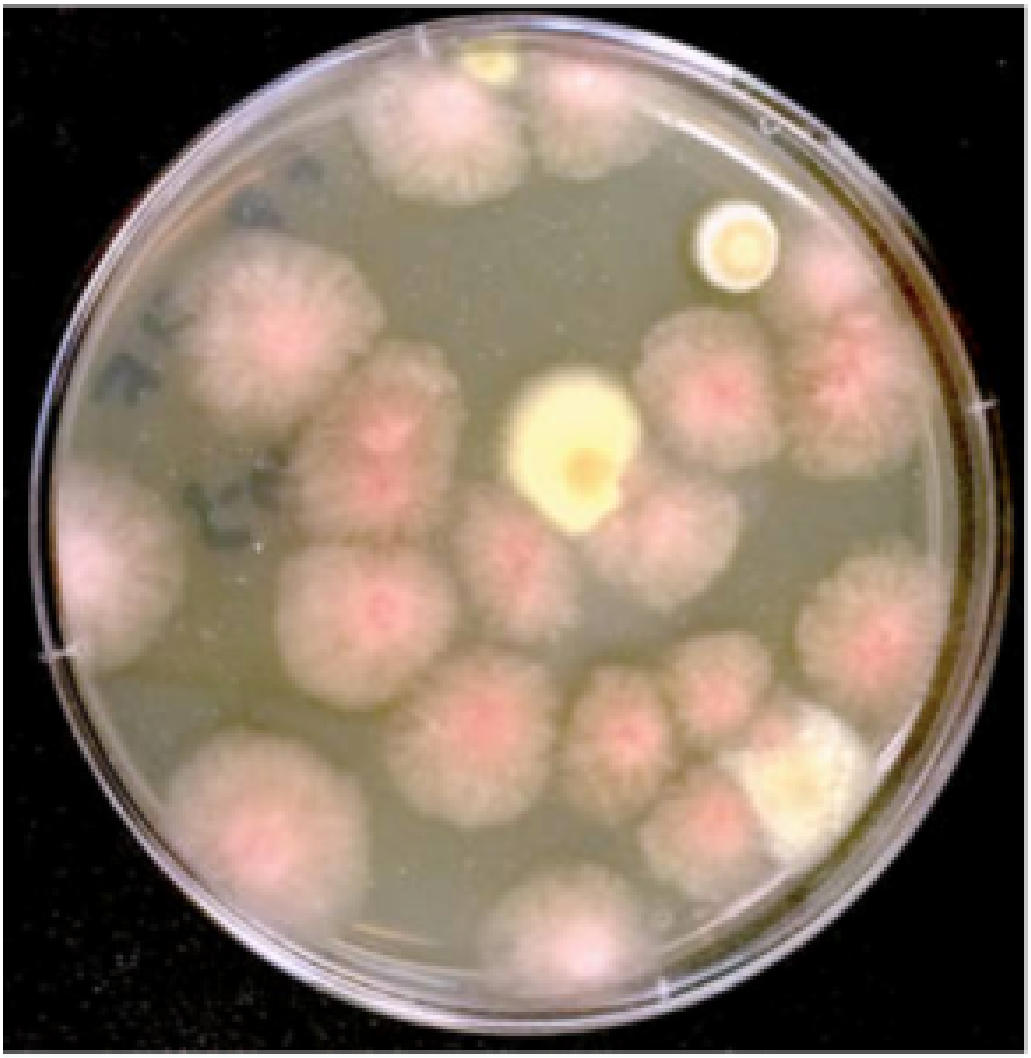
The health effects of biological threats on astronauts can range from mild symptoms to severe illness or even death. Bacterial infections can cause various symptoms, including fever, chills, nausea, vomiting, and diarrhea. Viral infections can cause similar symptoms but may lead to respiratory problems and pneumonia. Fungal infections can cause skin irritations or more severe respiratory problems if inhaled. Allergic reactions can cause symptoms such as itching, swelling, and difficulty breathing (Ball & Evans, 2001).

One of the significant health risks associated with biological threats in space is the increased virulence of microbes due to microgravity conditions. According to a Microbiology and Molecular Biology Reviews study, microgravity can alter microbial gene expression, metabolism, and behavior, increasing virulence and antibiotic resistance (Wilson, 2007). Furthermore, spaceflight has been shown to alter immune function, leading to increased susceptibility to infections and decreased vaccine efficacy (Crucian, 2015), posing a significant threat to the health of astronauts, who may be more susceptible to infections while in space.

To realize the scope of health risks to astronauts, NASA began a three-part investigation of potential disease-causing microorganisms aboard the International Space Station (ISS) from 2015 to 2021. These studies are known as the Microbial Tracking-1 (MT-1), Microbial Tracking-2 (MT-2), and Microbial Tracking-3 (MT-3) experiments. The MT-1 experiment aimed to study the effects of microgravity on the virulence of microbes (Lang et al., 2017), while the MT-2 project focused on furthering the research of MT-1 by understanding how microgravity affects the immune system of astronauts (Urbaniak, 2022). Finally, the MT-3 project expands on past experiments by studying the response of microbial cells to the spaceflight environment and evaluating DNA structures for microbes cultured in spaceflight (Gilbert, 2022). All the studies collected samples from eight different surfaces, including air and water sources, using swabs, filters, and other collection devices. Samples taken directly from astronauts were also taken during the MT-2 experiment.

The MT-1 & MT-2 experiments revealed diverse microbial communities within the ISS environment. The study identified the potential source of microbial contamination from crew members and cargo shipments. Most bacteria and fungi detected from surfaces were derived from human skin but became unique due to the enclosed microgravity environment. The most prominent bacteria and fungi found were Staphylococcus, Cutibacterium, Streptococcus, Haemophilus, and Malassezia. These pathogens cause various human health risks, including food poisoning, respiratory infections, and skin infections. The study also found that the pathogens had "resistance capabilities against 17 classes of drugs, many of which were broad-spectrum antibiotics, such as aminoglycosides, beta-lactams, fluoroquinolones, and tetracycline, all of which are part of the medical toolkit onboard the ISS" (Urbaniak, 2022). The results of the MT-3 experiments are currently still in progress.

FIGURE 9-5 Fungi from the Microbial Tracking-1 experiment



Source: (Landau, 2016)

Lastly, the possibility of encountering extraterrestrial pathogens has been a topic of interest for scientists and researchers for many years. The immune system is crucial in defending the host against pathogenic invaders. However, how our immune system would defend against extraterrestrial pathogens is still being determined.

One health risk for astronauts is that their immune system may not recognize the extraterrestrial pathogens as foreign and fail to mount an effective defense. According to the Encyclopedia of Astrobiology, "The immune system is particular and evolved to recognize and respond to Earth-based pathogens" (Muriel Gargaud, 2011). It is possible that our immune system will not recognize or have the appropriate defense against extraterrestrial pathogens due to their unique molecular structures.

While space exploration has brought us many advancements and discoveries, it poses significant health risks to astronauts. We do not understand how space travel alters a microbe's ability to adapt in space or what risks alien organisms could have on astronauts. Continued research studying microbial threats in space is an essential area of research that can provide valuable insights into its effects on human health.

IMPACT ON SPACECRAFT AND EQUIPMENT

One of the most significant threats that impact spacecraft, and its equipment is heavy contamination from biofilms. Most materials used in spacecraft construction cannot resist biofilm formations and require continual maintenance and sterilization to prevent formation. These threats can range from a broad assortment of bacterial and fungal growths presenting failures in essential equipment and dangers to astronauts (Urbaniak, 2022). In this section, we will explore the impacts that biological threats can have on spacecraft and equipment during space travel.

Microbial contamination can occur in various ways, such as by introducing bacteria, viruses, or fungi from Earth or human sources. This contamination can lead to the growth of microorganisms called biofilm on surfaces within the spacecraft, which can cause corrosive damage to essential equipment and distort the reliability of tests and other experiments (V.B. Vasin, 1995). According to NASA, biofilms on the Mir space station and the ISS have been observed clogging air and water purification systems that provide astronaut life support (Figliozzi, 2013).

Corrosion is caused by a chemical reaction that occurs when metal or polymers are exposed to oxygen and moisture. Microorganisms can accelerate corrosion by producing acidic compounds that corrode metal and plastic surfaces at a higher rate (Lekbach, 2011). This corrosion can weaken equipment and structures within the spacecraft, potentially leading to equipment failure or structural damage. Aboard the Mir space station, colonies of organisms were also found growing on "the rubber gaskets around windows, on the components of space suits, cable insulations, and tubing, on the insulation of copper wires, and communications devices," said Andrew Steele, a senior staff scientist at the Carnegie Institution of Washington working with other investigators at Marshall Space Flight Center (Bell, 2004).

Biological threats can also impact the performance of other electronic equipment within the spacecraft. Microorganisms can generate electrostatic charges that interfere with electronic signals and disrupt

communication systems (Chandan K. Sen, 2020). This interference can cause malfunctions in critical systems, such as life support or navigation systems.

In conclusion, biological threats pose a significant risk to spacecraft and equipment during space travel. Contamination, corrosion, and interference with essential systems are just a few examples of the impacts that these threats can have. Space agencies need to take measures to prevent and mitigate the risks associated with biological threats to ensure the safety of astronauts and the success of space missions.

ECONOMIC IMPACTS

Space exploration has always been associated with various risks and challenges. A significant concern is potential biological threats that may arise during space missions. These threats can have severe economic impacts on space-based programs, affecting the immediate mission and long-term investments in space exploration. This section explores the economic implications of biological threats in space exploration, highlighting such risks' potential costs and consequences.

1. **Impact on Mission Costs**:

Biological threats in space exploration can significantly impact mission costs. The presence of harmful microorganisms or pathogens onboard spacecraft can lead to contamination, resulting in a need for extensive decontamination procedures. These procedures require additional resources, including specialized equipment, disinfectants, and trained personnel, which can escalate mission costs. Moreover, the delay caused by decontamination processes may result in missed launch windows and rescheduling, further increasing expenses.

2. **Investment Uncertainty**:

The emergence of biological threats in space exploration introduces uncertainty in future investments. Potential contamination incidents could lead to public concerns and a loss of confidence in space agencies or private companies involved in space missions. Investors may hesitate to fund projects due to the perceived risks associated with biological threats. This uncertainty can hinder the flow of capital into space exploration programs, limiting their growth and development.

3. **Impact on International Collaboration**:

Biological threats in space exploration can strain international collaborations. In case of contamination incidents involving multiple countries or agencies, disputes may arise regarding responsibility and liability for the incident. Contamination incidents can lead to strained relationships and hinder future collaborative

efforts. The breakdown of international partnerships can result in restricted access to shared resources and expertise, affecting the progress and cost-effectiveness of space exploration missions.

4. **Public Perception and Support**:

Biological threats in space exploration can influence public perception and support for space programs. Contamination incidents can generate adverse publicity, raising concerns about the safety of space missions. This negative perception may lead to a decline in public support and reduced funding for space exploration programs. A decrease in public funding could limit the resources available for research, development, and future missions.

5. **Regulatory Compliance:**

The presence of biological threats in space exploration requires adherence to strict regulatory guidelines and protocols. Space agencies and private companies must comply with international regulations to ensure crew members' safety, prevent celestial body contamination, and protect Earth's biosphere (Belz, 2005). These compliance measures add additional costs to space exploration programs, including implementing stringent sterilization procedures and ongoing monitoring.

Overall, biological threats in space exploration can have significant economic impacts. The costs associated with decontamination procedures, investment uncertainty, strained international collaborations, public perception, support, and regulatory compliance can all contribute to increased expenses and hinder the progress of space exploration programs.

MITIGATING BIOLOGICAL THREATS IN SPACE

To protect against these potential biological threats, astronauts and scientists must take precautions when exploring new environments in space. This includes avoiding contact with unknown organisms whenever possible, sterilization techniques, quarantine measures, and wearing protective clothing whenever necessary. Additionally, astronauts need to monitor their health closely while in space so that any signs of illness or infection can be addressed quickly before it becomes a more significant problem for the mission team or other personnel on board the spacecraft.

STERILIZATION TECHNIQUES

Sterilization is crucial in space missions to prevent contamination of extraterrestrial environments with terrestrial microorganisms. The National Aeronautics and Space Administration (NASA) continuously

utilizes and develops various sterilization techniques to ensure that spacecraft and equipment sent to space are free of viable microorganisms. This section will discuss the different sterilization techniques used in modern space missions.

One of the approved sterilization techniques is dry heat sterilization. This method involves subjecting equipment to temperatures ranging from 160°C to 180°C for several hours. The high temperature kills all microorganisms, including bacterial endospores, and ensures that no viable organisms remain on the spacecraft (Belz et al., 2005).

Another widely used technique is chemical sterilization. This method involves using chemicals such as hydrogen peroxide or ethylene oxide to kill microorganisms instead of heating thermally sensitive electronics and hardware materials. Vapor phase hydrogen peroxide (VHP) is an alternative sterilization technique where equipment is placed in a sealed chamber with a vacuum, and the chemical is introduced into the chamber and kills all microorganisms present (Chen et al., 2013).

Finally, ultraviolet (U.V.) radiation is another method of sterilizing surfaces and equipment. The system is based on the Ultraviolet Germicidal Irradiation (UVGI) method of disinfection, where U.V. light, at sufficiently short wavelengths, is used to damage the DNA of microorganisms, rendering them unable to reproduce and kill microorganisms. However, this method is less effective against bacterial endospores (Eagan & Ridinger, 2017).

In closing, sterilization is critical in modern space missions to prevent contamination of extraterrestrial environments with terrestrial microorganisms. NASA has developed various sterilization techniques, including dry heat sterilization, chemical sterilization, and U.V. radiation. New sterilization techniques are being researched and will be used in future missions.

QUARANTINE MEASURES

Quarantine measures are essential in space travel and on Earth to avoid the lethality of alien biological threats. The risk of contamination from extraterrestrial life forms is a genuine concern for space agencies. To mitigate these risks, quarantine measures are implemented to prevent contamination from alien and earth-born biological threats. Quarantine measures include isolation procedures, decontamination processes, and strict crew health monitoring. There are several types of quarantine measures used for space travel:

- Pre-flight quarantine involves isolating astronauts from the general population before launch to prevent the spread of illness or infection.
- In-flight quarantine: includes isolating astronauts from each other and the rest of the spacecraft to prevent the spread of disease.
- Post-flight quarantine measures: isolating astronauts after returning to Earth to ensure they are not carrying harmful pathogens.
- Emergency quarantine procedures are designed to be implemented quickly in case of a medical

> emergency or disease outbreak on board a spacecraft. Emergency quarantine procedures may involve isolating affected individuals, decontaminating the spacecraft, or even aborting the mission if necessary. Isolation may be voluntary or involuntary, depending on the circumstances. Personal protective equipment (PPE) or Biological Isolation Garments have also been used to isolate an individual or be used by others to protect themselves (Dasch & O'Mara, 2018).

The primary quarantine measure is using a quarantine facility upon return to Earth. In 1964, federal officials and scientists assembled to discuss the possibility that microbes from the Moon or other worlds could potentially contaminate the Earth. Dr. Carl Sagan argued that lunar travelers might bring deadly organisms back with them that could theoretically destroy life on Earth (Carter, 2001). Congress shortly realized that rigorous quarantine protocols were needed to isolate astronauts, spacecraft, and lunar samples to prevent back-contamination from any possible lunar microorganisms into Earth's biosphere. Congress authorized NASA to build the specially designed Lunar Receiving Laboratory (LRL) in Houston, where returning astronauts, their spacecraft and all the samples of lunar material could be kept in strict quarantine and tested to determine if they posed a threat to the planet (Mars, 2021). The facility was completed in 1967 and was equipped with specialized air filtration systems, sealed dormitories, vacuum systems, a rare gas analysis system, a physical-chemical test area, vacuum glove boxes, and the radiation counting laboratory that was built 50 feet underground (Uri, 2021). Biological monitoring was also an essential part of the quarantine process. Samples of air, water, and surfaces within the laboratory were regularly tested for any signs of microbial growth or other contaminants. All waste products and equipment were also heavily sterilized before entering and leaving the facility.

Quarantine measures administered in the LRL were taken seriously. In a recent article by Dagomar Degroot, he explains, "LRL technicians agreed that if they were exposed to lunar contaminants and quarantined, they would not attempt to escape. If exposure killed them, their relatives could not claim their bodies. Rough plans drafted by NASA officials imagined that guards would seal the facility at gunpoint in case of a dangerous breach of lunar organisms that threatened to spill beyond the LRL. If all else failed, the entire facility and everyone inside it would be buried under a mountain of dirt and concrete (Scoles, 2023).

As space exploration advances, new quarantine measures must be developed to address new challenges. For example, future missions to Mars or other planets may require more extended periods of isolation and more extensive decontamination procedures due to the risk of contaminating these planets with Earth-based microbes (Keith, 2021). Modern policies are frequently being developed by the Committee on Space Research (COSPAR) and their special Panel of Planetary Protection, whose primary objective is to develop, maintain, and promote the COSPAR policy and "to protect against the harmful effects of forward and backward contamination" (European Space Agency, 2023). Modernized facilities are also being constructed. In 2017, NASA's Johnson Space Center unveiled Building 21, home of the Human Health and Performance Laboratory. Additionally, new technologies such as 3D printing and autonomous robots may reduce the risk of contamination by minimizing human contact with potentially contaminated surfaces.

USE OF PROTECTIVE EQUIPMENT

Modern space missions require protective equipment against biological threats to ensure the safety of astronauts and prevent the spread of harmful microorganisms. The use of protective equipment has become increasingly important as space exploration expands, and missions become longer. In this section, we will discuss the types of protective equipment used in modern space missions and how they are utilized to protect against biological threats.

One of the primary forms of protective equipment used in space missions is the spacesuit. Spacesuits are designed to provide a sealed environment for astronauts, protecting them from the vacuum of space, extreme temperatures, and harmful radiation. In addition to these hazards, spacesuits also protect against biological threats. Spacesuits are equipped with air filters that remove contaminants from the air before astronauts breathe it in (NASA, 2023). The suits are also made from materials resistant to microbial growth, preventing harmful bacteria or virus accumulation.

Another form of protective equipment used in space missions is personal protective equipment (PPE). PPE includes items such as gloves, masks, and gowns that are worn by astronauts when managing potentially hazardous materials. PPE is essential for preventing the spread of harmful microorganisms between crew members or back to Earth (NASA, 2021). PPE is also used during medical procedures or experiments involving biological samples.

In addition to spacesuits and PPE, spacecraft are equipped with environmental control systems (ECS) that help maintain a clean and sterile environment. ECS systems filter and purify the air inside spacecraft, removing contaminants that could threaten crew members (National Research Council; Division on Engineering and Physical Sciences; Commission on Engineering and Technical Systems; Committee on Advanced Technology for Human Support in Space, 1997). These systems also regulate temperature and humidity levels to prevent the growth of microbes.

To further protect against biological threats, NASA and the COSPAR Panel on Planetary Protection have implemented strict protocols for overseeing biological samples and conducting experiments involving living organisms. These protocols include sterilization procedures for equipment and surfaces and quarantine measures for crew members returning from space (NASA et al., 2020).

In conclusion, modern space missions require various protective equipment to ensure the safety of astronauts and prevent the spread of harmful microorganisms. Spacesuits, PPE, ECS systems, and strict protocols for managing biological samples are essential to modern space exploration.

FUTURE CHALLENGES AND OPPORTUNITIES FOR GROWTH

THE ROLE OF ADVANCED TECHNOLOGIES

Space exploration has always been a subject of great interest for scientists and researchers. As humans venture farther into space, it becomes crucial to understand and overcome the challenges posed by extended periods of space travel. One area that holds immense potential is advanced biological technologies. By harnessing the power of biology, scientists can develop innovative solutions to ensure the well-being and sustainability of astronauts during long-duration missions. This section examines several advancements in biotechnology that enable the further development of innovative solutions for sustaining life in space.

1. **CRISPR** (Clustered Regularly Interspaced Short Palindromic Repeats): is a gene-editing tool that allows scientists to make precise changes to DNA sequences. It has revolutionized the field of genetics and has numerous applications in medicine, agriculture, and biotechnology. In 2017, a team of scientists launched the Genes in Space-3 mission to study the effects of microgravity on DNA using a MinION CRISPR device. The researchers used CRISPR to edit specific genes in the DNA samples and then sequenced the edited DNA to see if microgravity caused any changes. The experiment results showed that microgravity did not cause significant changes in DNA sequences compared to earth-based experiments (Sarah Stahl-Rommel, 2021). This opened a significant door for the future use of CRISPR technology for space exploration.

Using CRISPR technology in space has significant implications for future space exploration and colonization. It could be used to genetically engineer plants and animals to withstand the harsh conditions of space or to treat genetic diseases in astronauts. However, there are ethical concerns about using gene-editing technology in space and the potential risks and consequences. A common concern is the potential for unintended consequences. Gene editing is a relatively new technology, and much is still unknown about its long-term effects. It is possible that genetic modifications made for space travel could have unintended consequences that are not apparent until years or even decades later (William, 2022).

However, the Genes in Space-3 experiment demonstrated the feasibility of using CRISPR technology to study DNA mutations in microgravity. It opens new avenues for genetics research and has potential space exploration and colonization applications.

2. **Synthetic phages**: Synthetic phages are genetically engineered viruses designed to target specific bacteria strains by modifying their genetic material. Their ability to combat bacterial infections makes them a promising tool against serious threats posed by drug-resistant bacterial infections during long-duration space missions. Phages have been used as a natural alternative to antibiotics for decades; however, synthetic modifications allow phages to recognize and destroy specific bacteria while leaving beneficial microorganisms unharmed.

Numerous research efforts are underway to develop synthetic phages for space exploration. Scientists are focusing on improving their efficacy, stability, and delivery methods. Additionally, the "Phage-Evolution" study is currently being conducted on the International Space Station (ISS) to understand the impact of microgravity on synthetic phage performance (NASA, 2020).

3. **Artificial Intelligence (A.I.) and Autonomous Systems**: A.I. has emerged as a powerful tool in various fields, including space exploration and mitigating biological threats. The ability of A.I. systems to analyze vast amounts of data, make autonomous decisions, and adapt to changing environments makes them invaluable in space exploration domains. Robotics are also crucial for performing complex tasks in space exploration. From sample collection and analysis to remote sensing, maintenance, teleoperation, and planetary exploration, robots play a vital role in ensuring the safety of astronauts. A.I. coupled with robotics (autonomous systems) can push robotics further, perform experiments, repair equipment, and even assist astronauts. The use of autonomous systems reduces human risk while enhancing the efficiency and effectiveness of space missions.

According to NASA, trusted autonomy within autonomous systems is a critical technology area necessary for the future of human and robotic space exploration (Bryan, 2020). A.I. has the potential to play a crucial role in combating biological threats in space but must be as dependable and capable as a human. By leveraging autonomous systems, scientists and researchers can enhance their ability to detect, analyze, and respond to threats without ever putting a human at risk. A.I. can be utilized to develop advanced algorithms that can quickly identify and classify various pathogens, monitor the spread of diseases, and predict their potential impact within a closed-loop system on space missions (Sanders, 2023). Furthermore, A.I. can aid in developing autonomous systems capable of performing medical procedures and administering treatments in space environments.

A workshop organized by the National Aeronautics and Space Administration on artificial intelligence, machine learning, and modeling applications in 2023 shared that a central goal of developing and employing autonomous, AI-supported bio-experimentation systems such as self-driving laboratories should be to generate longitudinal data (Sanders, 2023). The data gathered could inform autonomous health systems that provide decision support for crew health management during space missions.

4. **Digital to Biological Converters**: DBCs are innovative devices that convert biological sequence information from a transmitter location into biological material at a receiving unit. The system also has an assembly unit connected to the receiving unit, and the assembly unit assembles the biological entity according to the biological sequence information (Gill, 2021). DBCs utilize synthetic biology techniques to encode digital data into DNA sequences, which can then be synthesized and expressed in living organisms. This technology enables storing and retrieving vast amounts of information in a biologically stable format. DBCs can also be engineered to detect specific genetic signatures associated

with known pathogens or harmful organisms. By leveraging their ability to convert digital information into biological material, DBCs enable rapid and targeted detection of potential threats.

The key to the technology is that the transmitting or receiving units can be present at remote locations on Earth (Gill, 2021). This presents itself to be a valuable application to space exploration. For example, if an autonomous system collects a sample that contains life on another planet, its biological sequence could be analyzed, digitalized, then sent to a receiving unit via broadcast on Earth, and the assembly unit could build the lifeform synthetically in a safe environment on Earth. This would eliminate variables within the transfer of the organism, such as cost, travel time, and exposure issues. On the other hand, if a receiving and assembly unit were available on a Mars colony, the DBC could digitally transmit a valuable protein as a vaccine sequence from Earth (Gill, 2021).

5. **Quantum Computing**: Quantum computing utilizes the principles of quantum mechanics to perform computations. Unlike classical computers that use bits to represent information as either a 0 or 1, quantum computers use qubits, which can exist in multiple states simultaneously due to a phenomenon called superposition (Giles, 2019). This property allows quantum computers to simultaneously process vast amounts of information, leading to exponential computational power. In recent years, researchers have explored the potential applications of quantum computing in various fields, including space exploration.

Quantum computers have the potential to significantly enhance data processing capabilities significantly, enabling faster analysis of large datasets. In the context of biological threat detection, this facilitates the rapid identification and analysis of pathogens or biological agents that pose risks to astronauts during space missions. Quantum computing can also provide robust simulation and modeling tools for predicting the behavior of biological threats in space environments. By simulating the interactions between pathogens and various environmental factors, scientists can gain insights into how these threats may evolve and adapt in space conditions (Giles, 2019). Quantum machine learning algorithms can improve the accuracy and speed of pattern recognition, enabling the detection of subtle biological threat indicators in large datasets (Ahsan, Luna, & Siddique, 2022). This can aid in identifying and mitigating potential risks during space exploration missions.

Quantum computing holds great promise for detecting and mitigating biological threats during space exploration. Its ability to process vast amounts of data, simulate complex systems, optimize designs, and enhance pattern recognition can revolutionize our ability to safeguard astronauts from potential biological hazards. However, further research and development are required to overcome technical challenges and realize the full potential of quantum computing in this domain.

CONCLUSIONS

Advanced biological technologies hold immense potential for space exploration. Today, serious researchers who devote energy to assessing realistic threats may consider advanced technology's unrecognized but revolutionary evolution (Sincavage & McCreight, 2019). Understanding the effects of space travel on human physiology is crucial for developing effective countermeasures. Utilizing autonomous systems supported by A.I. could pave the way for creating sufficient environments before humans set foot on other worlds. Advancements in biotechnology that enable genetic modifications that enhance an organism's adaptability to space environments could create advanced life support for long-duration missions. Bio-generative support using digitally transmitted systems offers a sustainable solution for long-duration missions. By harnessing the power of biology, scientists can pave the way for successful and sustainable space exploration.

COLLABORATIVE EFFORTS WITH INTERNATIONAL SPACE AGENCIES

As space exploration advances, international collaboration has become crucial to scientific progress and technological development. This section explores the future collaborative efforts between space agencies from different countries. It examines the importance of these partnerships, potential areas of collaboration, and the benefits they bring to the global space community.

International collaboration in space exploration is essential for several reasons. Firstly, it allows for sharing of resources, expertise, and technology among participating nations. This cooperation enables countries to pool their knowledge and capabilities, leading to more efficient and cost-effective missions. Secondly, collaboration fosters diplomatic relations and strengthens international ties, promoting peace and understanding among nations. Lastly, by working together, space agencies can tackle complex challenges that only some countries can overcome, such as long-duration space travel or the colonization of other planets.

There are numerous areas in which international space agencies can collaborate to further scientific knowledge and technological advancements. One key area is deep space exploration. By combining resources and expertise, agencies can jointly plan and execute missions to destinations beyond Earth's orbit, such as Mars or the outer planets. Another area is the development of advanced detection systems. Collaborative efforts can lead to the creation of advanced sensor technologies that enable fast analysis of planetary bodies for life or biological threats. Additionally, international cooperation in satellite technology can enhance communication networks, weather forecasting, and planetary observation systems.

Collaboration between international space agencies yields several benefits for all participating nations. It promotes knowledge exchange and learning opportunities among scientists and engineers from different countries. This cross-pollination of ideas leads to innovation and the development of new technologies. Furthermore, collaborative missions allow for cost-sharing, reducing the financial burden on individual agencies and enabling more ambitious projects. Lastly, international partnerships foster cultural understanding and cooperation, contributing to peaceful relations among nations. The Space Treaty is an

excellent example of collaboration which addresses that" the exploration and use of outer space shall be conducted for the benefit and in the interests of all countries and shall be the province of all mankind" (United Nations Office for Outer Space Affairs, 2023).

Future collaborative efforts between international space agencies hold great potential for advancing space exploration and benefiting humanity. By pooling resources, expertise, and technology, space agencies can tackle complex challenges and achieve scientific breakthroughs that would otherwise be unattainable. The importance of international collaboration in space exploration cannot be overstated, as it promotes knowledge exchange, cost-sharing, and peaceful relations among nations.

REFLECTION ON THE IMPORTANCE OF ADDRESSING BIOLOGICAL THREATS IN SPACE

Space exploration has already provided us with incredible scientific discoveries and technological advancements. From the first human landing on the moon to the exploration of Mars, these achievements have expanded our knowledge of celestial bodies and their composition. The future promises even more remarkable breakthroughs, with plans for manned missions to Mars and the establishment of permanent human settlements on other planets or moons within our solar system. The importance of addressing biological threats in space through space biology, advanced technologies, and the protection of life cannot be overstated in this endeavor.

Space biology plays a crucial role in unraveling the mysteries of life beyond Earth. The research helps us comprehend the fundamental principles of life. It contributes to medical advancements on Earth, such as developing new disease treatments and improving our understanding of aging processes. The knowledge gained from space biology research can also have practical applications in fields such as medicine and agriculture, leading to advancements that benefit life on our planet. As humans venture further into space, studying the effects of microgravity and radiation on living organisms becomes crucial for long-duration space missions and the potential colonization of other celestial bodies. Moreover, exploring the possibility of extraterrestrial life and understanding how life can adapt and survive in extreme environments expands our knowledge of the origins and diversity of life in the universe.

The continuation of developing advanced technologies is essential for pushing the boundaries of space exploration. These technologies, from synthetic biology to autonomous systems with unprecedented capabilities, enable us to explore further and gather more data than ever. These technologies have the potential to revolutionize our understanding of the universe, enhance mission capabilities, increase efficiency, and mitigate risks. However, balancing human involvement and machine autonomy is essential to ensure the best outcomes for scientific discovery and advancing humanity's presence in space. Human astronauts bring unique qualities such as intuition, creativity, adaptability, and problem-solving skills that are difficult to replicate in machines. Therefore, a balanced approach that combines human and artificial intelligence strengths is crucial for future space missions' success. Advanced technology helps pave the way for future

missions to distant celestial bodies, potentially unlocking discoveries and expanding our understanding of the cosmos.

Protecting life, both on Earth and in space is a moral imperative. As we venture further into space, ensuring that our activities do not harm existing ecosystems or introduce harmful contaminants becomes increasingly essential, including implementing strict protocols to prevent the contamination of other celestial bodies with Earthly microorganisms, developing sustainable human colonization practices, and preserving cultural and scientific heritage. Furthermore, protecting life extends beyond our immediate concerns for astronauts and extraterrestrial organisms. It also encompasses our responsibility to safeguard Earth itself. Space exploration has revealed the fragility of our planet and highlighted the need for environmental preservation. By gaining a broader perspective from space, we realize the interconnectedness of all life on Earth and recognize the urgency to address biological processes, pathogens, and other threats to our planet's health. As we embark on these journeys, we must prioritize protecting life in all its forms. By approaching space exploration with a deep sense of responsibility and a commitment to protecting life, we can ensure that our endeavors in space contribute positively to advancing and preserving life on Earth.

RECOMMENDATIONS FOR FUTURE RESEARCH AND DEVELOPMENT

Space exploration poses unique challenges and risks, including the potential exposure to biological threats that could compromise the health and safety of astronauts. As humanity continues to venture into space, developing effective strategies to detect and mitigate such threats becomes crucial. This section provides recommendations for future research and development efforts that can be leveraged to enhance our ability to identify and counteract biological hazards during space exploration.

1. **Enhancing Bio-surveillance Systems:**

Bio-surveillance systems play a critical role in monitoring and detecting biological threats. Future research should focus on developing advanced biosensors capable of rapid and accurate identification of pathogens in real-time (Lederberg, et al., 2000). These biosensors could utilize innovative technologies such as nanotechnology or microfluidics to improve sensitivity, specificity, and portability. Additionally, integrating these biosensors with artificial intelligence algorithms can enhance their capability for early detection and prediction of potential outbreaks.

2. **Developing Space-Specific Pathogen Detection Methods:**

Traditional laboratory techniques for pathogen detection may not be suitable for space environments due to resource, time, and personnel limitations. Future research should explore the development of compact, automated, and self-contained pathogen detection systems specifically designed for use in space. These systems

should be capable of analyzing various sample types, including air, water, surfaces, and bodily fluids, with minimal human intervention.

3. **Establishing Onboard Diagnostic Capabilities:**

Space missions often involve long durations with limited access to medical facilities. Future research should focus on developing onboard diagnostic capabilities that enable astronauts to diagnose and treat potential infections independently. Research can include developing portable diagnostic devices capable of performing multiplexed testing for various pathogens and integrating A.I. technologies to facilitate remote medical consultations.

4**. Implementing Pre- and Post-Mission Monitoring:**

For the health and safety of astronauts, it is essential to implement comprehensive pre- and post-mission monitoring protocols. Future research should explore the development of non-invasive monitoring techniques that can assess an astronaut's immune system function, microbial composition, and overall health status. These techniques could include the analysis of biomarkers in bodily fluids, such as saliva or urine, to identify potential infections or alterations in the immune response.

5. **Conducting Long-Term Microbiome Studies:**

The human microbiome plays a crucial role in maintaining health and preventing infections. However, space exploration can disrupt the average microbial balance within the human body. Future research should conduct long-term microbiome studies on astronauts to understand how space travel affects their microbial composition and how these changes may contribute to increased susceptibility to infections. Such studies can provide insights into potential interventions or countermeasures to maintain a healthy microbiome during space missions.

REFERENCES

Ahmed, A. (2022, November 29). *BioSentinel NASA*. Retrieved from NASA: https://www.nasa.gov/centers/ames/engineering/projects/biosentinel.html

Ahsan, M. M., Luna, A. S., & Siddique, Z. (2022, March 10). *Healthcare.* Retrieved from MDPI Journals: https://doi.org/10.3390/healthcare10030541

Alberts, B., Johnson, A., & Lewis, J. (2022). *Introduction to Pathogens Molecular Biology of the Cell.* New York: Garland Science.

Aunins, T. R., Erickson, K. E., Prasad, N., levy, S. E., Jones, A., Shrestha, S., & Mastracchio, R. (2018).

Spaceflight Modifies Escherichia coli Gene Expression in Response to Antibiotic Exposure and Reveals Role of Oxidative Stress Response. Colorado: BioFrontiers Institute.

Ball, J. R., & Evans, C. H. (2001). *Safe Passage: Astronaut Care for Exploration Missions* . Washington, DC: National Academy Press.

Beischer, D. E., & Fregly, A. R. (1962). Pensacola: Naval School of Aviation Medicine.

Bell, T. E. (2004, May 11). *Preventing "Sick" Spaceships*. Retrieved from NASA Science Share The Science: https://science.nasa.gov/science-news/science-at-nasa/2007/11may_locad3

Belz, A. (2005, June 1). *Planetary Protection and Contamination Control Technologies for Future Space Science Missions.* Retrieved from NASA Solar System Exploration: https://solarsystem.nasa.gov/system/downloadable_items/161_PP-CC_final.doc(1).pdf

Bijlani, S., Stephens, E., Singh, N. K., Venkateswaran, K., & Wang, C. C. (2021, May 21). *Advances in Space Microbiology*. Retrieved from iScience: https://doi.org/10.1016/j.isci.2021.102395

Blachowicz, A., Raffa , N., Bok, J. W., Choera , T., Knox, B., Fong, Y. L., . . . Keller, P. (2020, February 8). *Contributions of Spore Secondary Metabolites to UV-C Protection and Virulence Vary in Different Aspergillus fumigatus Strains*. Retrieved from National Library of Medicine: https://pubmed.ncbi.nlm.nih.gov/32071276/

Bryan, W. (2020, April 24). *Working Toward an Autonomous Future Starts Now for NASA, Partners*. Retrieved from NASA: https://www.nasa.gov/offices/oct/working-toward-an-autonomous-future-starts-now-for-nasa-partners.html

Burgess, C., & Dubbs, C. (2007). *Animals in space: from research rockets to the space shuttle.* New York: Springer.

Camilla Urbaniak, M. D. (2022, June 29). *Microbial Tracking-2, a metagenomics analysis of bacteria and fungi onboard the International Space Station*. Retrieved from Microbiome Journal: https://microbiomejournal.biomedcentral.com/articles/10.1186/s40168-022-01293-0

Carter, K. (2001, December 1). *Moon Rocks and Moon Germs A History of NASA's Lunar Receiving Laboratory*. Retrieved from https://www.archives.gov/publications/prologue/2001/winter/nasa-lunar-lab

Catling, D. (2014). *Astrobiology: A Very Short Introduction.* Oxford: Oxford University Press.

Chandan K. Sen, S. S.-S. (2020, August 27). Electroceutical Management of Bacterial Biofilms and Surgical Infection. *Antioxidant and Redox Signaling*, pp. 713-724.

Chen, F., DiStefano, S., Colozza, A., Spry, J., & McKay, T. (2013). Planetary Protection Concerns During Pre-Launch Radioisotope Power System Final Integration Activities. *Nuclear and Emerging Technologies for Space 2013* (pp. 1-7). Albuquerque: NTRS NASA Technical Reports Server.

Dasch, E. J., & O'Mara, S. J. (2018). *A Dictionary of Space Exploration (3 ed.)* . Oxford: Oxford University Press.

Davidson, J. E. (1988). Lunar Placement of Mars Quarantine Facility. *Workshop on Mars Sample Return Science. A Lunar and Planetary Institute Workshop* (p. 62). Houston: Lunar and Planetary Institute.

Dunbar, B. (2017, August 3). *Curiosity Overview*. Retrieved from NASA MARS Curiosity : https://www.nasa.gov/mission_pages/msl/overview/index.html

Durante, M. &. (2008, May 2). *Heavy ion carcinogenesis and human space exploration*. Retrieved from Nature Reviews Cancer: https://www.nature.com/articles/nrc2391

European Space Agency. (2023, March 14). *ExoMars rover testing moves ahead and deep down*. Retrieved from ESA European Space Agency: https://www.esa.int/Science_Exploration/Human_and_Robotic_Exploration/ExoMars_rover_testing_moves_ahead_and_deep_down

Figliozzi, G. M. (2013, August 14). *Spaceflight Alters Bacterial Social Networks* . Retrieved from NASA Ames Research Center: https://www.nasa.gov/mission_pages/station/research/news/microorganisms.html

Gadd, G. M. (2006). *Fungi in Biogeochemical Cycles.* Cambridge: Cambridge University Press.

Giles, M. (2019, January 29). *Explainer: What is a quantum computer?* Retrieved from Technology Review: https://www.technologyreview.com/2019/01/29/66141/what-is-quantum-computing/

Gill, J. C. (2021, June 8). *Digital to biological converter*. Retrieved from Google Patents: https://patents.google.com/patent/US20170320061A1/en?oq=US20170320061A1

Howell, E. (2023, June 11). *International Space Station — Everything you need to know*. Retrieved from Space.Com: https://www.space.com/16748-international-space-station.html

Institute of Medicine (US) Committee on Creating a Vision for Space Medicine During Travel Beyond Earth Orbit. (2001). *Safe passage: astronaut care for exploration missions.* Washington DC: National Academies Press.

International Space Council. (2023, January 1). *Committee on Space Research (COSPAR)*. Retrieved from International Space Council: https://council.science/what-we-do/affiliated-bodies/committee-on-space-research-cospar/#:~:text=The%20Committee%20on%20Space%20Research,space%20vehicles%2C%20rockets%20and%20balloons

Johnson, M. (2018, June 14). *Investigation Tests BEST Method of DNA and RNA Sequencing*. Retrieved from NASA Space Station Research: https://www.nasa.gov/mission_pages/station/research/news/BEST_DNA_RNA

Joosse, T. (2023, January 12). *This Month in Physics History*. Retrieved from Advancing Physics News: https://www.aps.org/publications/apsnews/202302/history.cfm

Keith, S. (2021, August 1). *Planetary Protection*. Retrieved from NASA Office of Safety and Mission Assurance: https://sma.nasa.gov/sma-disciplines/planetary-protection

Kim, W., Tengra, F., Young, Z., Shong, J., Marchand, N., Chan, H. K., . . . Collins, C. (2013, April 29). *Spaceflight Promotes Biofilm Formation by Pseudomonas aeruginosa*. Retrieved from PLOS ONE: https://doi.org/10.1371/journal.pone.0062437

Kovo, Y. (2014, April 19). *Bion-M1*. Retrieved from NASA: https://www.nasa.gov/ames/research/space-biosciences/bion-m1

La Duc, M. T., Dekas, A., Osman, S., Moissl, C., Newcombe, D., & Venkateswaran, K. (2007, April

1). *Isolation and characterization of bacteria capable of tolerating the extreme conditions of clean room environments.* Retrieved from National Library of Medicine: https://pubmed.ncbi.nlm.nih.gov/17308177/

Landau, E. (2016, June 3). *Microbes in Space: JPL Researcher Explores Tiny Life*. Retrieved from NASA: https://www.nasa.gov/feature/jpl/microbes-in-space-jpl-researcher-explores-tiny-life

Lederberg, J., Alexander, M., Strick, J., Bloom, B., Hopwood, D., Hull, R., . . . Summers, W. (2000). *Encyclopedia of Microbiology, Four-Volume Set 2nd Edition.* Cambridge: Academic Press.

Lekbach, Y. L. (2011). *Advances in Microbial Physiology.* Amsterdam: Elsevier.

Luria, S. E., Darnell, J. E., Baltimore, D., & Campbell, A. (1978). *General Virology 3rd Edition.* New York: John Wiley & Sons Inc.

M A Juergensmeyer, E. A. (1999). Long-term exposure to spaceflight conditions affects bacterial response to antibiotics. *Microgravity Sci Technol* ., 12,47,7.

Mai, T. (1961, April 1). *First Human Entered Space*. Retrieved from NASA: https://www.nasa.gov/directorates/heo/scan/images/history/April1961.html

Mars, K. (2021, April 19). *50 Years Ago: Launch of Salyut, the World's First Space Station*. Retrieved from NASA: https://www.nasa.gov/feature/50-years-ago-launch-of-salyut-the-world-s-first-space-station

Mezhir, J. J., Advani, S. J., Smith, K. D., Darga, T. E., Poon, A. P., Schmidt, H., . . . Weichselbaum, R. R. (2005, October 15). *Ionizing Radiation Activates Late Herpes Simplex Virus 1 Promoters via the p38 Pathway in Tumors Treated with Oncolytic Viruses*. Retrieved from American Association for Cancer Research: https://aacrjournals.org/cancerres/article/65/20/9479/518682/Ionizing-Radiation-Activates-Late-Herpes-Simplex

Mihai G. Netea , J. D.-A. (2020, January 20). *Immune recognition of putative alien microbial structures: Host–pathogen interactions in the age of space travel*. Retrieved from PLOS Pathogens: https://journals.plos.org/plospathogens/article?id=10.1371/journal.ppat.1008153

Mikutta, R., Guggenberger, G., Haumaier, L., Schippers, A., & Baumgärtner, A. (2012, April 3). *Extracellular polymeric substances from Bacillus subtilis associated with minerals modify the extent and rate of heavy metal sorption*. Retrieved from National Library of Medicine: https://pubmed.ncbi.nlm.nih.gov/22443088/

Muriel Gargaud, R. A. (2011). *Encyclopedia of Astrobiology.* Berlin: Springer.

NASA. (2020, April 2017). *#PhageEvolution: Studying Viruses That Hunt Bacteria in Microgravity.* . Retrieved from National Aeronautics and Space Administration : https://www.issnationallab.org/phageevolution-rhodium-scientific-studying-viruses-microgravity/

NASA. (2023, January 1). *Bringing Mars Samples to Earth*. Retrieved from NASA MARS: https://mars.nasa.gov/msr/#Overview

NASA, K. (2021, November 2021). *KSC Personal Protective Equipment (PPE) Procedural Requirements.* . Retrieved from Kennedy NASA Procedural Requirements: https://procurement.ksc.nasa.gov › LASSOII › kscpage

National Research Council; Division on Engineering and Physical Sciences; Commission on Engineering

and Technical Systems; Committee on Advanced Technology for Human Support in Space. (1997). *Advanced Technology for Human Support in Space.* Washington, DC: National Academy Press.

Novikova, N. D. (2006, February 1). *Survey of environmental biocontamination on board the International Space Station*. Retrieved from National Library of Medicine: https://pubmed.ncbi.nlm.nih.gov/16364606/

Race, M. S., & Lupisella, M. (2020, July 16). *Low-Latency Teleoperations, Planetary Protection, and Astrobiology*. Retrieved from PubMed Central: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7365255/

Rooney, B. V. (2019, February 7). *Herpes Virus Reactivation in Astronauts During Spaceflight and Its Application on Earth*. Retrieved from Frontiers in Microbiology: https://www.frontiersin.org/articles/10.3389/fmicb.2019.00016/full

Rummel, J., Allton, J., & Morrison, D. (2011, January 1). *A MICROBE ON THE MOON? SURVEYOR III AND LESSONS LEARNED FOR FUTURE SAMPLE RETURN MISSIONS.* Retrieved from Lunar and Planetary Institute: https://www.lpi.usra.edu/meetings/sssr2011/pdf/5023.pdf

Sanders, L. M. (2023, March 23). *Biological research and self-driving labs in deep space supported by artificial intelligence. Nature Machine Intelligence*. Retrieved from Nature Machine Intelligence: https://doi.org/10.1038/s42256-023-00618-4

Sarah Stahl-Rommel, D. L.-W. (2021, June 30). *A CRISPR-based assay for the study of eukaryotic DNA repair onboard the International Space Station*. Retrieved from PLOS: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0253403

Savage, D. L., Hartsfield, J., & Salisbury, D. (1996, August 7). *Meteorite Yields Evidence of Primitive Life on Early Mars* . Retrieved from NASA: https://www2.jpl.nasa.gov/snc/nasa1.html

Scalice, D. (2022, January 18). *An Update from ALH84001*. Retrieved from Astrobiology at NASA Life in Universe: https://astrobiology.nasa.gov/news/an-update-from-alh84001/

Scoles, D. (2023, June 9). *Cosmic Luck: NASA's Apollo 11 Moon Quarantine Broke Down*. Retrieved from New York Times: https://www.nytimes.com/2023/06/09/science/nasa-moon-quarantine.html

Sincavage, S., & McCreight, R. (2019). *Trajectory Significance of Convergent Technology Geospatial Intelligence.* Herndon: United States Geospatial Intelligence Foundation. Retrieved from https://www.academia.edu/42702961/
Trajectory_Significance_of_Convergent_Technology_Geospatial_Intelligence

Stromberg, J. (2014, May 20). *NASA's Curiosity rover may have carried bacteria to Mars*. Retrieved from VOX: https://www.vox.com/2014/5/20/5734360/nasas-curiosity-rover-may-have-carried-bacteria-to-mars

Stutte, G. W., Flynn, M. T., & Acevedo, M. F. (2008). *Space Microbiology.* Boca Raton: CRC Press.

Tabor, A. (2021, December 7). *The Astronaut's Guide to Microbe Hitchhikers*. Retrieved from NASA AMES: https://www.nasa.gov/ames/microbial-tracking

The Guardian. (2010, November 10). *Gimme some space: inside the International Space Station – in pictures*. Retrieved from The Guardian: https://www.theguardian.com/artanddesign/gallery/2020/nov/10/gimme-some-space-inside-the-international-space-station-in-pictures

Tom, E., Molineux, I. J., Paff, M., & Bull, J. (2018, July 9). *Experimental evolution of UV resistance in a phage*. Retrieved from Peer Life and Environment: https://doi.org/10.7717/peerj.5190

United Nations Office for Outer Space Affairs. (2023, January 1). *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*. Retrieved from United Nations Office for Outer Space Affairs: https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html

Urbaniak, C. M. (2022, June 29). *Microbial Tracking-2, a metagenomics analysis of bacteria and fungi onboard the International Space Station*. Retrieved from microbiomejournal-biomedcentral: https://microbiomejournal.biomedcentral.com/articles/10.1186/s40168-022-01293-0

Uri, J. (2021, October 13). *Building on a Mission: The Lunar Receiving Laboratory*. Retrieved from Roundup RU in the Loop?: https://roundupreads.jsc.nasa.gov/roundup/1779/Building%20on%20a%20Mission%20The%20Lunar%20Receiving%20

V.B. Vasin, V. T. (1995). The experimental study of microbial contamination of the space hardware. *Advances in Space Research*, 3-453.

Versalovic, J. (2011, May 16). *Introduction to the 10th Edition of the Manual of Clinical Microbiology*. Hoboken: Wiley. Retrieved from Microbe Canvas: https://microbe-canvas.com/Bacteria/gram-negative-rods/obligate-aerobic-3/oxidase-positive-2/colistin-susceptible-4/methylobacterium-species.html

Warnes, S. L., & Keevil, C. W. (2013, September 9). *Inactivation of Norovirus on Dry Copper Alloy Surfaces*. Retrieved from PLOS ONE: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0075017

William, B. (2022, October 17). *Working Toward an Autonomous Future Starts Now for NASA, Partners*. Retrieved from NASA Science and Technology Partnership Forum: https://www.nasa.gov/offices/oct/working-toward-an-autonomous-future-starts-now-for-nasa-partners.html

Wilson, J. W.-G. (2007, October 9). *Space flight alters bacterial gene expression and virulence and reveals a role for global regulator Hfq*. Retrieved from PNAS: https://www.pnas.org/doi/full/10.1073/pnas.0707155104

10.

SPACE ELECTRONIC WARFARE [NICHOLS]

PURVIEW

Space is the entire physical universe. Outer Space is all of the Space outside the Earth. Deep Space is the vast distance of Space far away from a reference point or observer. (What is Deep Space, 2023) For our purposes, let us redefine Space as the new frontier of *Electronic Warfare (EW), Intelligence, and Reconnaissance (EWIR)*. For purposes of this chapter and Chapter 10, we have three general altitude reference points: 1) Earth's surface (ground zero); 2) The maximum distance to Geosynchronous and Geostationary Satellites from the Earth's surface(22,236 mi); and 3) Deep Space beyond the maximum altitude for Satellites (>22,236 mi). (High Earth Orbit, 2023)

Of the three EWIR, our concern is with EW. However, EW alone is a huge discipline and encompasses many different sciences. Chapter 3 Book 7 (Nichols & al, Space Systems: Emerging Technologies and Operations, 2022) focused on space electronic warfare, signal jamming, and spoofing. Jamming was presented only as a precursor attack to a spoofing attack. In addition to the basics presented in Chapter 3, Book 7 (Nichols R. &., 2022), there are plenty of learning seminars available by SMEs like Rhode & Schwartz and fundamental textbooks to inform the reader. (Wolff, 2022) (Adamy D. , 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., EW 102 A Second Course in Electronic Warfare, 2004)[1] [2] On Linkedin, visit Paul Szymanski, an SME author who teaches expert courses for Space Warfighters. Rhode and Schwartz in Munich, Germany, provides advanced courses in Radar, EW, and various synchronous topics. Similarly, there is a plethora of Open-Source information on Intelligence and Reconnaissance functions. They are the menu and dessert of the intelligence community (IC) -especially related to UAS/CUAS/UUV systems. (Nichols & Sincavage, 2022)

OBJECTIVES

Chapter 10 is about EW, signals, and vulnerable communication links. Chapter 10 is a condensed treatment of the subjects addressed in fair detail in our published UAS/CUAS/UUV/Space series Book 7, Chapter 3: *Space Systems: Emerging Technologies and Operations.* (Nichols & al, Space Systems: Emerging Technologies and Operations, 2022) *Chapter 3 was entitled: Space Electronic Warfare, Jamming, Spoofing, and ECD* (Nichols R. &., 2022). Chapter 3 covered in detail the principles of space electronic warfare:

- 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
- Promising ECD technology countermeasures to spoofing can detect, mitigate, and recover fake and genuine signals. (Eichelberger, 2019)

EW definitions from Book 7, Chapter 3 are incorporated in this book's Abbreviations and Acronyms section. dB math and spherical trigonometry concepts, the bread and butter of EW, are presented as a primer in Appendix A. (Adamy D. L., Space Electronic Warfare, 2021) presents detailed mathematical concepts fundamental to space electronic warfare calculations.

Chapter 10 focuses on three types of EW signal activities: Interception, Jamming, and Spoofing. It looks at vulnerable satellite links and threats to those links. It presents a controllable region and prepares for discussing the uncontrollable deep space region covered in chapter 12.

ORBITAL MECHANICS – THE LANGUAGE OF THE SKIES

To understand satellite functions, velocity, and locations in real-time, we use an interesting geometric mathematics known as Orbital Mechanics.

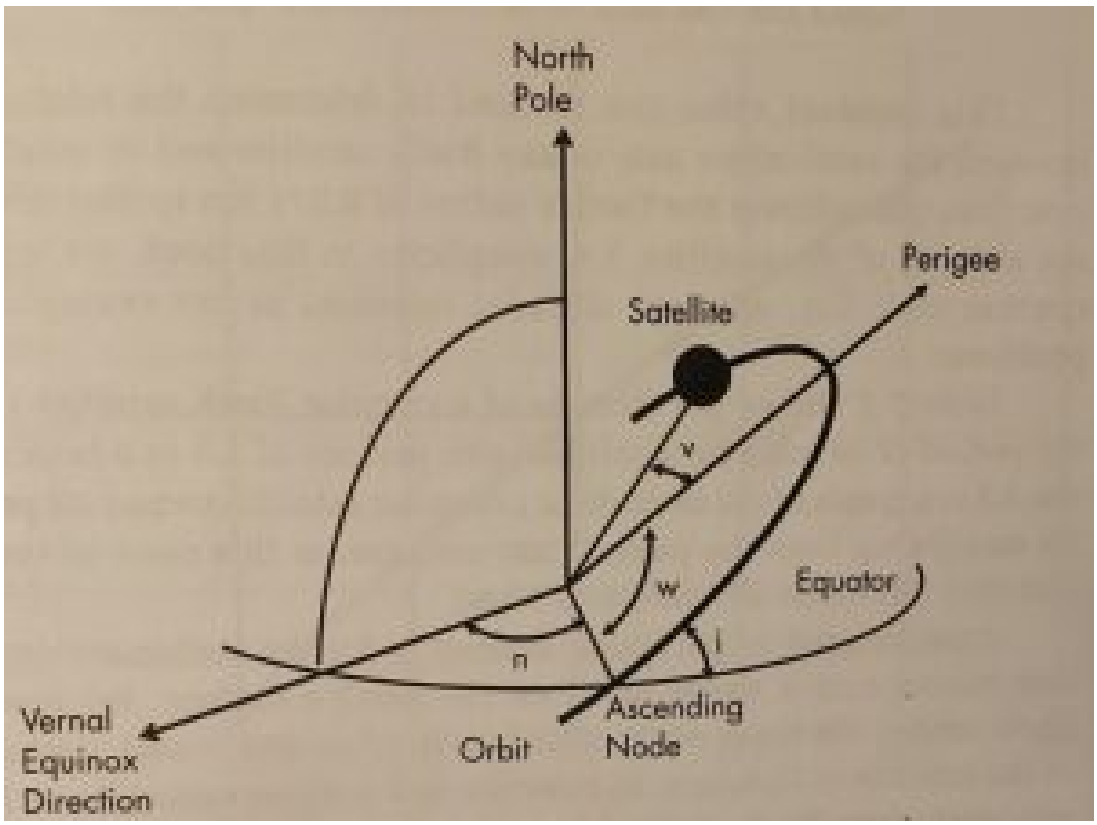
Spherical and Elliptical geometry are used to explain Orbital Mechanics. The difficulty trying to understand Spherical Triangles versus Plane Triangles is because Spherical Triangles are 2-dimensional, mapped onto a sphere rather than a plane. An example would be looking at a map and drawing a line from one point to the other, but in reality, the Space between is actually curved. Spherical Trigonometry takes the curvature of the Earth into account. This mapping is defined/known as the *Keplerian Ephemeris*. The Ephemeris elements of Spherical Triangles can be seen in Table 10-1 and Figure 10-1.

Table 10-1 Earth Satellite Ephemeris

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

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

Figure 10-1 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 that the relationship between the size of the orbit and its period is defined by:

$$\mathbf{a^3 = CP^2; \text{ therefore, } C = a^3 / P^2.} \qquad \textbf{Eq. 10-1}$$

Where:

a = the semi-major axis of the orbit ellipse,

C = 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

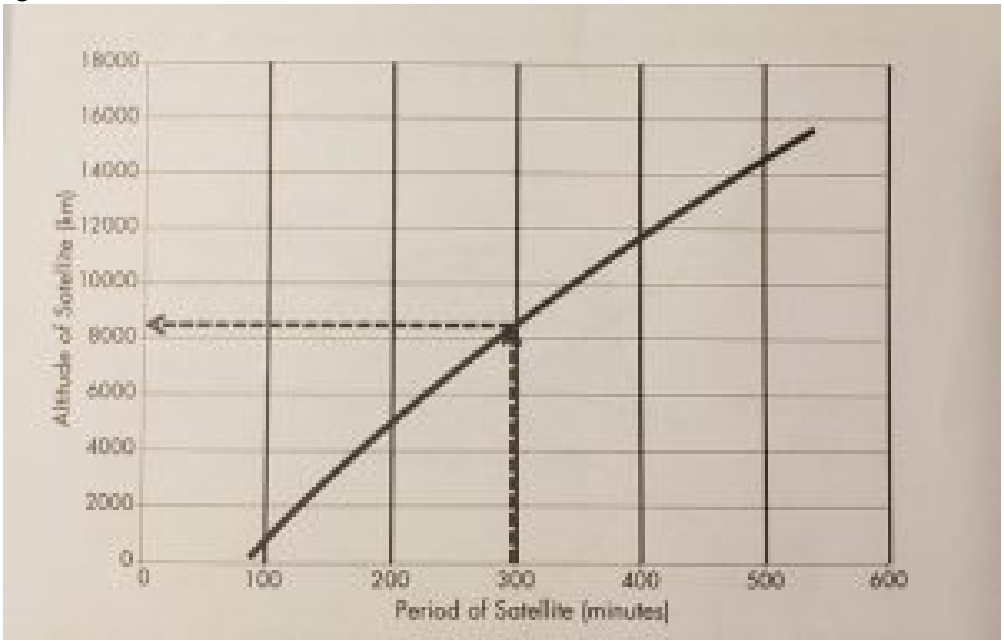
Table 10-2 Shows the altitude of a circular Earth satellite versus the period of its orbit for satellites with periods of 1.5 hours to 9 hours.

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 10-2 Altitude of a Circular Satellite is a Function of its Orbital Period



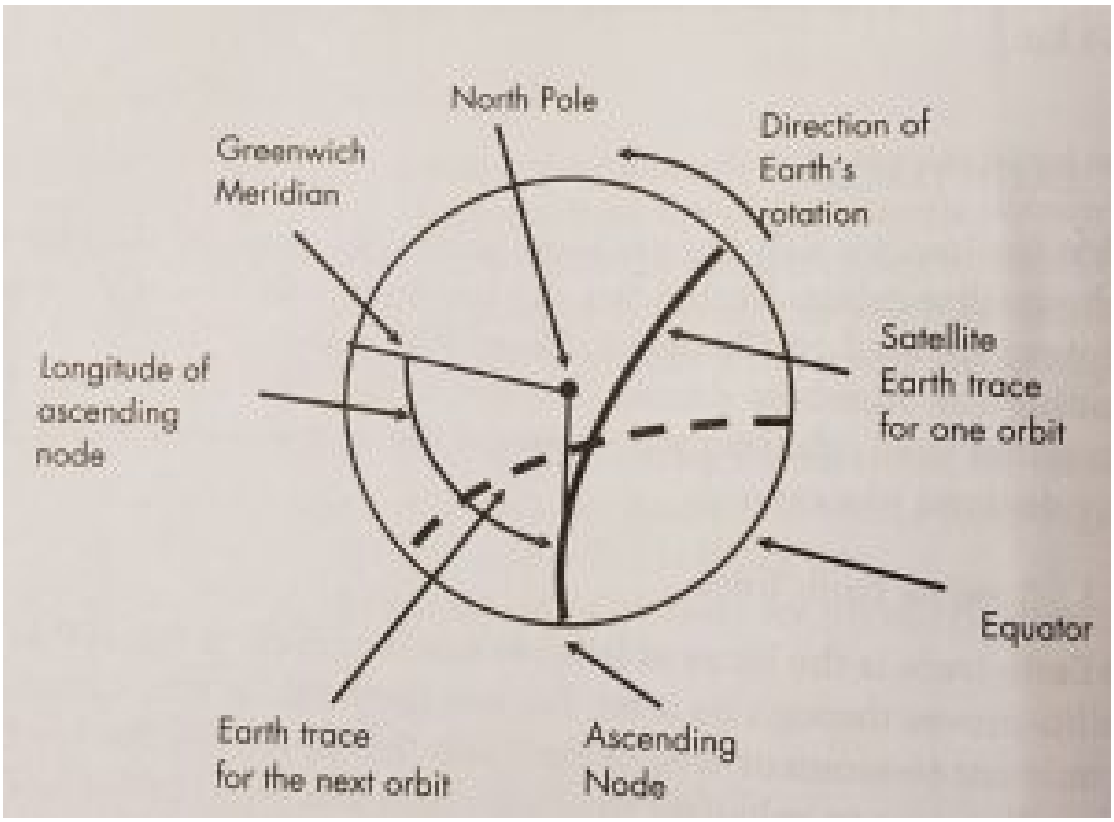
Source courtesy of (Adamy D. L., Space Electronic Warfare, 2021)

LOOK ANGLES

An 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. See Figure 10-3.

Using the six elements of Ephemeris, 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. Earth Traces are very important in using emerging space technologies for humanitarian purposes. They give policymakers new approaches to feeding populations, increasing crop efficiencies, routing navigation, improving cattle feeding, and building more effective fire barriers. (Nichols & al, Space Systems: Emerging Technologies and Operations, 2022)

Figure 10-3 Earth Trace of the satellite is the path of the SVP over the Earth's surface in a Polar view.

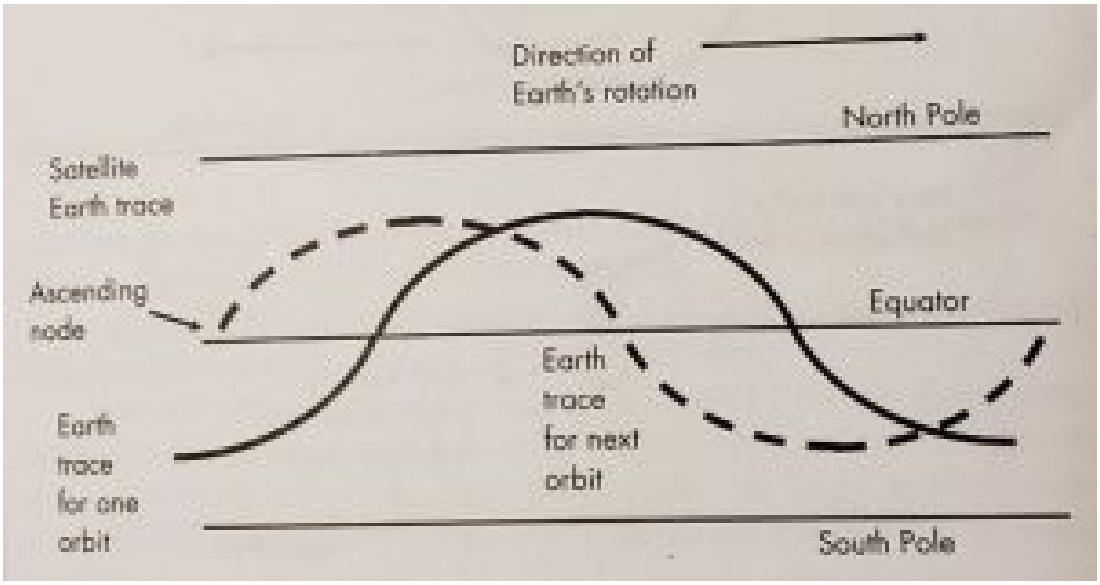


Source: Courtesy of (Adamy D. L., Space Electronic Warfare, 2021)

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 satellite's altitude 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 10-4 Earth Trace of a satellite is the path of the SVP over the Earth's surface in an equatorial view.

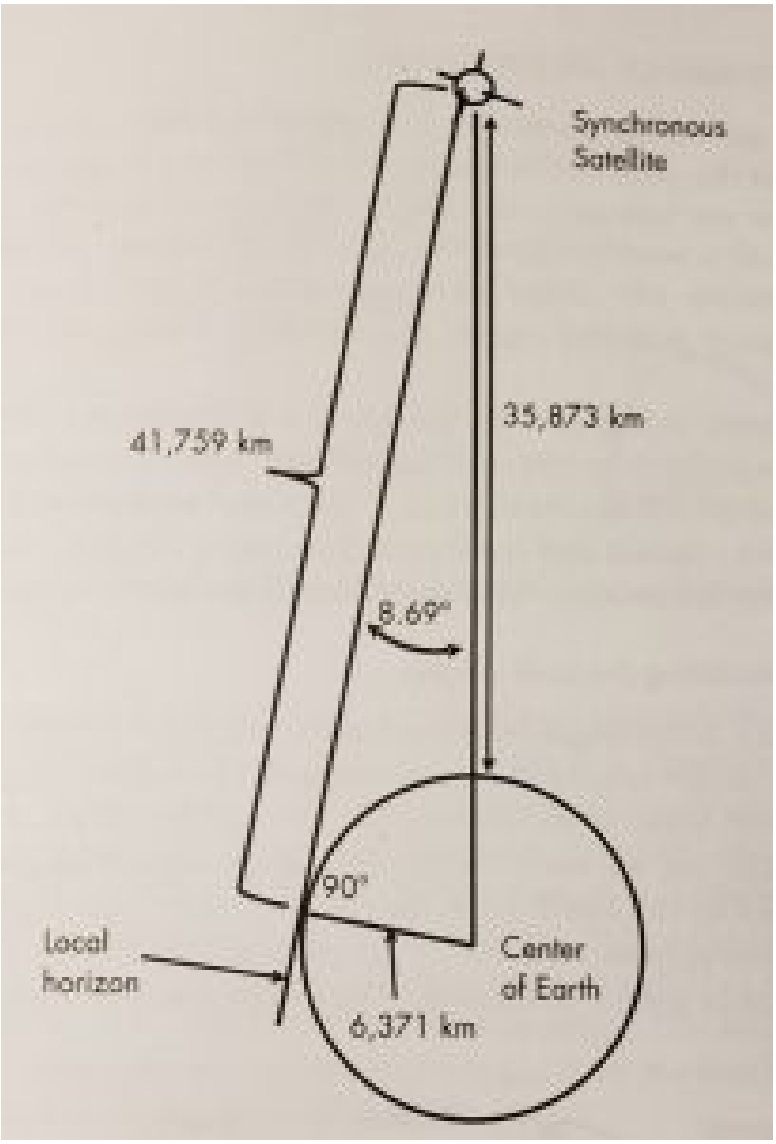


Source: Courtesy of (Adamy D. L., Space Electronic Warfare, 2021)

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 10-5 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's surface station (ESS) to the synchronous satellite with a circular orbit. The diagram is a planer triangle in the plane containing the Earth's ESS, satellite, and center. 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)

Figure 10-5 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

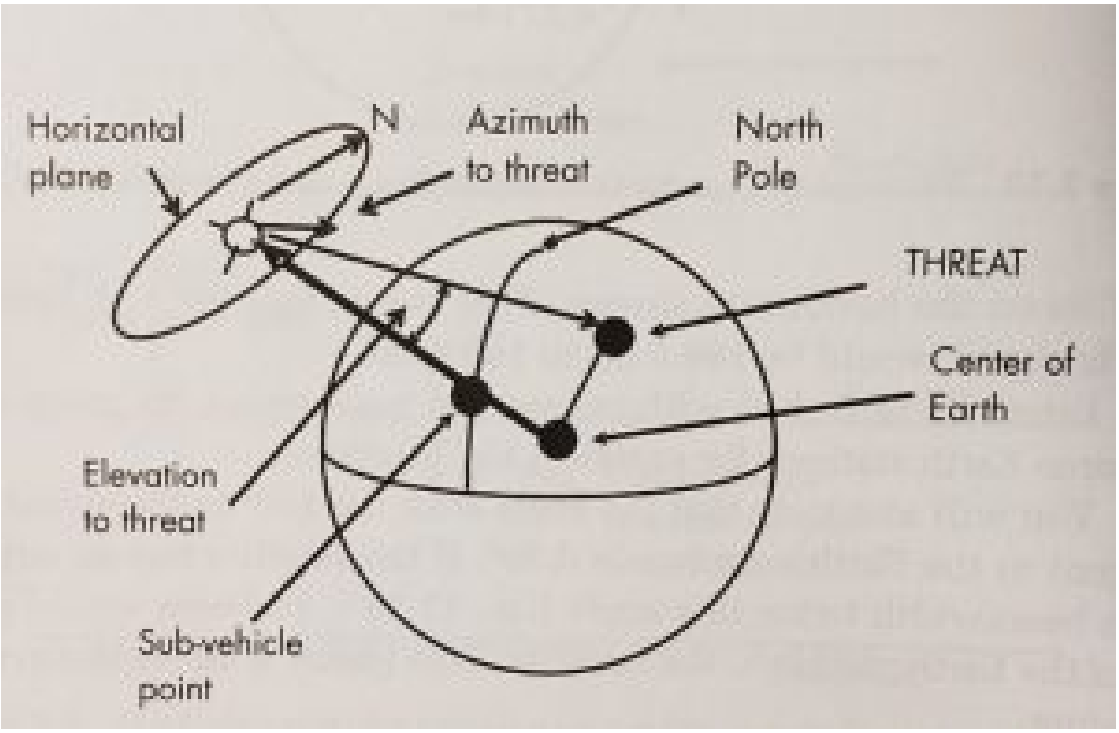


Source: Courtesy of **(Adamy D. L., Space Electronic Warfare, 2021)**

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 or spoofing signals to a threat receiver at the considered location. (Adamy D. L., Space Electronic Warfare, 2021) (Nichols R. &., 2022) See Figure 10-6.

Figure 10-6 The azimuth and elevation angle from the nadir defines the direction of a threat to a satellite.



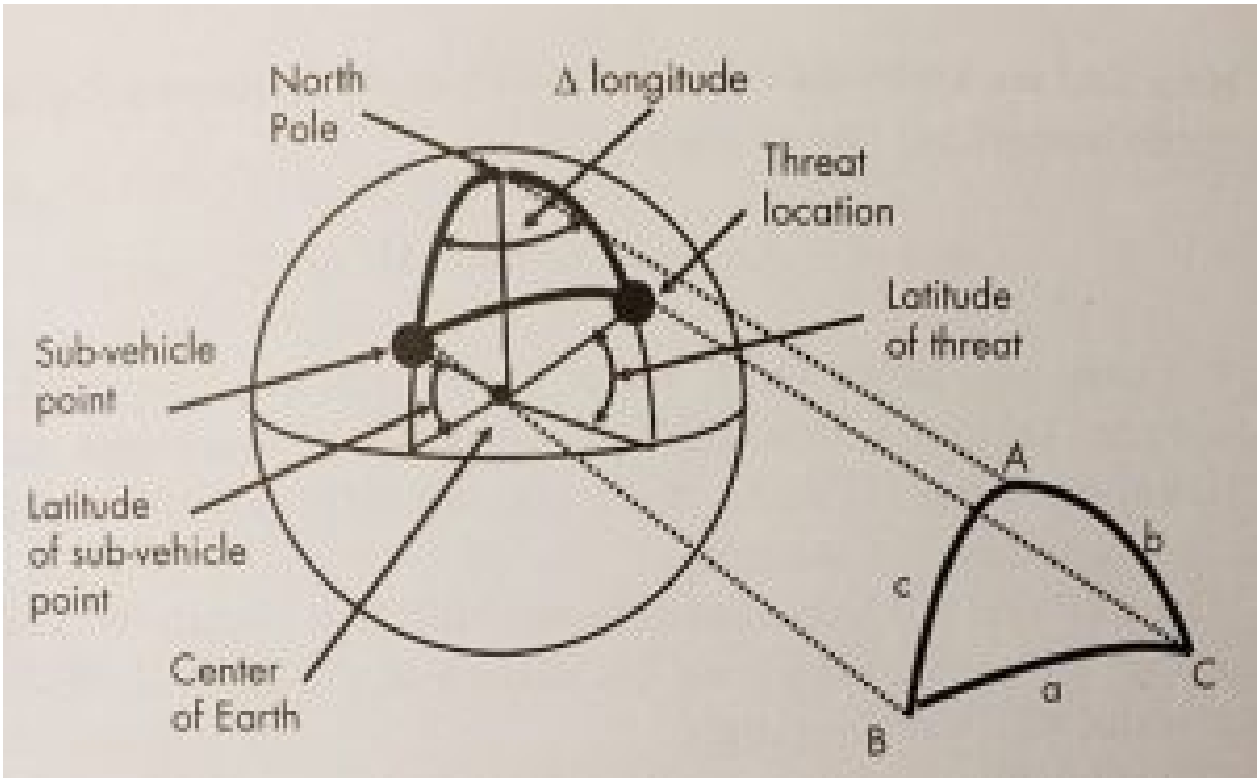
Source: Courtesy of (Adamy D. L., Space Electronic Warfare, 2021)

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 LOOK ANGLES

For the azimuth calculation, we need to consider the spherical triangle. Consider Figures 10-7 and 10-8.

Figure 10-7 A spherical triangle is formed between the North Pole, the SVP, and the Threat location.

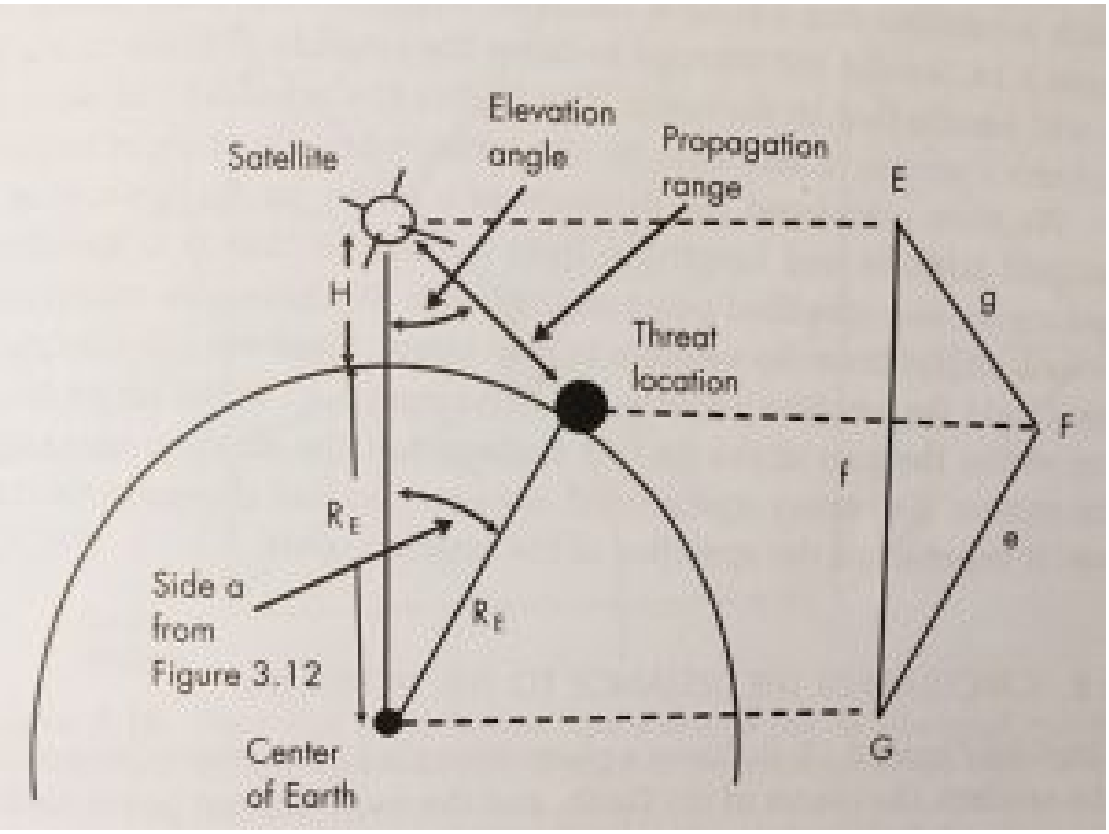


Source: Courtesy of (Adamy D. L., Space Electronic Warfare, 2021)

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. We use the law of cosines for plane triangles to calculate the relationships – specifically the propagation distance between the satellite and the threat; to wit:

$$g^2 = e^2 + f^2 - 2ef\cos(G) \qquad \textbf{Eq. 10-2}$$

Figure 10-8 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)**

PROPAGATION LOSS MODELS

Messages travel (propagate) through Space as radio waves (electromagnetic waves). This is similar to the radio waves we receive with our car radio. Each spacecraft has a transmitter and receiver for radio waves and a way of interpreting the information received and acting on it. Electromagnetic waves are unlike sound waves because they do not need molecules to travel. This means electromagnetic waves can travel through air, solid objects, and Space. This is how astronauts on spacewalks use radios to communicate.

Space wave propagation refers to the satellite signals of radio transmitted freely through the Earth's atmosphere. Space wave propagation refers to the radio waves transmitted from the antenna to propagate (travel) along Space to reach the receiver antenna.

It is not a clean transmission because of the long distances to satellites. There are losses in the link between the antenna and the receiver. (R.K. Nichols & Lekkas, 2002)

(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 10-3. 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 10-3 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)

RECEIVED POWER AT THE RECEIVER

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 10-3 formula gives the *received power to the receiver*:

$$\mathbf{P_R = ERP - L + G_R} \qquad \textbf{Eq. 10-3}$$

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) [3]

ONE-WAY LINK EQUATION

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

$$\mathbf{P_R = P_T + G_T - L + G_R} \qquad \textbf{Eq. 10-4}$$

Where:

PR – 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 (non-decibel units), this formula is:

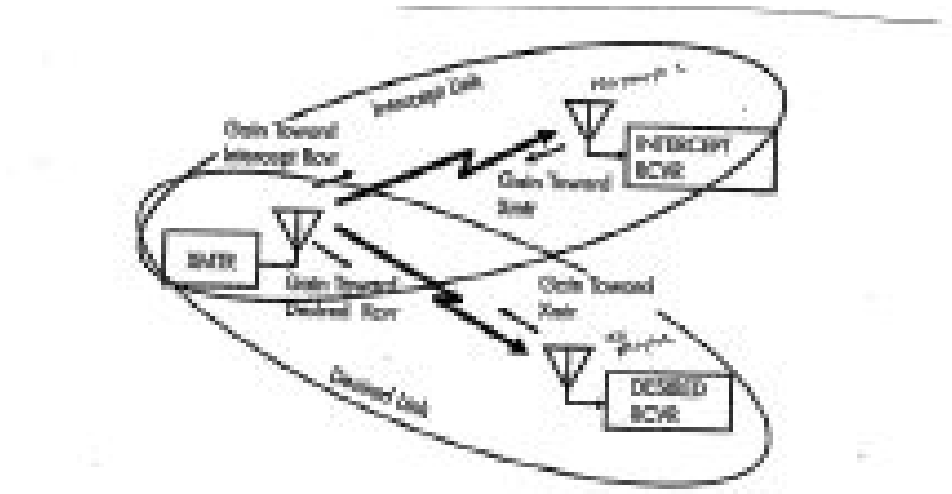
$$P_R = (P_T G_T G_R) / L \qquad \text{Eq. 10-5}$$

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)

INTERCEPTED COMMUNICATION SIGNAL

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 10-9.

Figure 10-9 Intercepted Communication Signal

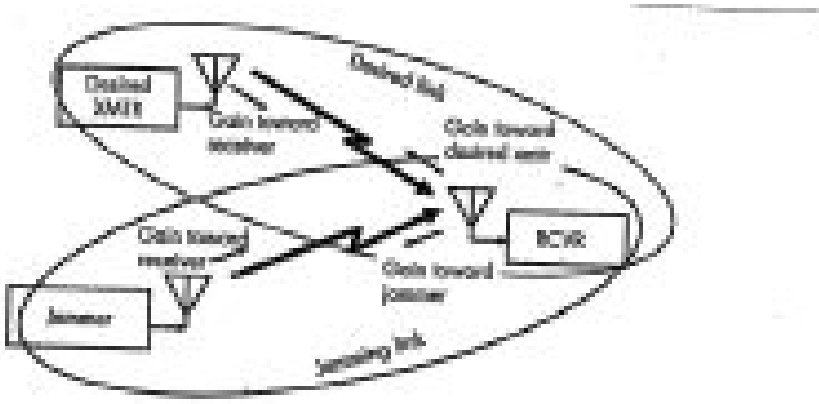


Source: Reprinted /modified from Figure 4-3 courtesy of (Adamy D. L., Space Electronic Warfare, 2021)

JAMMED / SPOOFED COMMUNICATIONS SIGNAL

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) [4] Refer to Figure 10-10.

Figure 10-10 Jammed / Spoofed Communications Signal



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

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.

Uplinks have transmitters on or near Earth's surface and receivers in the satellite. The uplink equation is 10-4. **L** is the in that equation is Link Losses. Table 10-4 shows the various Uplink Losses.

Table 10-4 Uplink Losses

Loss	Description
Transmit antenna misalignment	Reduction from boresight gain at the offset angle from the direction to the satellite
Receiving antenna misalignment	Reduction from boresight gain at the offset angle from the direction to the ground-based transmitter
Space loss	LOS loss assuming that both the transmit and receive antennas are isotropic
Atmospheric loss	Atmospheric attenuation at the elevation angle through the atmosphere from the ground transmitter
Rain loss	Rain attenuation over the part of the link that passes through the rain

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

Command links control functions of the satellite, such as its orientation, payloads, and synchronization of multiple payloads. (Adamy D. L., Space Electronic Warfare, 2021)

Intercept links (satellite-borne system) are defined from the hostile transmitter to the satellite payload receiver

The power received by the satellite payload receiver in the presence of a hostile transmitter is given by equation 10-6:

$$\mathbf{P_R = P_T + G_T - Link\ Losses + G_R} \qquad \textbf{Eq. 10-6}$$

Where:

P_R – Power received by satellite payload receiver

P_T – Hostile transmitter output power

G_T – Boresight gain of the hostile transmitter

Link Losses – Table 10-4

G_R – Boresight gain of satellite payload receiving antenna

Downlinks from the satellite to the ground can be the satellite's control station, to other receivers at stations that require information that the satellite has gathered, or to hostile receivers that intercept the satellite downlink. They can also be to hostile receivers that are jammed or spoofed from the satellite. (Adamy D. L., EW 103: Tactical Battlefield Communications Electronic Warfare, 2009) (Nichols R. &., 2022)

The downlink equation is given by 10-7.

$$\mathbf{P_R = P_T + G_T - Link\ Losses + G_R} \qquad \textbf{Eq. 10-7}$$

Where:

PR – Power received by the ground-based receiver or hostile receiver

P_T – Output power of the satellite's transmitter

G_T – Boresight gain of satellite's antenna

Link Losses – Table 10-4

G_R – Boresight gain of ground-based receiving antenna

Table 10-5 Downlink Losses

Loss	Description
Transmit antenna misalignment	Reduction from boresight gain at the offset angle from the direction to the ground-based receiver
Receiving antenna misalignment	Reduction from boresight gain at the offset angle from the direction to the satellite
Space loss	LOS loss assuming that both the transmit and receive antennas are isotropic
Atmospheric loss	Atmospheric attenuation at the elevation angle through the atmosphere from the ground-based receiver
Rain loss	Rain attenuation over the part of the link that passes through the rain

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

User data links – a satellite may collect usage data for many users. User data links receive satellite data directly. Users may not be authorized to receive all the data available /collected from /by the satellite. The ground station may edit the data and retransmitted back to the satellite and back again to users. (Adamy D. L., Space Electronic Warfare, 2021)

Jamming Links – ground communication links and satellite radar links can be jammed. The target receiver can either be on the Earth's surface or in an aircraft or UAS flying above the Earth. Like intercept links, the received power into the target receiver is calculated by the same formula. Still, the transmitted power is from the satellite jammer, and the received power is at the target receiver.

The Jammed link equation is given by 10-8.

$$\mathbf{P_R = P_T + G_T - Link\ Losses + G_R} \qquad \textbf{Eq. 10-8}$$

Where:

P_R – Power received by the target receiver

P_T – Satellite jammer output power

G_T – Boresight gain of jammer transmitter

Link Losses – Table 10-5

G_R – Boresight gain of target receiver antenna

LINK VULNERABILITY TO EW: SPACE-RELATED LOSSES, INTERCEPT JAMMING & SPOOFING

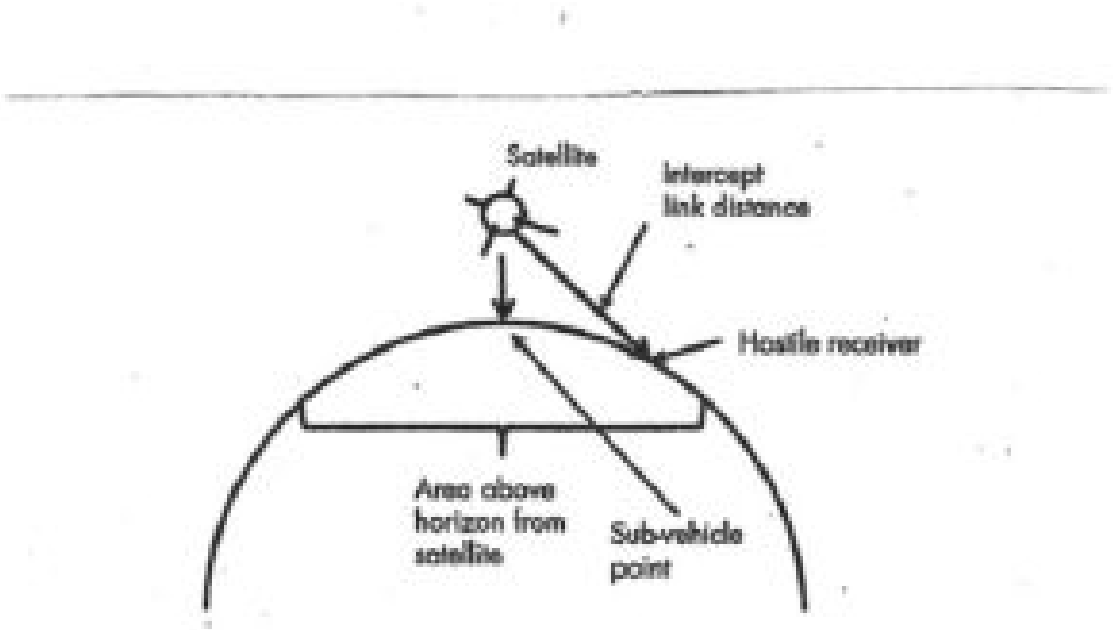
Satellites are from Earth but present excellent loss of signal **(LOS)** from a large part of the Earth's surface. As reported previously, satellite links are highly susceptible to three kinds of hostile activity. Signals from satellites can be intercepted, and strong hostile transmissions can be jamming signals, interfering with uplink or downlink signals to prevent proper reception. (Adamy D. L., Space Electronic Warfare, 2021) They can also be spoofing signals that cause the satellite to interpret them as functional commands that are harmful or transmit useless positional data. This section and the following will focus heavily on spoofing and the downlink interpretation of false signals in GNSS/GPS/ADS-B receivers. (Nichols R. &., 2022)

Figure 10-11 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 another 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) (Nichols R. &., 2022)

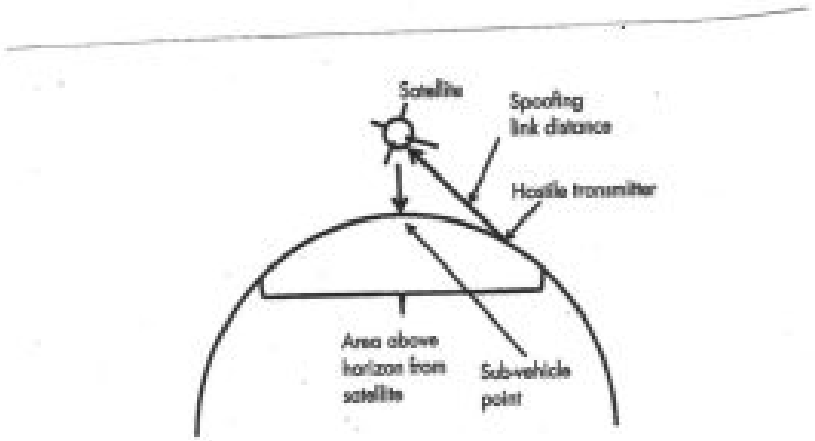
Figure 10-12 shows a successful spoofing of a satellite signal. A ground-based spoofer operating against a satellite uplink transmits to the link receiver in the satellite. The ground station and the jammer must be above the horizon from the satellite.[5]

Figure 10-11 Successful Intercept



Source: Figure 10-32 Modified from Figure 7.1 Courtesy of (Adamy D. L., Space Electronic Warfare, 2021)

Figure 10-12 Successful Spoofing



Source: Figure 10-12 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 data – especially localization data. (Nichols R. &., 2022) (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:

$$\mathbf{J / S = ERP_J - ERP_S - LOSS_J + LOSS_S + G_{RJ} - G_R} \qquad \textbf{Eq. 10-9}$$

Where:

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

$\mathbf{ERP_J}$ = Effective radiated power (ERP) of jamming transmitter toward the target receiver in dBm

$\mathbf{ERP_S}$ = ERP of the desired signal toward the receiver in dBm

$\mathbf{LOSS_J}$ = Transmission loss from the jammer to target a receiver in dBm

$\mathbf{LOSS_S}$ = Transmission loss from transmitter to target a receiver in decibels

$\mathbf{G_{RJ}}$ = Gain of receiving antenna in the direction of a jammer in decibels

$\mathbf{G_R}$ = 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. [6] [7]

GPS/GNSS SPOOFING -PRACTICAL SPOOFING

GPS spoofing detection and mitigation for GNSS / GPS using the ECD algorithm will be addressed. GPS spoofing of ADS-B systems was covered in detail (Nichols R. &., 2022).[8] **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 computationally burdensome. Civilian COTS anti-spoofing

countermeasures are rare**. Nevertheless, 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, 2019) ECD implementation and evaluation *show that with some modifications, the robustness of collective detection (CD) can be exploited to mitigate spoofing attacks.* (Eichelberger, 2019) *shows that multiple locations, including the actual one, can be recovered from scenarios where several signals are present.* [9] [10]

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)

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. (Humphreys & al., 2008)

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, 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, 2019)

Before discussing E*CD – Collective detection maximum likelihood localization approach* (Eichelberger, 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. [11]

GPS SIGNAL

The GPS consists of control, space, and user segments. The space segment contains 24 orbiting satellites. The network monitor stations, GCS, and antennas comprise the control segment. The third and most important are the receivers, 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.[12] (Eichelberger, 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 the satellite and receiver introduces a significant Doppler shift to the carrier frequency. [13] 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, 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, 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. [14] 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, 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. [15]

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. [16] This technique is critical to the (Eichelberger, 2019) invention to mitigate spoofing attacks on GPS /GNSS or ADS-B. CD can tolerate a few low-quality satellite signals and is more robust than CTN. CD requires much 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, 2019) (J.Liu & et.al., 2012) (Axelrod & al, 2011) (P. Bissag, 2017)

ECD

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, 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.[17] (Wesson, 2014) For each location fix, the ECD approach uses only a few milliseconds of raw GPS signals, so-called *snapshots*. This enables offloading of the computation into the Cloud, which allows knowledge of observed attacks. [18] Existing spoofing mitigation methods require a constant stream of GPS signals and tracking those signals over time. Computational load increases because fake signals must be detected, removed, or bypassed. (Eichelberger, 2019)

SPOOFING TECHNIQUES

According to (Haider & Khalid, 2016), there are three common GPS Spoofing techniques with different sophistication levels. They are **simplistic, intermediate, and sophisticated**. (Humphreys & al., 2008)

The *simplistic spoofing attack* is the most commonly used technique to spoof GPS receivers. It only requires a COTS GPS signal simulator, amplifier, and antenna to broadcast signals to the GPS receiver. It was performed successfully by Los 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 receive a genuine GPS signal and a spoofing device to transmit a fake GPS signal. The idea is to estimate the target receiver antenna position and velocity and then broadcast a fake signal relative to the genuine GPS signal. This 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) [19]

Note that prior research on spoofing was to exclude fake signals and focus on a single satellite. ECD *includes* the fake signal on a minimum of four satellites and then progressively / selectively eliminates their effect until the real *weaker* GPS signals become apparent. (Eichelberger, 2019)

GPS SIGNAL JAMMING AS A PRECURSOR TO SPOOFING ATTACK

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 tolerate more noise or stronger jamming. (Eichelberger, 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. [20] (Eichelberger, 2019)

There is a more powerful and subtle attack on the jammed signal. To spoof the receiver successfully, the spoofer can send satellite signals with adjusted power levels synchronized to the authentic signals. (Eichelberger, 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, 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, 2019)

Regarding the fourth point, spoofing and multipath signals are similar from a receiver's perspective. Both result in several observed signals from the same satellite. The difference is that multipath signals have a delay dependent on the environment while spoofing signals can be crafted to yield 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, 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) (Eichelberger, 2019) describes improved Branch and Bound implementations to reduce the calculation load and find plausible receiver locations.[21]

SIGNALS INTELLIGENCE (SIGINT), EW, AND EP

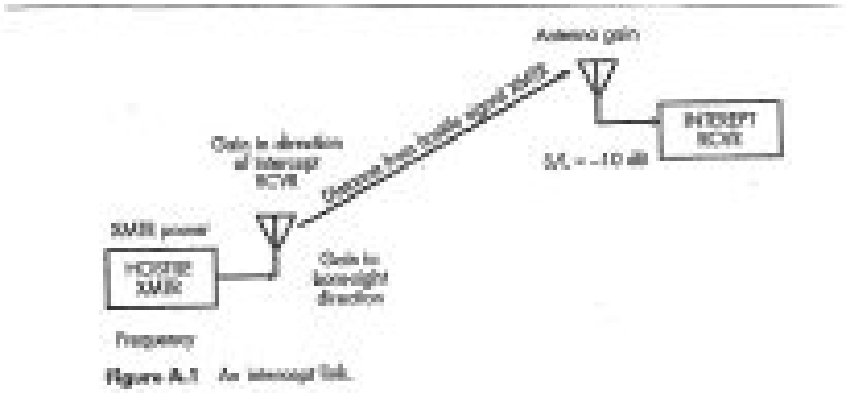
Satellites are perfect for implementing SIGINT and EW, depending on the specific situation and activity. [22]

This final section will cover the key formulas for successful intercept, the intercept link equation, communications jamming (by extension spoofing), and communications EP (electronic protection). Radar Jamming will not be covered but can be found in (Adamy D. L., EW 103: Tactical Battlefield Communications Electronic Warfare, 2009) and (Adamy D. L., EW 104: EW against a new generation of threats, 2015)

SUCCESSFUL INTERCEPT

Figure 10-13 shows an intercept link.

Figure 10-13 Intercept Link



Source: Courtesy of and modified from Figure A-1, p200 in (Adamy D. L., Space Electronic Warfare, 2021)

The *parameters of this link are the hostile transmitter power, the transmit antenna gain in the direction of the intercept receiver, the distance to the intercept receiver (the satellite), and the antenna configuration at the intercept site*. (Adamy D. L., Space Electronic Warfare, 2021)

A successful intercept occurs when a receiver in the satellite receives a hostile signal with enough quality to recover the information carried by the signal. For communication signals, transmission frequency, modulation, the type of encryption employed, the signal's timing, or the signal's location can constitute hostile level quality.[23] Modulation, voice imagery, and data can also constitute hostile quality. [24] (Adamy D. L., Space Electronic Warfare, 2021)

THE INTERCEPT LINK EQUATION

In order to intercept a signal, the received signal strength must exceed the sensitivity level of the receiver. The Sensitivity (**S**) is the weakest signal the receiver can receive and still extract the required information from that signal. We need to budget for the power out of the receiving antenna. The intercept link equation is (Adamy D. L., Space Electronic Warfare, 2021):

$$P_R = ERP - Loss + G_R \qquad \text{Eq. 10-10}$$

Where:

PR – **P**ower out of the receiving antenna, dBm,

ERP – Effective radiated power of the Hostile signal to be intercepted,

Loss – Loss is the sum of all the losses between the Hostile transmitter's antenna and the intercept receiver's antenna (in decibels), **(L)**

$\mathbf{G_R}$ – is the receiving antenna gain.

S/L – Signal to Noise Level measure in some minimum, -dB

Received signal quality is normally stated in a signal-to-noise ratio or minimum level of combined noise factors to overcome. This is the received signal level at the output of the receiving antenna divided by the noise level at the same point in the receiver system. The minimum discernable signal (MDS) is the received signal level when the signal power equals the noise power. (Adamy D. L., Space Electronic Warfare, 2021)

Communications Jamming and radar jamming plus EP (electronic protection measures) are covered in (Adamy D. L., EW 103: Tactical Battlefield Communications Electronic Warfare, 2009) (Adamy D. L., EW 104: EW against a new generation of threats, 2015) (Nichols R. &., 2022). They are beyond the scope of this chapter.

CONCLUSIONS

For purposes of this chapter and Chapter 10, we have arbitrarily chosen three general altitude reference points: 1) Earth's surface (ground zero); 2) The maximum distance to Geosynchronous and Geostationary Satellites from the Earth's surface(22,236 mi); and 3) Deep Space beyond the maximum altitude for Satellites (>22,236 mi). (High Earth Orbit, 2023). Satellites are from Earth and present an excellent LOS from many of Earth's surfaces. Satellites are vulnerable and susceptible to three types of hostile activity: Signal Interception, Signal Jamming, or interference with uplink or downlink signals and spoofing signals to make the signals function incorrectly. Our main concentration has been on EW, with a secondary interest in spoofing signals. We have barely skimmed the topics of Orbital Mechanics (the language of Satellites), signal interception, jamming, spoofing, and ECD. However, it should give us enough of a flavor of the EW purview to extend our thinking into Deep Space Warfare (Chapter 12).

REFERENCES

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

Adamy, D. L. (2004). *EW 102 A Second 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. (2011 (2281st edition)). *Electronic Warfare Pocket Guide.* Raleigh, NC: SCItech.

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.

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.

Christian Wolff. (2022). *Radar and Electronic Warfare Pocket Guide.* Munich, Germany: Rhodes & Schwartz.

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.

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.

High Earth Orbit. (2023, Feb 1). Retrieved from Wikipedia: en.m.wikipedia.org

Humphreys, T., & al., e. (2008). Assessing the spoofing threat: Development of a portable GPS civilian spoofer. *In Radionavigation Laboratory Conf. Proc.*

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/

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.

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.

Nichols, R. &. (2022). Space Electronic Warfare, Jamming Spoofing and ECD. In R. Nichols, & e. al, *Space Systems: Emerging Technologies and Operations* (pp. 112 – 232). Manhattan, KS: New Prairie Press #47.

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. (2022). *Space Systems: Emerging Technologies and Operations.* Manhattan, KS: New Prairie Press # 47.

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

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.

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

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

Ranganathan, A., & al., e. (2016). SPREE: A Spoofing Resistant GPS Receiver. *Proc. of the 22nd ann Inter Conf. on Mobile Computing and Networking, ACM*, pp. 348-360.

S.A.Shaukat, & al., e. (2016). Robust vehicle localization with GPS dropouts. *6th ann Inter Conf on Intelligent and advanced systems* (pp. 1-6). IEEE.

USGPO. (2021, June 14). *What is GPS.* Retrieved from Gps.gov: www.gps.gov/sysytems/gps

Warner, J., & Johnson, &. R. (2002). A Simple Demonstration that the system (GPS) is vulnerable to spoofing. *J. of Security Administration*. Retrieved from https://the-eye.eu/public/Books/Electronic%20Archive/GPS-Spoofing-2002-2003.pdf

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

What is Deep Space. (2023, Feb 2). Retrieved from Wikipedia: https://www.quora.com>whats the difference between 'space', 'outer space', 'deep space'

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.

ENDNOTES

[1] Professor Adamy has about 50+ years of experience and, as an SME, has written an accelerated set of EW 101-104 textbooks to define the entire EW playing field. The author was privileged to study under this accomplished researcher, practitioner, lecturer, and author.

[2] 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.

[3] (Adamy D. L., Space Electronic Warfare, 2021) covers all these losses in nauseating detail. From a ChE POV (ye author), they are just a total system loss regardless of root causes. One number. EEs and RADAR engineers will find this statement heresy.

[4] Spoofing affects the same path as a jammer.

[5] A precursive jamming operation often accompanies spoofing. (Nichols R. K., 2020)

[6] There are important numbers for space EW calculations: A solar day is 24 hours or 1440 minutes. The sidereal 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 min**2. The 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. The synchronous satellite period is 23 hours and 56 minutes. The 12-hour satellite is 20,241 km high. The 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.

[7] This is truly a complex subject. Chapter 10 has scratched only the surface. Rhode & Schwartz presents a marvelous Pocket Guide to initiate the student in Radar and EW. It is illustrated and gives all the formulas on the subject. (Christian Wolff, 2022) Professor Adamy has also issued a popular Electronic Warfare Pocket Guide that reiterates all the Chapter 10 formulas and explains them better. (Adamy D. L., Electronic Warfare Pocket Guide, 2011 (2281st edition))

[8] Aircraft signal transfer is one of many means to localize indoor signals. HAPs, WiFi, Ultrasound, Light, Bluetooth, RFID Sensor fusion, and GSM are all in the decision-making process.

[9] 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)

[10] 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.

[11] The author has nicknamed Dr. Manuel Eichelberger's brilliant doctoral research ECD. ECD is Dr. Manuel Eichelberger's advanced implementation of CD to detect and mitigate spoofing attacks on GPS or ADS-B signals

[12] This is a key point. CD reduces this timestamping process significantly.

[13] Data is sent on a carrier frequency of 1575.42 MHz (IS-GPS-200G, 2013)

[14] GPS satellites operate on atomic frequency standards; the receivers are not synchronized to GPS time.

[15] 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 costs the user both latency and power.

[16] The vector/tensor mathematics for localization are reasonably complex and can be found in Chapter 5.3 of (Eichelberger, 2019)

[17] (Eichelberger, 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)

[18] Cloud offloading also makes ECD suitable for energy-constrained sensors.

[19] (Nichols & al., Unmanned Vehicle Systems and Operations on Air, Sea, and Land, 2020) have argued the case for cryptographic authentication on civilian UAS /UUV and expanded the INFOSEC requirements.

[20] 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.

[21] His work borders on brilliant, and all mathematicians/computer scientists need to read about it.

[22] EW and EW subsets are defined in the Acronyms and Abbreviations front matter.

[23] These factors are called *externals.*

[24] These factors are known as internals.

11.

SPACE SYSTEMS MODELING AND SIMULATION [DIEBOLD]

PURVIEW

Various industries, from business to engineering to the military, use the concepts of modeling and simulations for multiple applications. Regardless of the use case, modeling and simulation strive to predict the results of an actual event, accounting for all the potential variables and performance parameters, to improve the likelihood of success during execution.

This chapter seeks to 1. describe the history and value of modeling and simulation in the context of modern aerospace and national defense challenges, 2. provide current techniques and toolsets that apply modeling and simulations, 3. and describe the use cases for leveraging these techniques.

LEARNING OBJECTIVES

- Students will understand the criticality of aerospace systems modeling and simulations in the context of modern threats and multi-domain operations.
- Students will have a working knowledge of the inputs that contribute to building a space model and methods for simulating space threats.
- Students will understand the use cases for modeling and simulation for commercial and defense purposes.

KEY TAKEAWAYS

- Modeling and simulation of a space shuttle's flight or a satellite's orbit are inherently different from aviation because, in most cases, a spacecraft cannot be recalled and must be validated across the totality of its operational mission before the first launch attempt.
- The use of space for civil, commercial, and military purposes has expanded exponentially since the 1960s, with over 4,000 operational satellites and estimated hundreds more pieces of debris in orbit today

flying at thousands of km/h. The advent of intercontinental, hypersonic, and anti-satellite weapons further complicated operations in space, which the US now interprets as a warfighting domain.

- Models and simulations can be categorized by their application (area/environment), resolution level (scale), role (function), and technique. In addition, various computer-based tools are widely available for civil, commercial, and military uses, which augment or replace the legacy tabletop wargaming techniques used to inform decisions about space operations.

INTRODUCTION

Before the advent of computers and automation, military theorists aptly described the enduring characteristics of war and what made great leaders successful in predicting the outcomes of battles. In *The Art of War*, written approximately 2,500 years ago, Sun Tzu articulated a component of strategy as knowing the enemy and oneself. If you can clearly understand both, you need not fear the result of a hundred battles (Tzu). In the 1800s, Carl von Clausewitz wrote *On War*, describing probability as one component of the paradoxical trinity. Probability amounts to the fog and friction inherent in combat, comparable to the operational and mission variables[1], as well as chance, accounting for the factors of any given situation that one cannot predict (Clausewitz). In the same period, Baron de Jomini wrote *The Art of War*, taking a scientific approach by applying critical tenants to the planning and execution of war that would guarantee a commander's success (Jomini). The latter two theorists built their concepts after observing Napoleon, whom many considered a "military genius" during the rise of nation-states and the French Revolution. Unlike modern military, civilian, and business leaders, Napoleon relied on intellect and aptitude to make decisions, observed as having the gift of *coup d'oeil*.[2] In other words, he had the ability to see all factors and variables of a battle wholistically in a way that allowed him to make rapid and accurate decisions with near clairvoyance (Clausewitz).

Although each theorist described the timeless principles of war and what made leaders like Napoleon successful, none lived in a period where the prospect of space warfare, computers, or automation was possible. However, their observations collectively highlight the same problems modern modeling and simulations address, which historical military leaders solved with theory, strategy, and intuition. Given a set of resources, an operating space, and unpredictable variables, how can we reliably estimate the outcome of any given space operation?

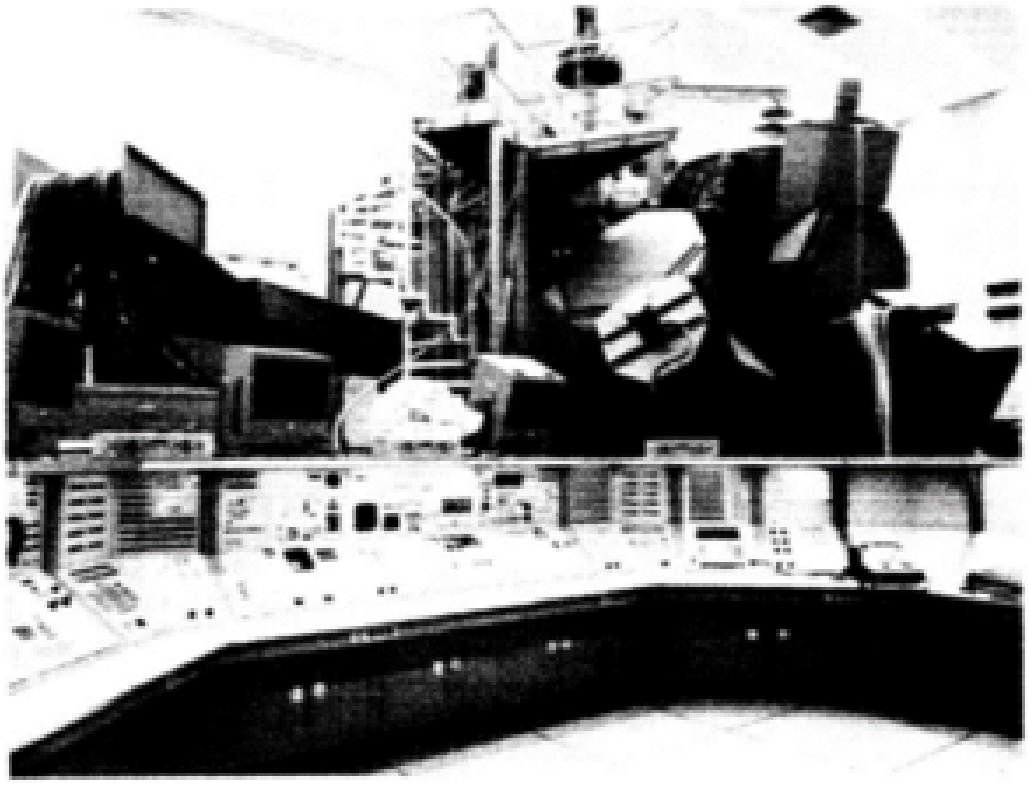
The modern age of computing and automation made simulations famous when predictions became more than just thoughts in the minds of expert planners, using vast data sets and calculations to rapidly and objectively compute an outcome that humans would never be able to complete. *WarGames*, the 1983 classic movie where David Lightman (Matthew Broderick) discovers North American Aerospace Defense Command's (NORAD) War Operation Plan Response (WOPR) supercomputer simulator, fantasizes about the impact of modeling thermonuclear and biotoxic chemical war. WOPR simulated a Soviet Union first-strike nuclear attack against the United States, autonomously triggering a response by US nuclear sites that

nearly started World War III. WOPR performed hundreds of simulations with different variables and found no scenario where a ballistic missile-enabled atomic war could be won (Badham, 1983). The fantasy dreamed by Hollywood 40 years ago is now a reality of the 21st century, with the WOPR demonstrating an actual use case of modeling and simulations used by the US military. Today, dozens of modeling software programs and fully customized simulators for aerospace purposes are widely accessible and, in some cases, made secretly for national defense. Although supercomputers are necessary for some simulations, depending on the precision and accuracy required, devices as small as a smartphone or a tablet computer now have the computational power to get results for various use cases. Before attempting to understand the "what" and "how," it is essential to know why space modeling and simulations are critical in modern aerospace challenges.

SPACE LAUNCH HISTORY AND CONTEXT

The National Aeronautics and Space Administration (NASA) opened on October 1, 1958, with aspirations to achieve President Kennedy's objective of completing the first human trip to the moon in the 1960s. NASA accomplished this goal with the Apollo 11 mission in July 1969 and subsequently expanded the mission with five more successful moon landings through 1972 (NASA, 2018). However, none of NASA's early successes in the Mercury (1958-1963), Gemini (1962-1966), and Apollo (1961-1972) programs could have been possible without extensive modeling and simulations of the first spaceflights before they launched. In 1973, Carroll H. "Pete" Woodling, Chief of NASA's Crew Training and Simulation Division from 1972-1974 (NASA, 2000), published an experience report of the simulations of manned space flight for crew training. He defined a simulator as a "complex set of hardware (including computers, visual display systems, and simulated crew stations) that presents, with a high degree of accuracy, the total flight characteristics of the actual spacecraft and mission." In the years leading up to Mercury, Gemini, and Apollo program launches, flight crews spent one-third or more of their total training time in simulations, such as the Command Module Simulator depicted in Figure 11-1. During this period, mission simulators dominated much of the total simulation time, growing from 53% to 67% to 80% across the Mercury, Gemini, and Apollo programs. The 59 crew members in these programs spent 38,261 hours (~4.37 years) conducting simulations before their space missions between 1958 and 1972 (See Figure 11-2) (Woodling, et al., 1973).

Figure 11-1: Apollo Program Command Module Simulator



Source: (Woodling, et al., 1973)

Figure 11-2: Simulator Use for Flight Crew Training

Simulator	Time per program, hr			Total time, hr
	Mercury	Gemini	Apollo (through mission 11)	
Mercury procedures simulator (2)	708	--	--	708
Air-lubricated free-attitude trainer	83	--	--	83
Multiple-axis spin test inertial facility	27	--	--	27
Part-task trainer (2)	175	--	--	175
Centrifuge	239	100	59	498
Gemini mission simulator (2)	--	6883	--	6 883
Dynamic crew procedures simulator	--	438	507	945
Translation and docking simulator	--	276	64	340
Part-task trainer	--	81	--	81
Rendezvous simulator	--	1417	--	1 417
Command module simulator (2)	--	--	16 584	16 584
Lunar module simulator (2)	--	--	10 672	10 672
Command module procedures simulator	--	--	1 008	1 008
Lunar module procedures simulator	--	--	753	753
Lunar landing training vehicle and simulator, lunar landing research facility[a]	--	--	949	949
Manned Spacecraft Center mission evaluators	--	--	146	146
Translation and docking simulator (Langley Research Center)	--	--	87	87
Contractor mission evaluators	--	--	899	899
Massachusetts Institute of Technology evaluators (2)	--	--	56	56
Full-mission engineering simulator	--	--	174	174
Simulator prebriefing and postbriefing	[b]175	[b]403	[b]769	[b]1 349
Partial-gravity simulator, mobile partial-gravity simulator	--	[b]50	[b]37	[b]120
Total	1359	8994	29 907	39 261

[a]Time computed on the basis of 2 hours logged for each LLTV flight.
[b]Not included in total simulator hours.

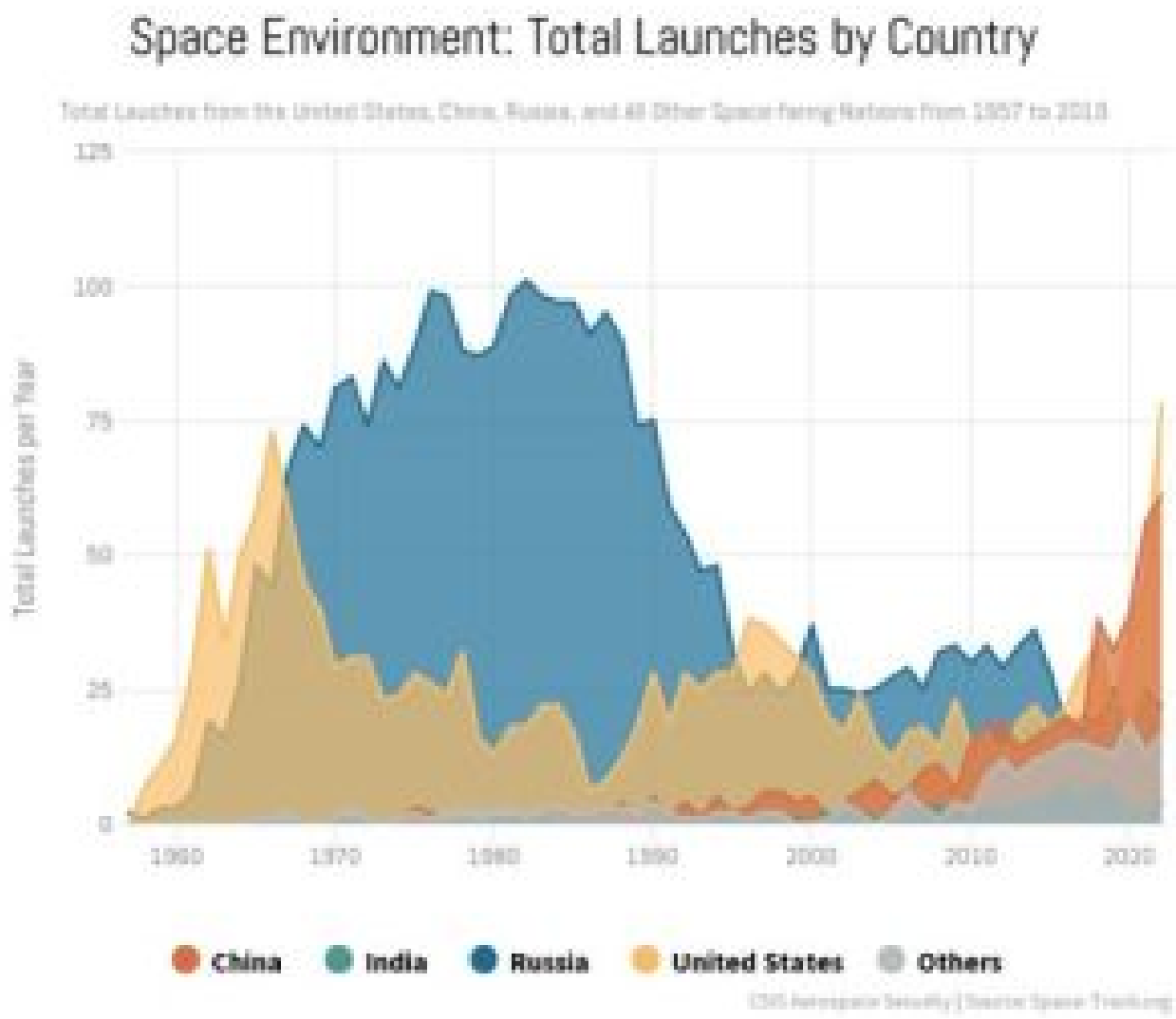
Source: (NASA TN D-7122)

The success or failure of space missions and the crew's safety relies more on modeling and simulation than any type of aviation operation. The nature of space flight, both in the 1960s and today, is unique in that the vehicle is fully committed at lift-off or launch to the entire mission, experiencing a broad range of mission variables during extended operational timelines. There is no immediate ability to recall vehicles launched into space, like cruise, ballistic, hypersonic missiles, torpedoes, and many unmanned vehicle operations in denied

areas (FCNL Education Fund, 2021). Space flight is starkly different from manned aviation where aircraft and crew members are trained and evaluated through live environment flights to validate proficiency and capability gradually. Space vehicles and their crew members must be prepared, proficient, and validated on the entirety of the mission, accounting for all potential flight variables and contingencies before the first launch attempt. After analyzing all of NASA's earliest space endeavors, Woodling noted the use of comprehensive, high-fidelity simulators as a firm requirement in future space programs (Woodling, et al., 1973).

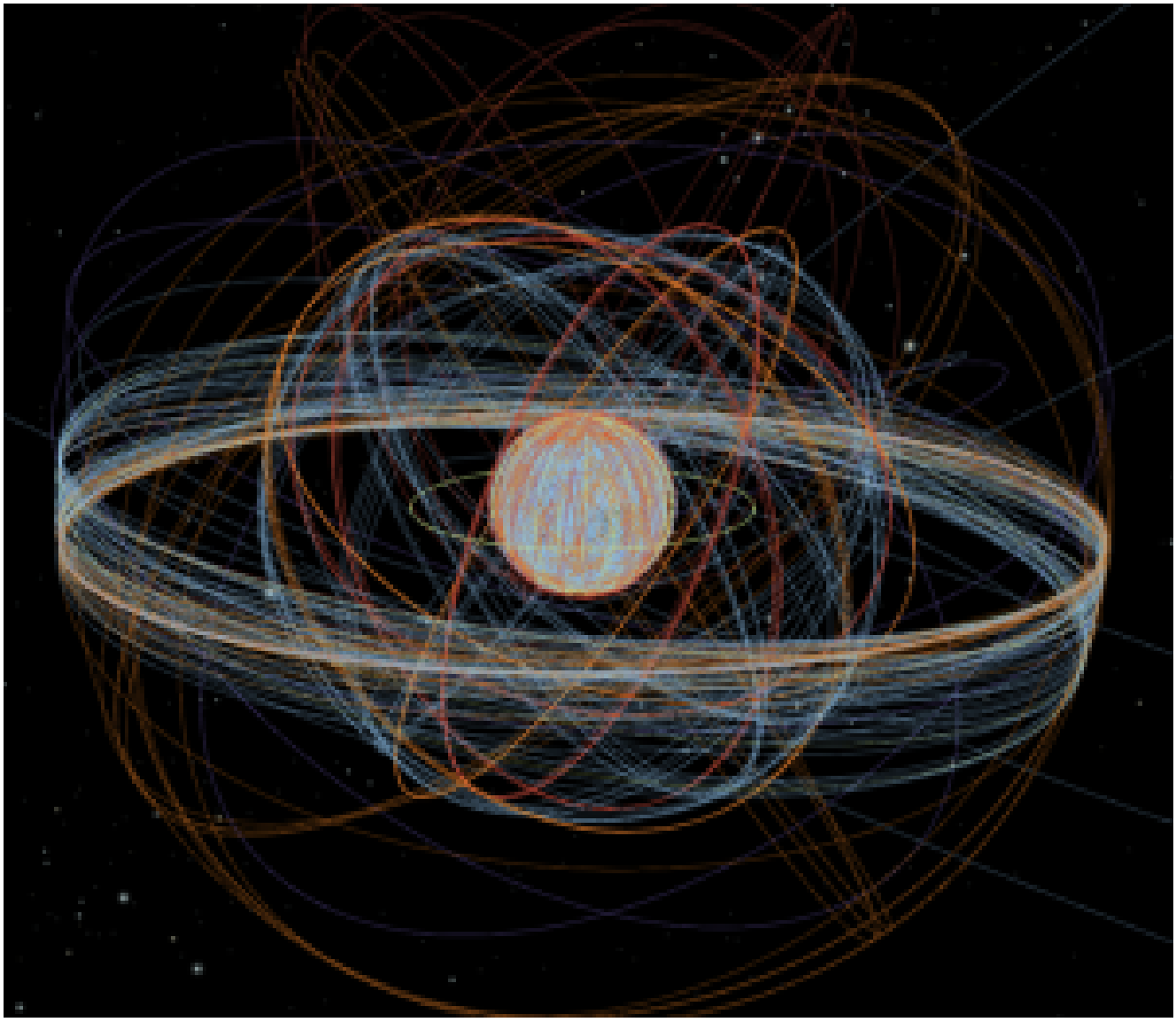
The wide use of modeling and simulation is essential moving into the 21st century as space flight becomes increasingly commonplace. Although sources differ on the number of successful space missions, there were more space launches in 2022 than in any other year. The Center for Strategic and International Studies (CSIS) reported 182, a 29% increase over 2021 (See Figure 11-3) (CSIS, 2023). Space-based capabilities are also becoming increasingly ubiquitous in everyday life as the cost of commercial space use decreases, and private companies take the lead. Following the retirement of the US space shuttle program, the US government had to rely on other national and commercial launch providers to move goods and astronauts to the international space station. New micro and nanosat technology facilitated the development of small satellites at low cost, which drove the increase in commercially licensed space launches by 100% between 2016 and 2018, primarily in the Low Earth Orbit (LEO) category. As of 2020, approximately 2,000 active satellites were orbiting Earth with 1,300 in LEO, 75 in Medium-Earth Orbit (MEO) (primarily for global navigation services), and 430 in Geosynchronous-Earth Orbit (GEO) (most often used for telecommunications and weather) with 2021 breaking a trend by adding over 1,400 satellites in a single year (International Trade Administration, n.d.) (Chakrabarti, 2021) (NASA, 2009). Some sources place the total number of satellites in orbit today at well over 4,000, with 75 countries owning at least one satellite, over 60% of the total attributed to the US, and SpaceX being the largest private company owner responsible for over 43% of active satellites (See Figure 11-4) (ESRI, 2022). In addition to the commercial satellite space, SpaceX's Inspiration4 made history on September 15, 2021, as the first all-civilian space mission to launch into Earth's orbit, following two successful sub-orbital space flights by Virgin Galactic's Unity 22 and Blue Origin's New Shepard (Howell, 2021). Although science and technology have improved the capability to launch satellites dramatically since *Sputnik* (the first satellite launched into Earth's orbit on October 4, 1957), the number of players, time constraints, weather, and space obstacle variables have increased concurrently, placing a more significant burden on advanced modeling and simulations to achieve successful space flights. However, civilian space vehicles and satellites are not the only use case for aerospace simulators today. Advanced missile systems and unmanned vehicles developed since the 1940s now require the same precision and accuracy as a rocket flying into space. This represents another modeling and simulation use case applied across the multi-domain operations spectrum.

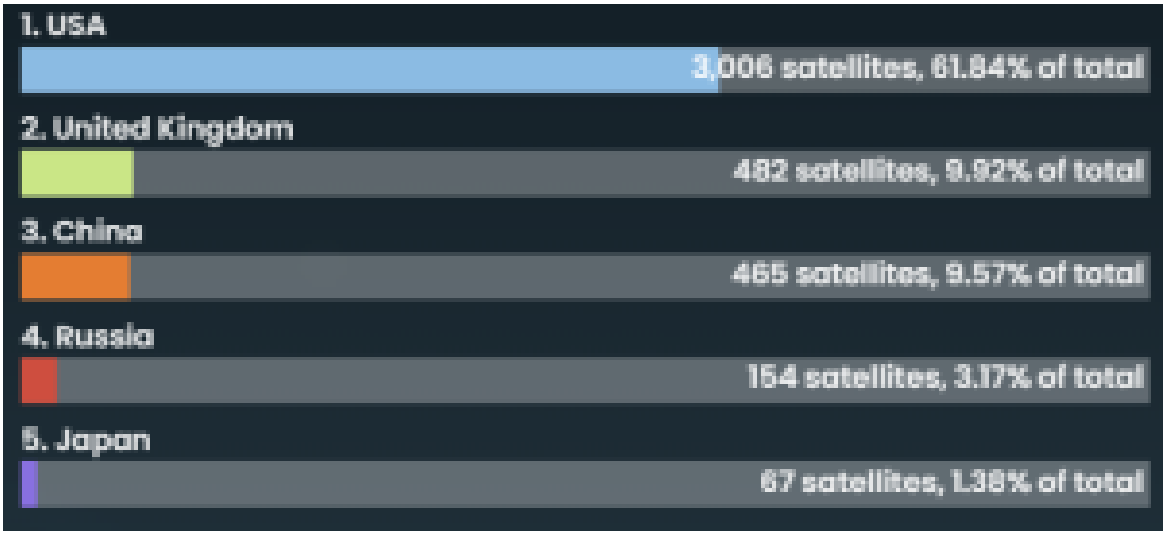
Figure 11-3: Space Environment: Total Launches by Country from 1957 to 2022



Source:(CSIS Aerospace Security | Space-Track.org)

Figure 11-4: Graphic Representation of All Satellites Orbiting Earth by Country of Ownership




1. USA
3,006 satellites, 61.84% of total
2. United Kingdom
482 satellites, 9.92% of total
3. China
465 satellites, 9.57% of total
4. Russia
154 satellites, 3.17% of total
5. Japan
67 satellites, 1.38% of total

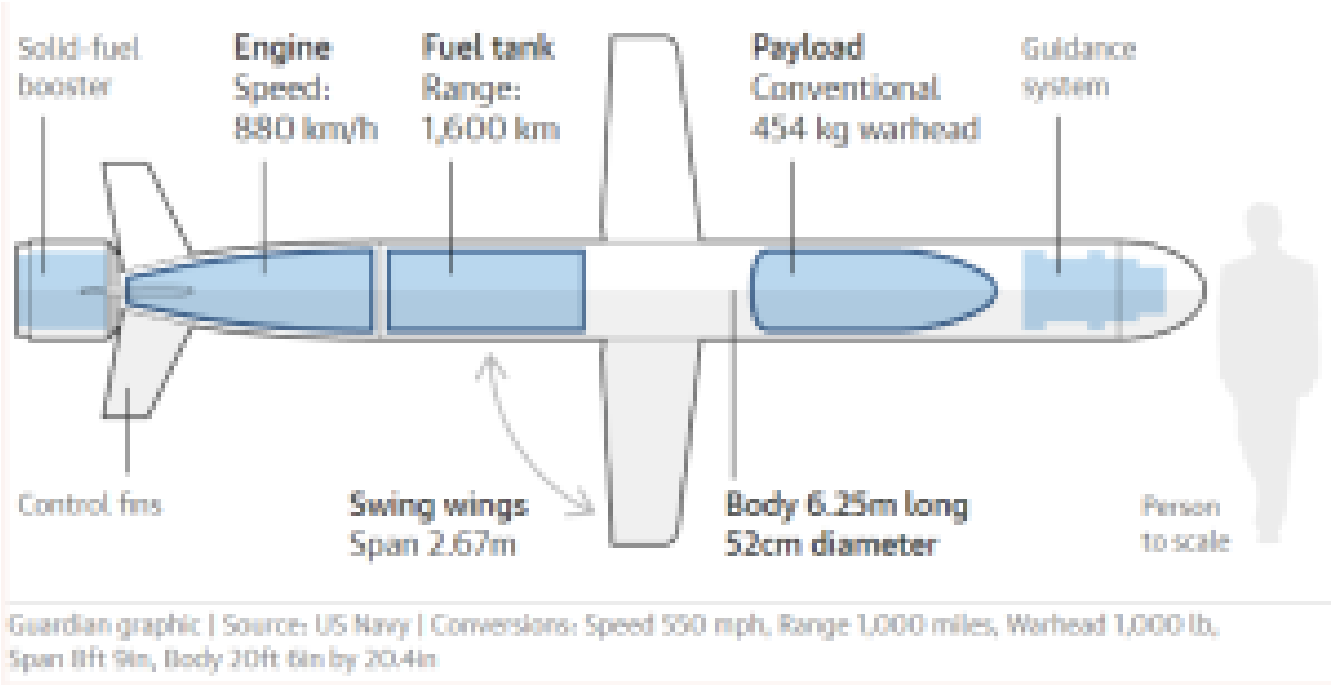
Source: (Satellite Explorer | ESRI)

EVOLVING THREAT CONTEXT

The tools of war have evolved with revolutions in military affairs, providing a temporary asymmetric advantage to the user who had it first. Regarding the use cases for modeling and simulation, none is more significant than the advent of the cruise missile, a low-flying, guided rocket weapon with a low radar cross-section. The German V-1, developed in the early 1940s, is widely understood to be the first cruise missile, and was initially used against London from 1942-1944 (The Editors of Encyclopedia Britannica, 2023). As a precursor to the weapons later developed by the US, Soviet Union, China, and others, the V-1 had a length of 27 ft, carried an 850 kg warhead, flew at 640 km/h, and had an operational range of 250 km (P., 2014). It had limited aerodynamic controls and poor accuracy, with only about 25% reaching its intended targets (University of Florida Department of Mechanical & Aerospace Engineering). Although its characteristics are similar, the lacking range, in-flight controls, and accuracy of the German V-1 are almost incomparable to the most capable cruise and ballistic missiles employed today by the US.

The US's most prominent operational cruise missile is the Tomahawk (See Figure 11-5), which comes in dozens of variants and can carry both conventional and nuclear payloads. The Tomahawk has been in service since 1983, can carry a 454 kg payload, and range as far as 2,500 km at subsonic speeds or up to 800 km/h depending on the mission and weapon variant.[3] Unlike the V-1, the Tomahawk incorporates a mix of Terrain Contour Matching (TERCOM), Digital Scene Matching Area Correlation (DMAC), and Global Positioning Satellite (GPS) guidance to achieve precision and accuracy, validated through service in the 1991 Gulf War and 2003 Iraq invasion among other conflicts. One of the most public, widely known examples of a mass cruise missile strike was on April 6, 2017, when the US fired 59 Tomahawks against Shayrat Air Base to destroy Syrian forces that conducted a chemical attack against the city of Khan Sheikhoun (See Figures 11-6, 11-7, and 11-8) (CSIS Missile Defense Project, 2023). To execute this attack, each missile had to be individually planned from launch to impact and synchronized in time and space to ensure the mission's success and limit collateral damage (Eckstein, 2017). This type of operation is only possible with modern modeling of the weapon's characteristics and a thorough simulation of the missile's flight against numerous variables, including weather and threat missile defenses. For responsible nation-states seeking to limit collateral damage, the planning, accuracy, and precision requirements for each missile launch only increase as the weapon becomes more deadly.

Figure 11-5: Tomahawk Missile Model

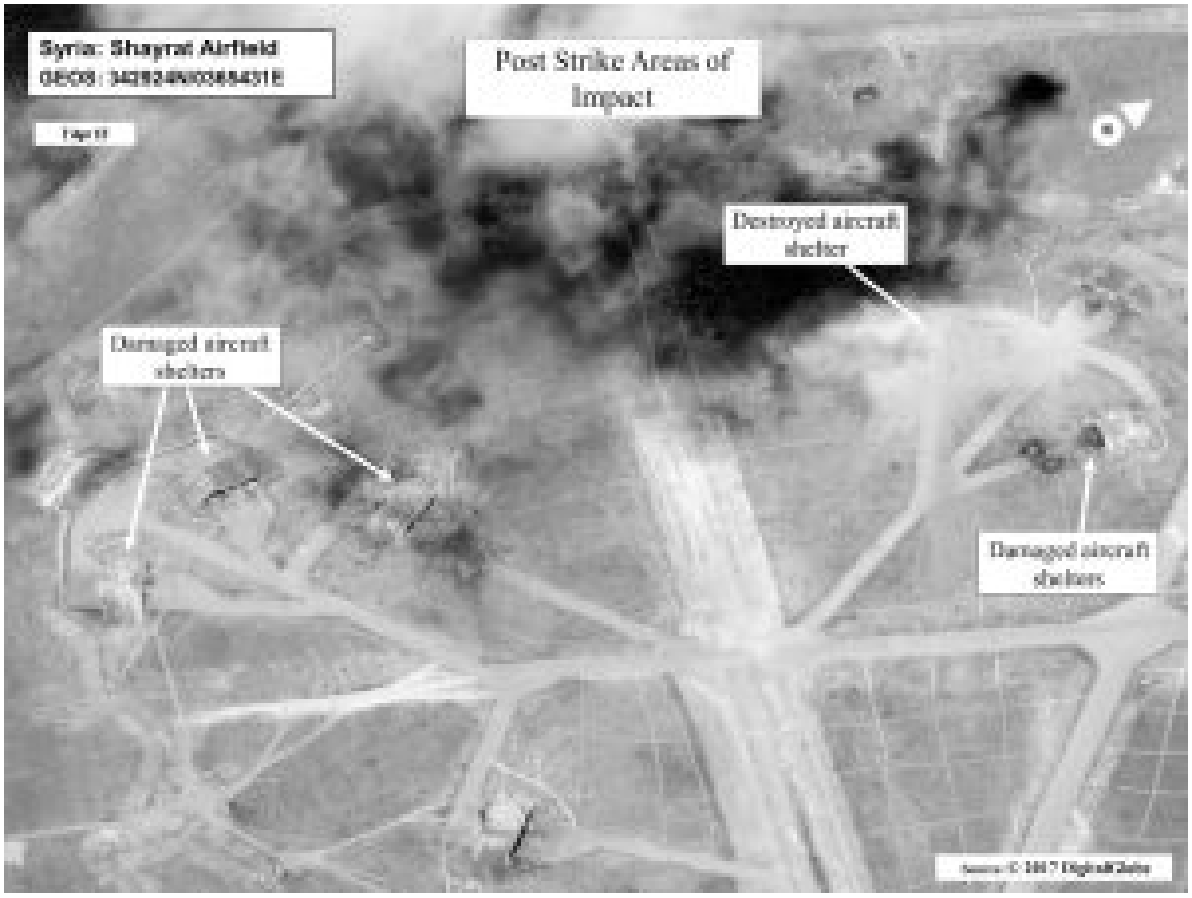


Source: (The Guardian | Credit: US Navy)

Figure 11-6: Image of Sharyat Airfield, Syria

Source: (USNI News | Image Credit: US Department of Defense)

Figure 11-7: Aftermath of 2017 Tomahawk Strike on Shayrat Airfield



Source: (USNI News | Image Credit: US Department of Defense)

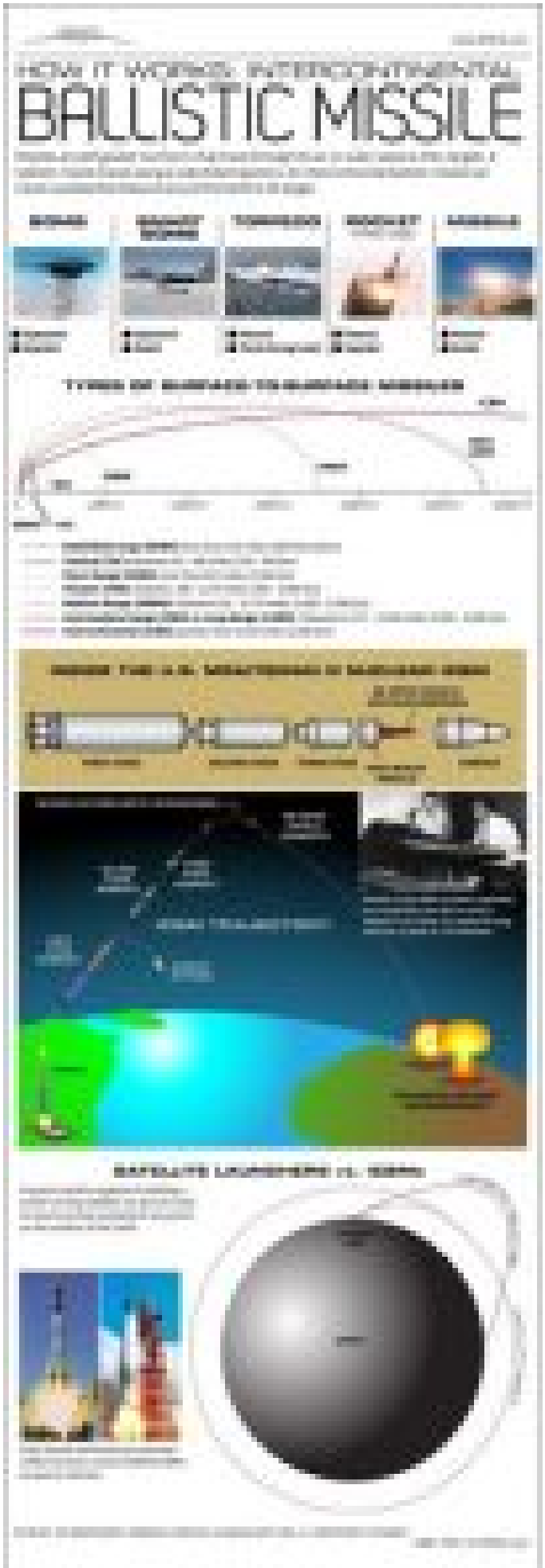
Figure 11-8: Aftermath of 2017 Tomahawk Strike on Shayrat Airfield

Source: (USNI News | Image Credit: US Department of Defense)

The LGM-30G Minuteman III, which started service in 1970, is a solid-fueled Intercontinental Ballistic Missile (ICBM) and the only remaining land-based component of the US nuclear triad. By the numbers, it has a length of 18.2m, carries either a 335kT (W78) or 300kT (W87) nuclear warhead, and has a range of 13,000km. Although details on the US nuclear triad are limited, available documentation suggests the Minuteman III has a fast launch time (consistent with solid fuel propellant), 100% reliability in testing, and backup launch controllers that make the system more resilient (CSIS Missile Defense Project, 2021). Moreover, the Minuteman III travels on a suborbital trajectory outside Earth's atmosphere, like the early ICBMs modified for use as launch vehicles for manned orbital missions (Refer to Figure 11-9) (Tate, 2021). Unlike cruise missiles, nuclear weapons have only been used offensively twice in history, during the bombings of Hiroshima and Nagasaki, Japan, by the US on August 6th and 9th, 1944 (History.com Editors, 2022). The "Little Boy" and "Fat Man" bombs were delivered by B-29 aircraft and instantly killed 80,000 and 40,000 people between Hiroshima and Nagasaki, respectively. "Little Boy" and "Fat Man" were deployed over their targets without modern weapons' precision guidance and accuracy (History.com Editors, 2009).

Imagine a scenario where a Minuteman III is launched from North Dakota, intending to strike Hiroshima over 9,500 km away. In one simulation with the W78 payload, the Minuteman III could cause over 329,000 fatalities and 457,000 injuries at Hiroshima in a single airburst strike, quadrupling the immediate casualty count observed in World War II (Wellerstein, 2022). The impact of a failure or deviation at any point from missile launch to detonation could be catastrophic. Like a spacecraft, there is no ability to recall an ICBM-delivered nuclear weapon and, indeed, no ability to evaluate the exact mission profile before launch. The situation, performance characteristics of the flight, and impact all justify the heavy application of modeling and simulation before ever attempting an ICBM launch to increase the chances of a successful flight and the accuracy of the missile itself. Space-based modeling, concerning ICBMs, is even more important as the prospect of a launch vehicle in orbit capable of delivering a nuclear weapon to any point on Earth becomes a reality.

Figure 11-9: How it Works – Intercontinental Ballistic Missile

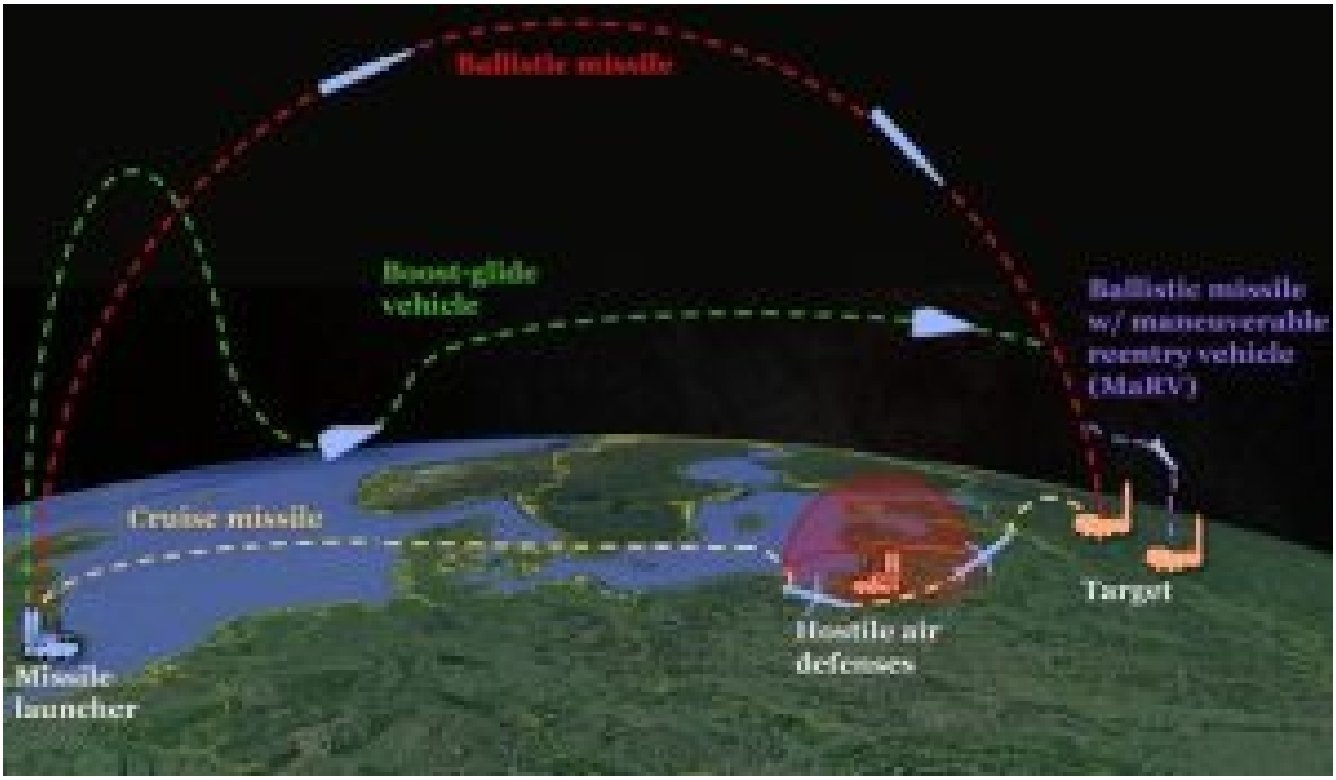

BALLISTIC MISSILE

(Sources: The Independent, Wikimedia Commons, Globalsecurity.org, U.S. Department of Defense | Image Credit: Karl Tate/Space.com)

Hypersonic weapons further complicate the modeling and simulation process in both the offensive use of the missile and defense against missile attacks from peer adversaries. Although hypersonic weapons have existed for over 50 years, China, Russia, and the US have made recent progress in the capability to deploy these missiles for reliable, sustained flight (Watts, Trotti, & Massa, 2020). There are two basic categories of hypersonic weapons. Like ICBMs, Hypersonic Glide Vehicles (HGV) can launch into space using a rocket and orbit the Earth under their momentum or travel at suborbital speeds before re-entry and maneuvering through the atmosphere. HGVs are sometimes called hypersonic boost-glide weapons when combined with their rocket booster. The second category is the Hypersonic Cruise Missile (HCM), which is powered by a high-speed, air-breathing engine after acquiring its target (Congressional Research Service, 2023). HCMs are like other cruise missiles in their ability to maneuver throughout flight rather than following a specific trajectory, but differ from other missile types in their speed, traveling between Mach 5 and 25 for an entire flight if required. Refer to Figures 11-10 and 11-11 for a graphic comparison of hypersonic, cruise, and ballistic missiles. Modern hypersonic weapons can capture the best characteristics of both ICBMs and cruise missiles by adding speed and the ability to maneuver for an entire flight, forming a hybrid of existing model classifications (Brockmann & Schiller, 2022). The US Army, with cross-service participation, plans to integrate these new classifications of hypersonic missiles into the 1st Multi-Domain Task Force (MDTF) in 2023, forming a battery within the Strategic Fires Battalion (Congressional Research Service, 2023). See Figure 11-12 for a depiction of a generic MDTF structure. In concept, these weapons will be commanded through the Army's Advanced Field Artillery Tactical Data System (AFATDS) and require unique Transporter-Erector-Launchers (TEL) (Freedberg, 2019). See Figure 11-13 for a picture of the prototype hypersonic weapon delivered to 17th Field Artillery Brigade. Among the multiple reported hypersonic projects on the horizon, the U.S. Air Force has also evaluated the air-launched AGM-183A (See Figure 11-14) with the B-52H since April 2021 (Tingley, 2022). Concurrent with US developments, China and Russia have also built and evaluated capable hypersonic weapons. In mid-2021, China experimented with two hypersonic gliders launched into LEO, traveling partially around the Earth before being released to engage test targets (See Figure 11-15 for a model of the Chinese DF-ZF). These tests differed from the short, suborbital, ballistic flight with which an HGV is typically deployed, demonstrating an intercontinental travel capability (The International Institute for Strategic Studies, 2022). Additionally, Russia has used the Kinzhal hypersonic missile (See Figure 11-16), an air-launched variant deployable by MiG-31 and Su-34 fighters unveiled in 2018, in combat against Ukraine as recently as March 2023 in conjunction with a conventional missile attack (Neuman, 2023). Requirements for planning a hypersonic missile strike in the modeling and simulations space also translate to defending against them, complicating existing homeland defense planning for Aegis Ballistic Missile Defense (BMD), Ground-Based Mid-Course Defense (GMD), and Terminal High Altitude Area Defense (THAAD) systems (GAO, 2022). See Figures 11-17 and 11-18

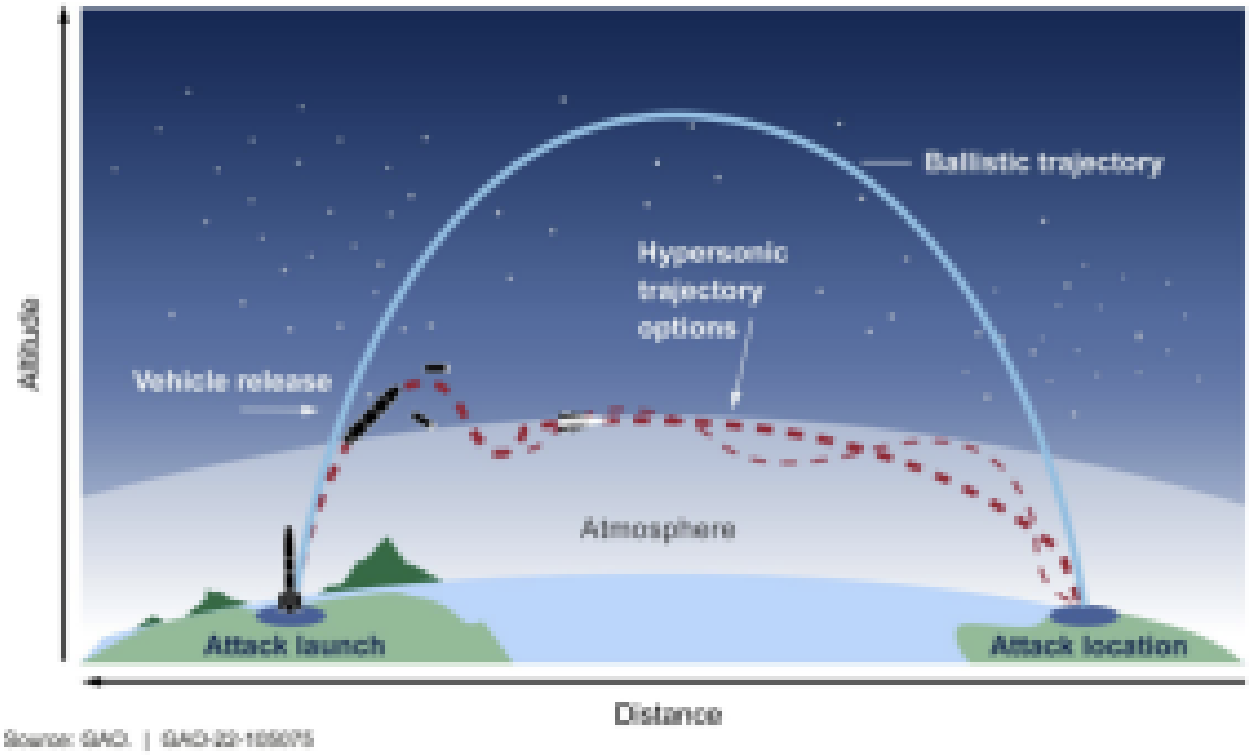
for graphic depictions of notional, layered missile defense scenarios. See Figure 11-19 for a description of US missile defense system programs.

Figure 11-10: Notional Flight Paths of Hypersonic Boost-Glide Missiles, Ballistic Missiles, and Cruise Missiles



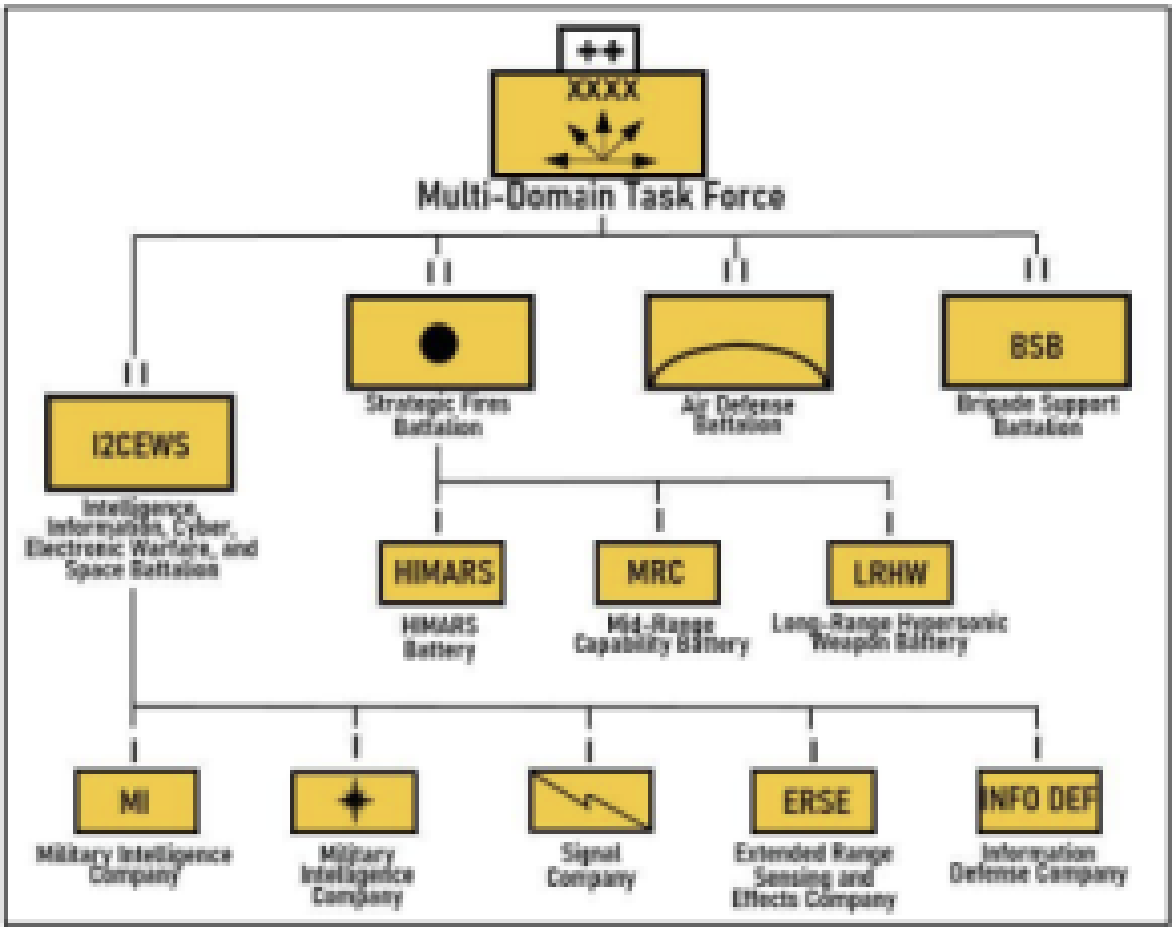
Source: (Breaking Defense | Credit: CSBA)

Figure 11-11: Ballistic vs. Hypersonic Missile Trajectories



Source: (GAO-22-105075)

Figure 11-12: Notional Generic MDTF



Source: (CRS IF11797 | Credit: Chief of Staff Paper #1 Army Multi-Domain Transformation Ready to Win in Competition and Conflict)

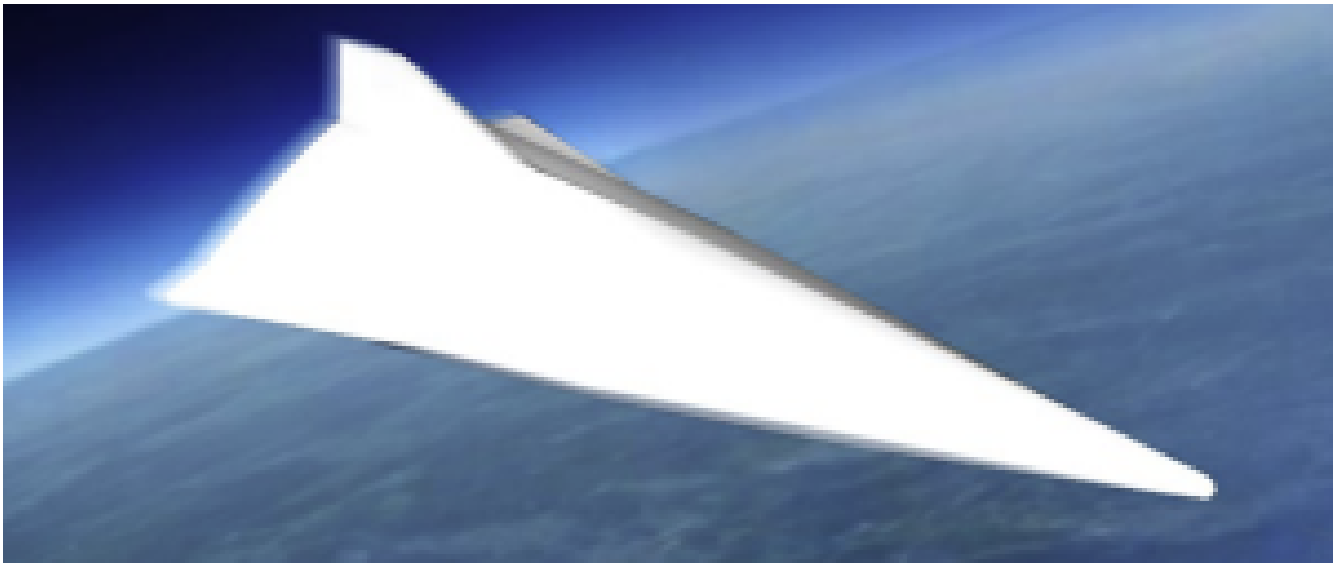
Figure 11-13: The delivery of the prototype hypersonic hardware to soldiers of 5th Battalion, 3rd Field Artillery Regiment, 17th Field Artillery Brigade is completed Oct. 7, 2021, with a ceremony at Joint Base Lewis-McChord, Washington

Source: (Defense News | Image Credit: Staff Sgt. Kyle Larsen/U.S. Army)

Figure 11-14: Crew members from the 912th Aircraft Maintenance Squadron secure the AGM-183A Air-launched Rapid Response Weapon Instrumented Measurement Vehicle 2 as it is loaded under the wing of a B-52H Stratofortress during a hypersonic test, Edwards Air Force Base, Calif., Aug. 6, 2020.

Source: (Space.com | Image Credit: USAF/Giancarlo Casem)

Figure 11-15: Model of Chinese DF-ZF Hypersonic Missile

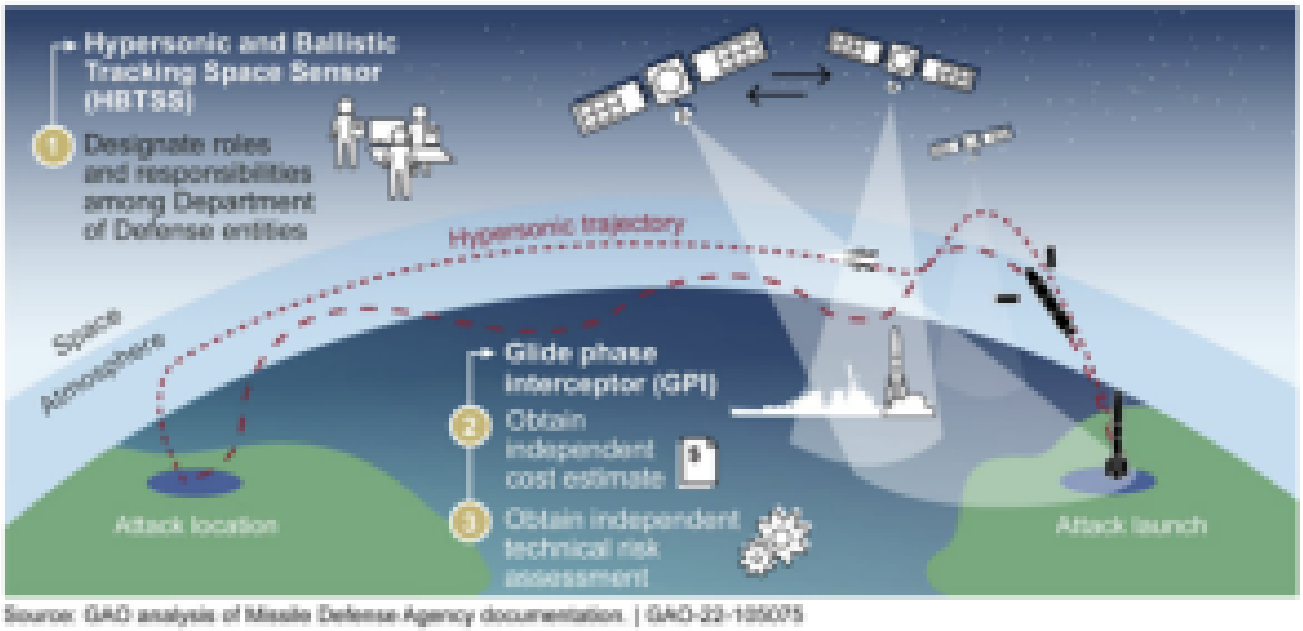


Source: (Atlantic Council | Credit: Wikimedia Commons)

Figure 11-16: Russian Kinzhal Hypersonic Ballistic Missile

Source: (Atlantic Council | Credit: Wikimedia Commons)

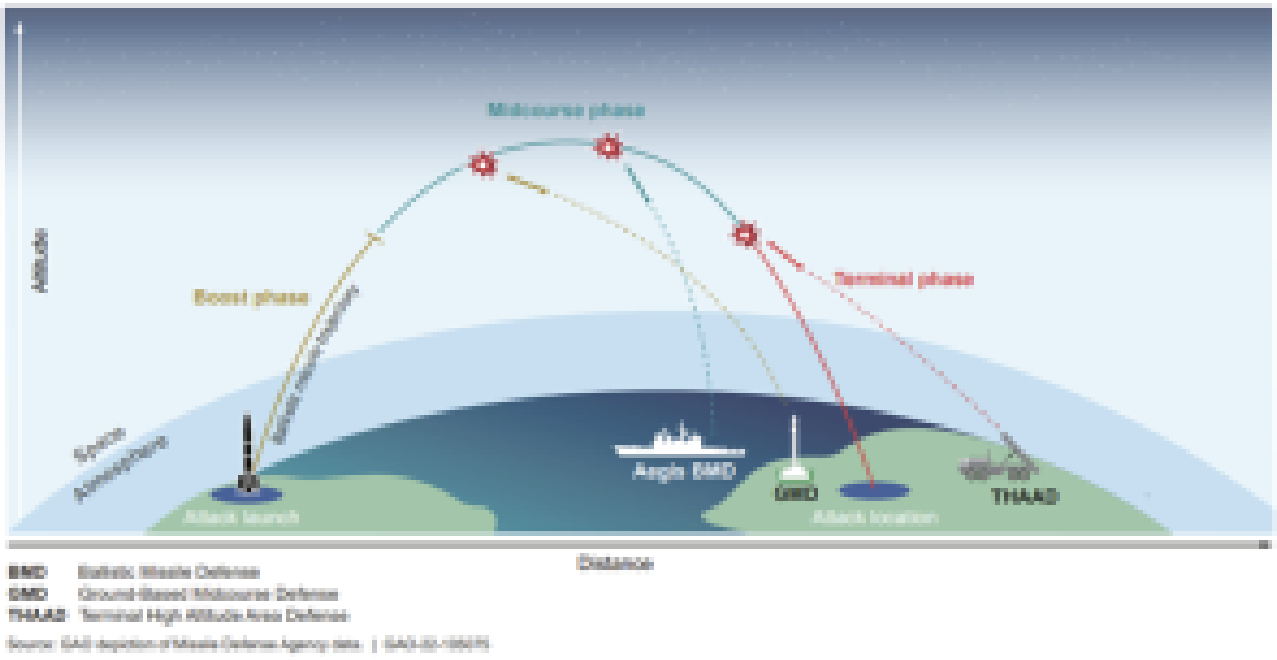
Figure 11-17: Missile Defense Agency's Hypersonic Efforts in a Notional Scenario



Source: GAO analysis of Missile Defense Agency documentation. | GAO-22-105075

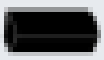
Source: (GAO-22-105075 from analysis of Missile Defense Agency Documentation)

Figure 11-18: Notional Depiction of Layered Homeland Defense



Source: (GAO-22-105075 from Depiction of Missile Defense Agency Data)

Figure 11-19: Description of Missile Defense System (MDS) Programs

	Name	Description
Aegis Weapon System	 Aegis BMD	Ship- and land-based ballistic missile defense capabilities using a radar, command and control, and Standard Missile (SM)-3 interceptors.
	 Aegis Ashore	A land-based system that uses a radar, command and control, and SM-3 interceptors. There are three locations: a test site in Hawaii, and two operational sites—one in Romania and one under construction in Poland.
	 Aegis Ballistic Missile Defense Standard Missile (SM)-3 interceptors	SM-Block IA, IB, and IIA interceptors capable of identifying, tracking, and defending against short, medium, and intermediate-range threat missiles. The most recent interceptor variant—SM-3 IIA—has increased range, more sensitive seeker technology, and an advanced kill vehicle.
	 Command, Control, Battle Management, and Communications (C2BMC)	A globally deployed system of software and hardware—workstations, servers, and network equipment—that facilitates the integration and management of diverse weapon systems and sensors to enable a coordinated response to defend against incoming threat missiles.
	 Ground-Based Midcourse Defense (GMD)	A ground-based system with launch, communications, and fire control that uses interceptors with a booster and kill vehicle to defend against intermediate- and intercontinental-range missile threats.
Sensors	 Army Navy/Transportable Radar Surveillance and Control Model-2 (AN/TPY-2)	A transportable X-band high-resolution radar capable of tracking missiles of all ranges. It operates in two modes: (1) forward-based mode—used to detect threat missiles once launched, or (2) terminal mode—used to guide an interceptor to the descending threat missile.
	 Long Range Discrimination Radar (LRDR)	A stationary, land-based, S-band radar that tracks incoming missiles for GMD and improves discrimination between the warhead-carrying vehicle and the decoys and other non-lethal objects.
	 Sea-Based X-Band Radar (SBX)	A mobile, ocean-going capable of being positioned across the globe to track missile threats. SBX primarily supports GMD missions and missile defense flight testing.
	 Upgraded Early Warning Radar	A solid-state, phased-array, long-range radar that detects and provides critical early warning of sea-launched or intercontinental threat missiles. There are five locations: Alaska, California, Greenland, Massachusetts, and United Kingdom.
	 Targets and Countermeasures[a]	A variety of short-, medium-, intermediate-, and intercontinental-range targets to represent threats during missile defense flight testing. The target ranges in kilometers are: short (less than 1,000), medium (1,000-3,000), intermediate (3,000-5,500), and intercontinental (greater than 5,500).
	 Terminal High Altitude Area Defense (THAAD)	A mobile, ground-based system organized as a battery that consists of interceptors, launchers, a radar, and fire control and communications to defend against short-, medium-, and limited intermediate-range threat missiles.

Source: GMD presentation of Missile Defense Agency data. | GAO-22-105075

Source: (GAO-22-105075 from Presentation of Missile Defense Agency Data)

Anti-Satellite Weapons (ASAT) present another complex problem for modeling and simulations as their targets orbit at approximately 28,000 km/h in LEO relative to an observer on Earth (National Air and Space Museum, 2017). Although a satellite in LEO travels at the upper end of the high hypersonic regime (Mach 23), orbits are predictable, unlike the flight trajectories of HGVs and HCMs. ASATs come in various weapon platforms, ranging from missiles meant to destroy satellites to lasers and jammers that disrupt them physically. The US built the first ASAT, an air-launched ballistic missile named Blue Orion, in response to the Soviet Union's launch of Sputnik in 1957 (Blatt, 2020). Over the next 30 years, Cold War competition brought the Soviet co-orbital ASATs that attempted to synchronize their orbits with target satellites before detonating, as well as the US ASM-135, which used a hit-to-kill method exploiting kinetic force alone. The

Reagan administration first evaluated the ASM-135 in 1985, demonstrating its capability to destroy an actual satellite in orbit (Blatt, 2020). Since the first successful ASAT tests, China, India, and Russia have researched and expanded their capabilities. Each have recently demonstrated that these weapons remain a threat in the space domain. On January 11th, 2007, China destroyed one of its weather satellites with a modified ballistic missile that created over 3,000 trackable pieces of debris, the largest ever debris field generated by an ASAT (Hadley, 2023). India performed a more carefully planned test on March 27th, 2019, using the Prithvi Delivery Vehicle Mark-II (PDV MK-II) to destroy their own Microsat-R satellite (launched on January 24th, 2019, specifically for this test) in a sun-synchronous orbit at approximately 282 km above the Earth. India's test only produced about 400 fragments of space debris, most of which would decay naturally in the weeks and months following the test (Tellis, 2019). On November 15th, 2021, Russia used the Nudol PL-19 (See Figure 11-20) anti-ballistic missile interceptor as an ASAT to destroy its own Cosmos 1408 satellite approximately 500 km above the Earth, creating about 1,500 pieces of trackable debris in orbit. The debris from both the Chinese and Russian events still poses a direct threat to astronauts on the International Space Station, who must routinely maneuver their vehicle in orbit to avoid debris and will for many years to come. In the wake of the ongoing Russo-Ukrainian War, Russia has publicly noted the threat of Western satellites aiding Ukraine, such as the Starlink constellation, and has threatened action against US assets in space (Bugos, 2021). Unlike other types of weapon tests conducted on Earth or inside the atmosphere, debris created in space from ASATs is technically challenging to remove and, currently, only occurs through natural degradation. Technical demonstrations such as Japan's End-of-Life Services by Astroscale Demonstration (ELSA-d) and the ongoing Swiss ClearSpace debris-removing spacecraft planned for launch in 2025 are working towards orbital debris removal capabilities, but are only nascent compared to the scale of the problem (David, 2021) (Skibba, 2021) (Kim, 2021). Although ASATs are not the only cause of space debris, they deliberately induce havoc and could pose an enduring problem through a theoretical phenomenon known as the Kessler Syndrome. In this theory, cascading debris perpetually creates more space junk through subsequent collisions to form debris belts that make orbits unusable (Smith, 2022). The use of ASATs and the corresponding requirement to simulate their effects across all objects orbiting in space is a more complex problem, requiring more advanced models and simulations than any previous contextual example in this chapter. As of this chapter's writing, China, India, Russia, and the US are the only nations that have conducted an ASAT test. The US is the only of those four who self-imposed a moratorium on testing future direct-ascent ASAT missile systems (Panda & Silverstein, 2022) (Arms Control Association, 2022).

Figure 11-20: The Nudol PL-19 Anti-Ballistic Missile Interceptor

Source: (Arms Control Association | Credit: Russian Ministry of Defense)

Holistically, China and Russia have expanded their total missile, air defense, and space arsenals to incorporate evolving technology described earlier in this chapter as a component of their anti-access area denial networks. China and Russia combine ballistic, cruise, and hypersonic missile technology with survivable and mobile delivery mechanisms that can launch them from the air, land, and sea. The combination of their total missile forces dispersed in orders of battle presents a complex problem for any future war with the ability to threaten any safe haven on Earth (CSIS Missile Defense Project, 2021) (Missile Defense Advocacy Alliance, 2023). See Figures 11-21 and 11-22 for Chinese missile capabilities and Figure 11-23 for Russian land-based missile capabilities.

Figure 11-21: China's Ballistic & Cruise Missile Capabilities

Source: (CSIS Missile Defense Project)

Figure 11-22: China's Regional Missile Threats

Source: (CSIS Missile Defense Project)

Figure 11-23: Russia's Land-Based Missile Capabilities

Source: (CSIS Missile Defense Project)

MODELING AND SIMULATION IN DOCTRINE

Strategy and wargames have existed for thousands of years, with the Chinese board game "go" dating back as early as 2356 BCE (The Editors of Encyclopedia Britannica, n.d.). However, recent history suggests that the earliest adaptations of modern wargaming techniques originated from the Prussians, who were, at the time, trying to overcome Napoleon's advantages. In 1811, Herr von Reisswitz, Prussian War Counselor, invented a wargame that included a terrain table, computations for attrition, technical factors such as range and terrain, and even the issue of chance, which had not previously been used. General Helmuth von Moltke continued the practice while in competition with France once he became Chief of Staff of the Prussian Army (Caffrey, 2000). Wargaming captured what a model-based simulation could not at the time, but that would soon change with additional technology and complexity on the 20th and 21st-century battlefields.

The US Army adopted its current decision methodology, aptly named the Military Decision-Making Process (MDMP), in 1997 with the publication of Field Manual (FM) 101-5, *Staff Organization and Operations*. MDMP created a single decision-making model from the previous deliberate, combat, and quick

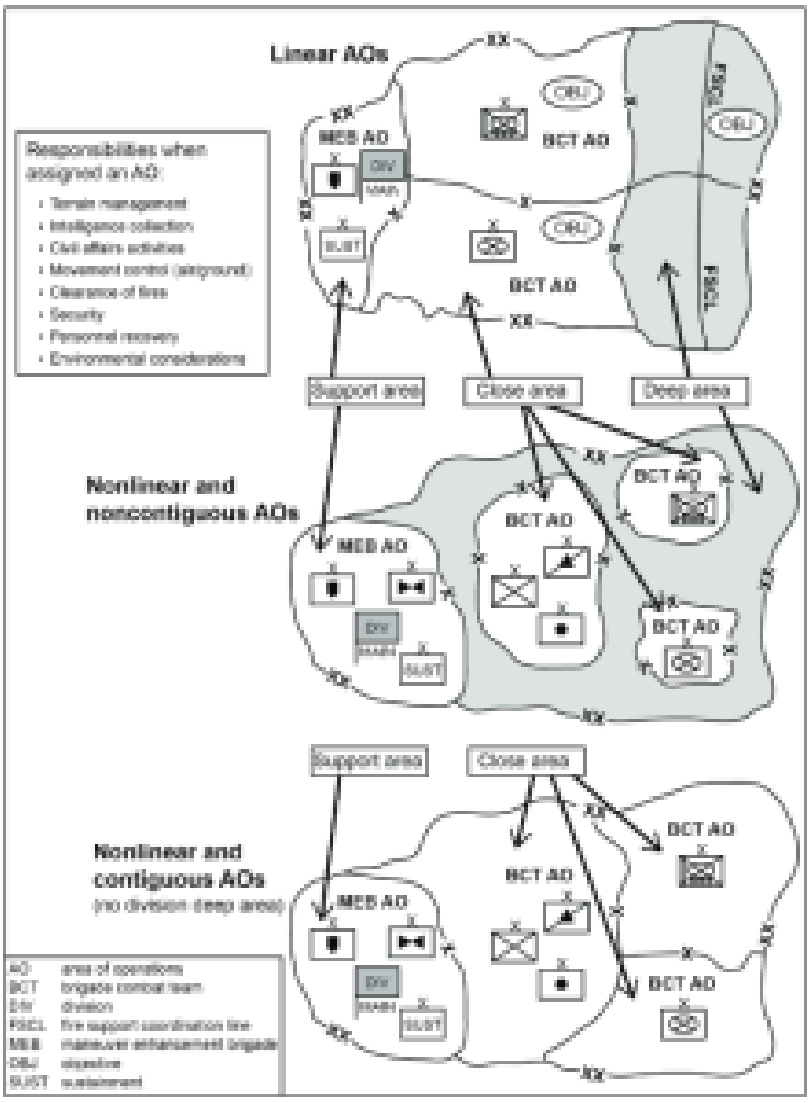
models used in the outdated Tactical Decision-Making Process (TDMP). The basic steps in MDMP include 1. Receipt of Mission, 2. Mission Analysis, 3. Course of Action Development, 4. Course of Action Analysis (Wargaming), 5. Course of Action Comparison, 6. Course of Action Approval, and 7. Orders Production (Wampler, Centric, & Salter, 1998). MDMP remains the procedural decision-making tool for tactical-level US Army staff and requires at least a basic application of wargaming to validate that any given course of action meets the criteria of being feasible, acceptable, and suitable. In other words, wargaming validates that the actions a given organization is about to take will achieve the end state intended in an order. Since the 1800s, models, simulations, and wargames have also changed with new operational concepts, especially complicated by adding joint concepts and multiple domains.

US joint warfighting concepts that acknowledged a need for interoperability between multiple domains date back to the War of 1812, when naval operations on Lake Champlain proved decisive in the Army's land-based campaigns. However, it took 100 years and the aftermath of the Spanish American War for the US military to establish a joint board composed of military leaders in multiple services, including the Army and Navy. Finally, at the end of World War II, the National Security Act of 1947 formally established the Joint Chiefs of Staff, which set conditions for many of the joint concepts and doctrine used today for warfighting (Joint Chiefs of Staff, n.d.).

Over the past 50 years, the US Army underwent five major overhauls in operational concepts, each adapting to the most significant national security challenges of its time. The US Army introduced Active Defense in 1976 on the heels of the Vietnam War as the US shifted its focus to Europe and the threat posed by the Soviet Union. Active Defense echoed more traditional concepts of attrition and terrain-focused warfare forms, remaining separate from the air and maritime operational concepts. As commander of Training and Doctrine Command, General Donn Starry noted the shortcomings in Active Defense that could not address Soviet second-echelon forces and emphasized the need for early interdiction. To tackle the problems with a flexible response to the Soviet Union's extreme numerical advantage in combat power, the US Army adopted AirLand Battle in 1982. AirLand Battle acknowledged the three-dimensional nature of war, with the land and air warfighting domains as inseparable, capturing the impact of technological advances in modern battles and the fast tempo associated with future wars (Skinner, 1988).

After Desert Storm, the US Army implemented Full Spectrum Operations (FSO) in 2001 and Unified Land Operations (ULO) in 2011 (Granai, 2015) (See Figure 11-24 for a graphic depiction of the ULO operational framework). Both operational concepts incorporated offense, defense, and stability, but they viewed warfighting domains differently than AirLand Battle. Although Space Command was first introduced in 1985, FSO was the first Army operational concept to characterize battlespaces in the air, land, sea, and space domains (Headquarters Department of the Army, 2001) (Lopez, 2019). ULO also acknowledged the need for Army forces to execute operations across multiple domains, including space, but also added cyberspace as a domain (Headquarters Department of the Army, 2011).

Figure 11-24: Unified Land Operations Example Deep-Close Security Operational Framework



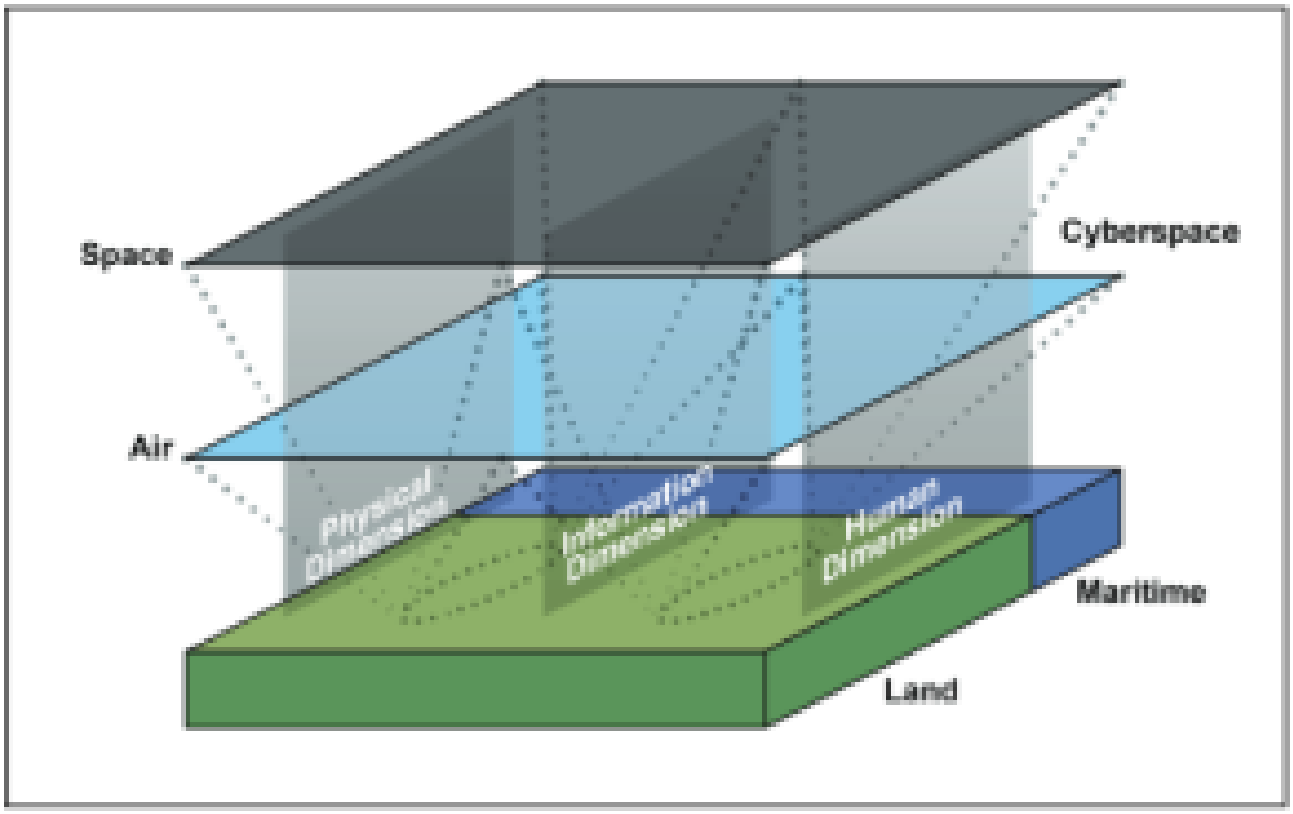
Source: (ADRP 3-0, 2012)

Before discussing Multi-Domain Operations, it is important to note three significant structural and policy changes that directly impact the US interpretation of actions in the space domain and how combat power can be applied. In 2018, President Trump published a National Space Strategy that recognized space as a warfighting domain (Fact Sheets: President Donald J. Trump is Unveiling an America First National Space Strategy, 2018). Many previous administrations acknowledged the need to protect US national security in and from the space domain, but never had a national strategy acknowledged space as a warfighting domain. In 2019, US Space Command was formally re-established, this time as a functional unified combatant command (Lopez, 2019) (Title 10 USC Ch 6: Combatant Commands, n.d.). Finally, the US Space Force was established in 2019 as a service in the US military to organize, train, and equip Guardians (US Space Force, n.d.). Each

of these central policy and organizational changes acknowledges the growing criticality of operations in outer space and the threats posed by near-peer competitors such as China and Russia noted earlier in this chapter.

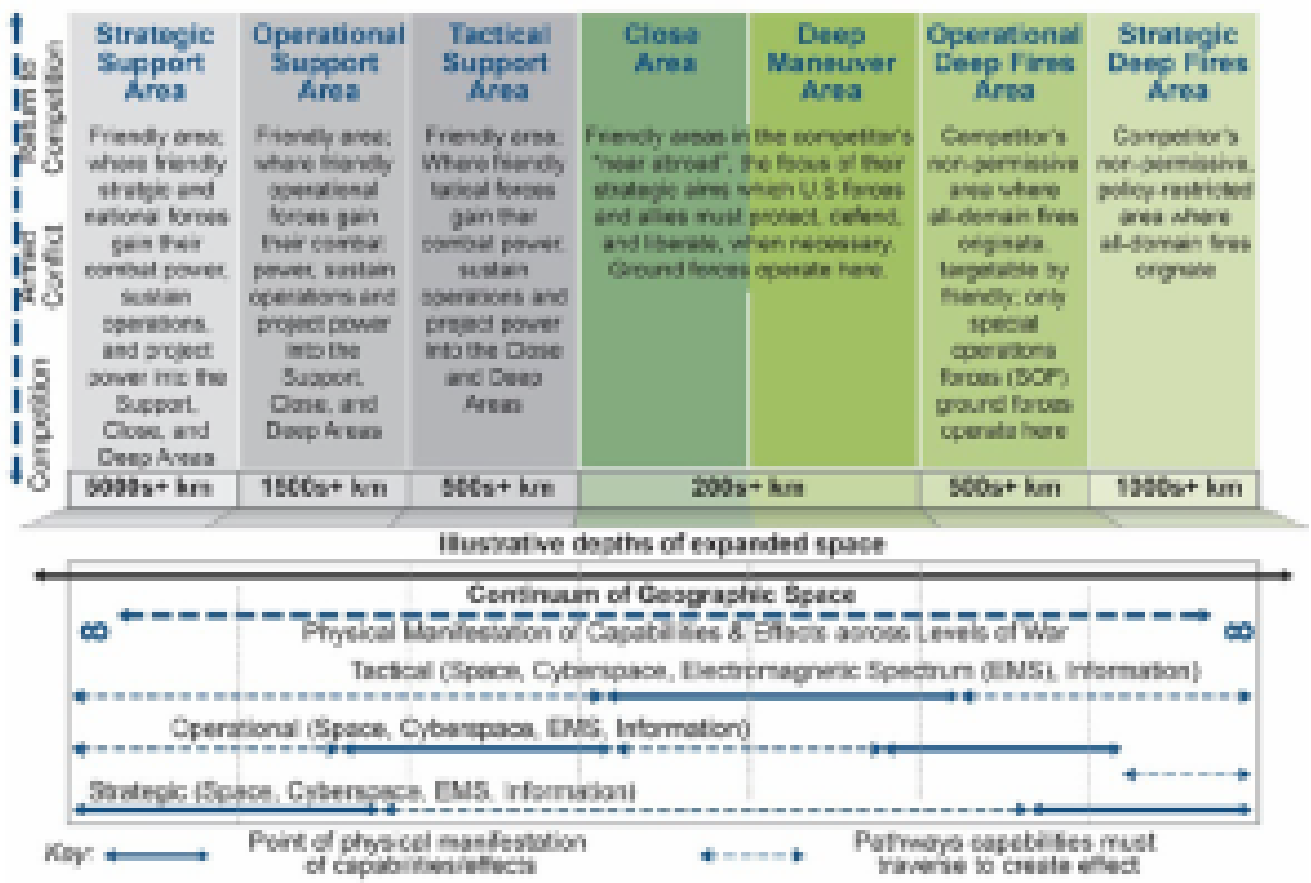
The US Army's newest operational concept was implemented in 2022 and is now called Multi-Domain Operations (MDO). MDO acknowledges the existence of land, maritime, air, space, and cyberspace and emphasizes Army operations spanning the physical, information, and human dimensions in each of the five domains (See Figure 11-25). MDO also expanded the deep area into the extended deep area, including the operational and strategic deep fires areas depicted in Figures 11-26 and 11-27 (Headquarters Department of the Army, 2022). In practice, MDO elevated the US Army's primary unit of action from the Brigade to the Division level (See Figures 11-28 and 11-29 for the MDO operational framework and roles of each echelon) and now accounts for the need to provide effects convergence across the spectrum in support of unified action with the joint force. Figures 11-30 to 11-33 graphically depict the concept of effects convergence within the MDO operational framework while Figures 11-34 and 11-35 showcase notional offense and defense scenarios.

Figure 11-25: Domains and Dimensions of an Operational Environment



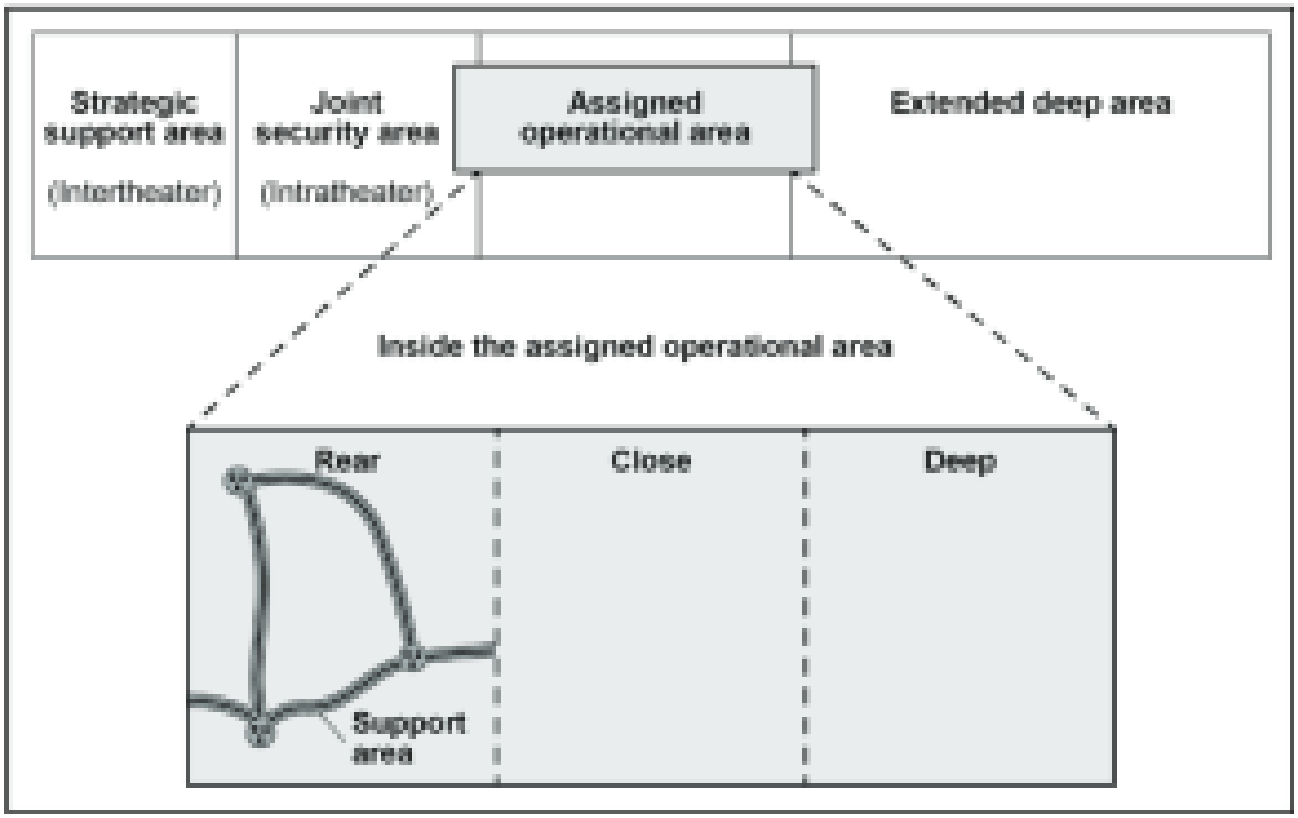
Source: (FM 3-0, 2022)

Figure 11-26: The Multi-Domain Operations Framework



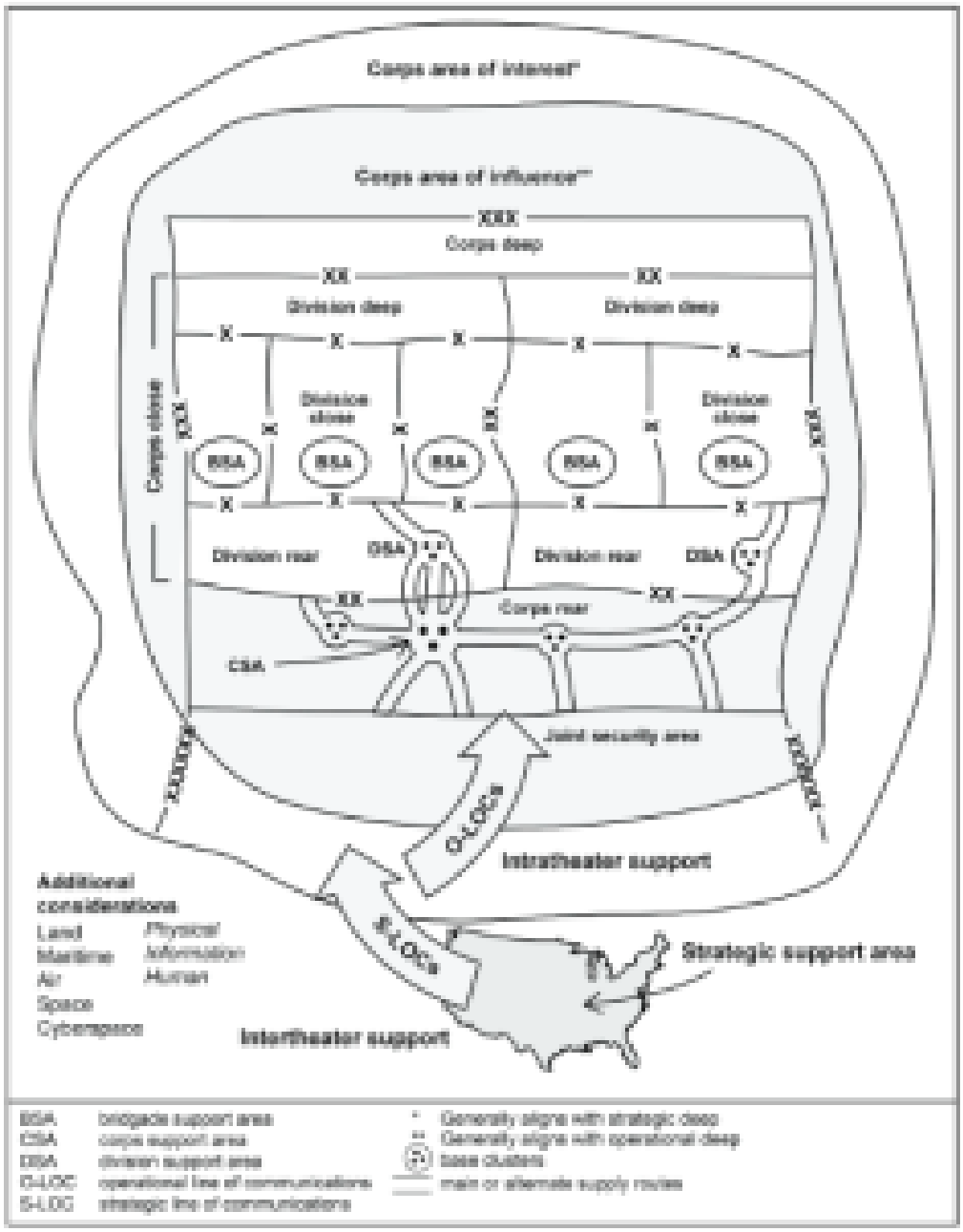
Source: (TP 525-3-1)

Figure 11-27: The Operational Framework in the Context of the Strategic Framework



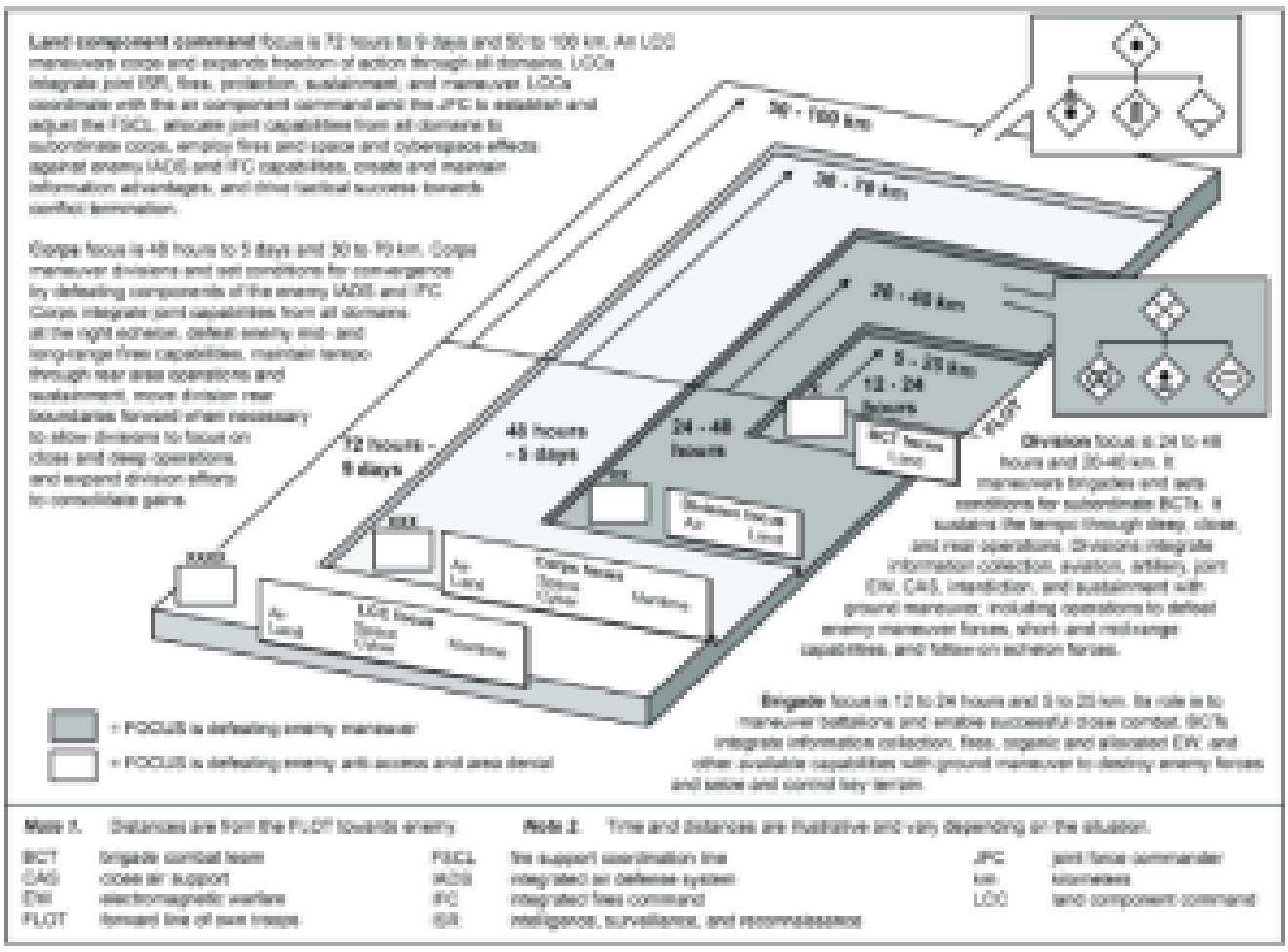
Source: (FM 3-0)

11-28: Notional Corps Deep, Close, and Rear Areas with Contiguous Divisions



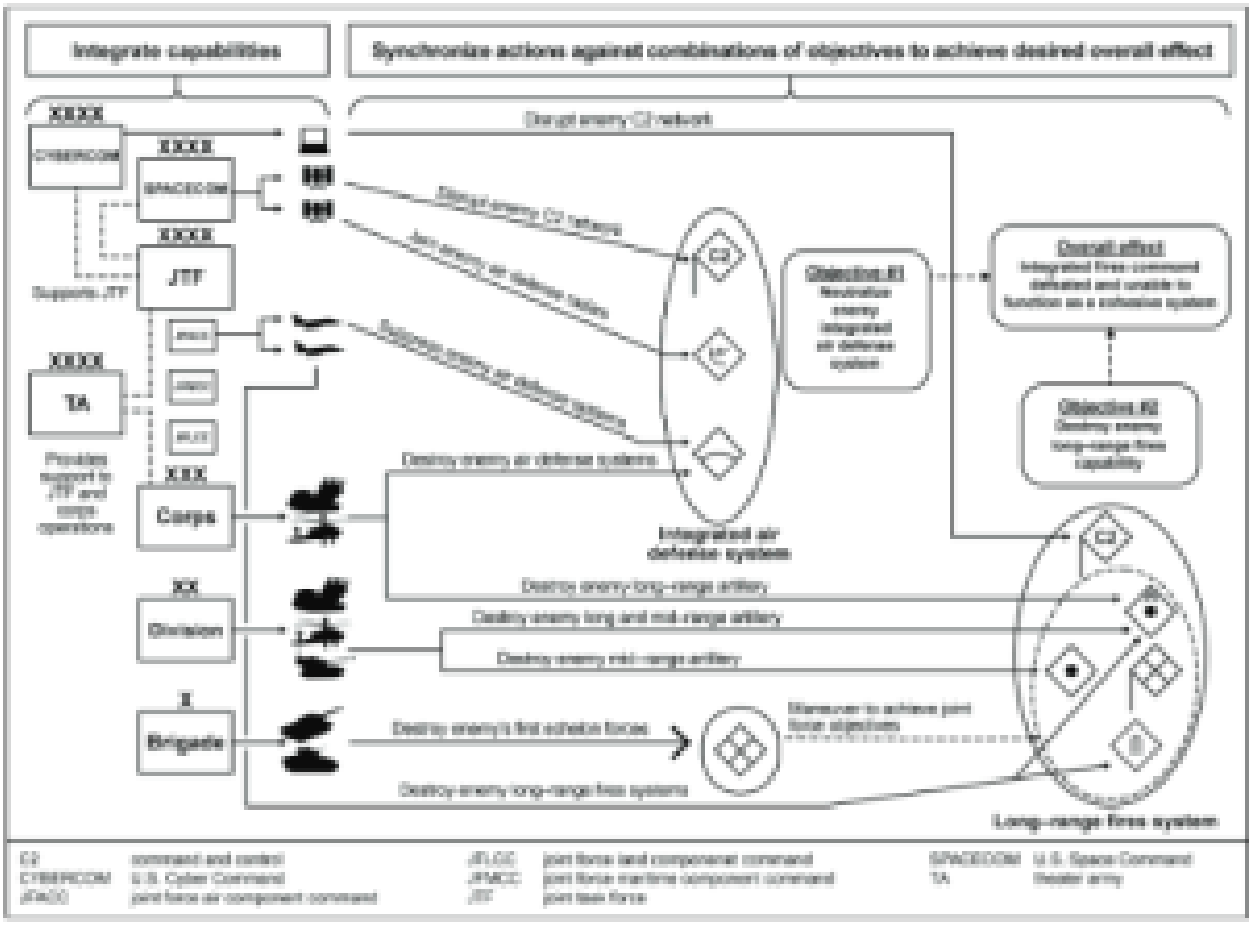
Source: (FM 3-0, 2022)

Figure 11-29: Notional Roles and Responsibilities in Terms of Time, Space, and Purpose at Different Echelons



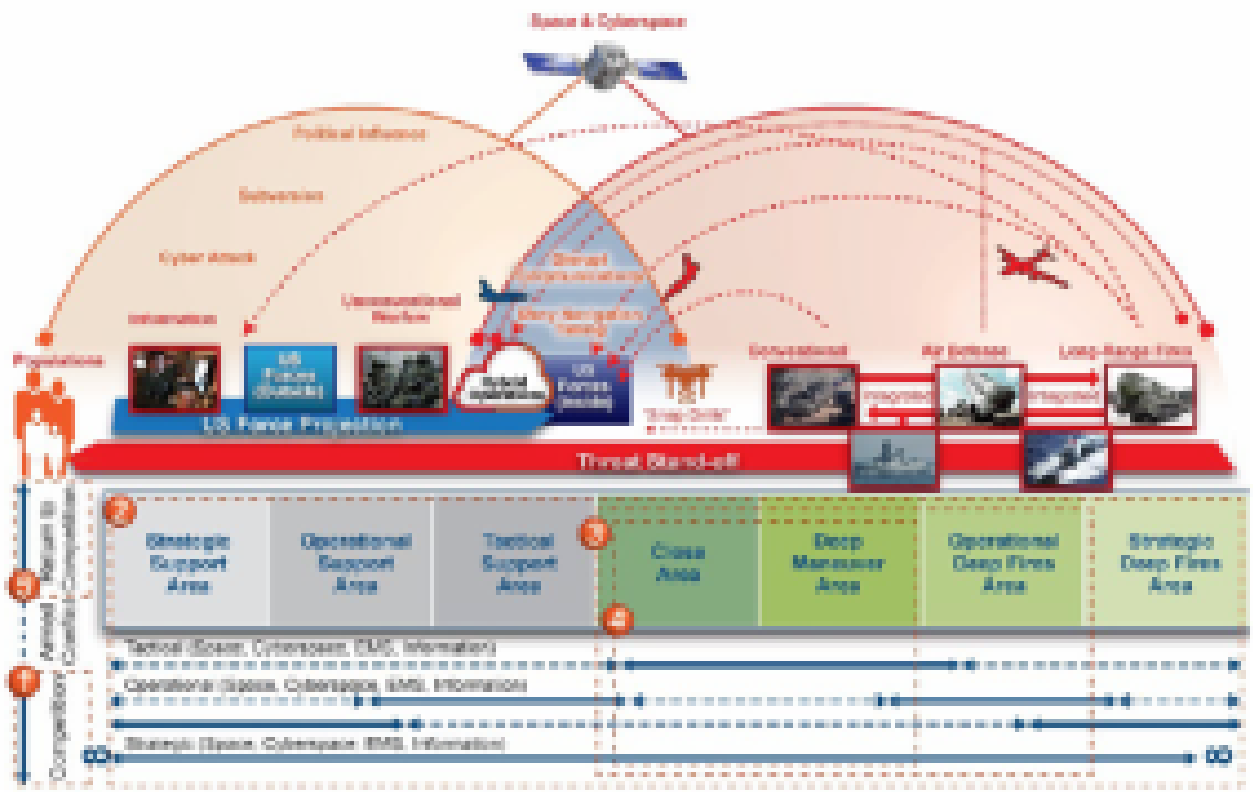
Source: (FM 3-0, 2022)

Figure 11-30: Convergence in Multi-Domain Operations



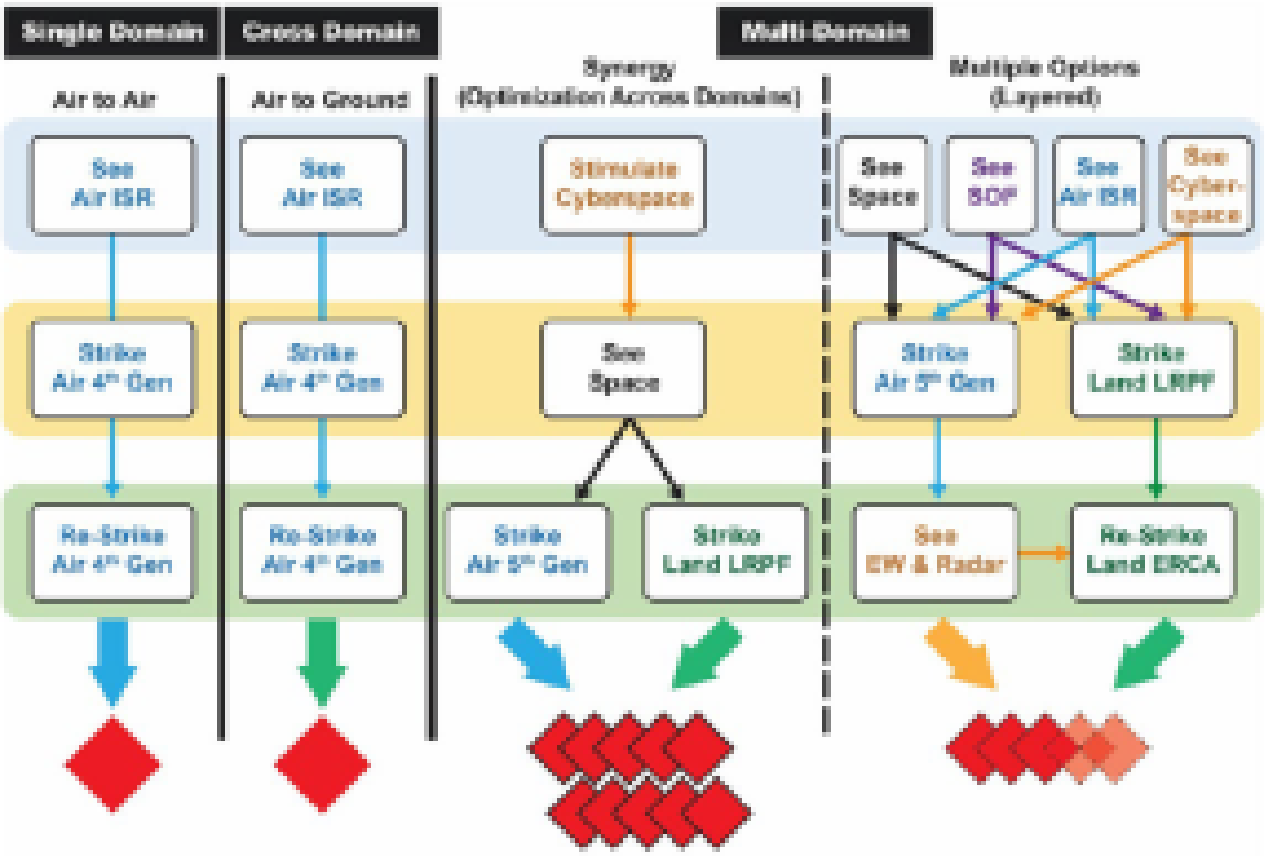
Source: (FM 3-0, 2022)

Figure 11-31: China and Russia in Competition and Armed Conflict Problems Superimposed on the MDO Framework



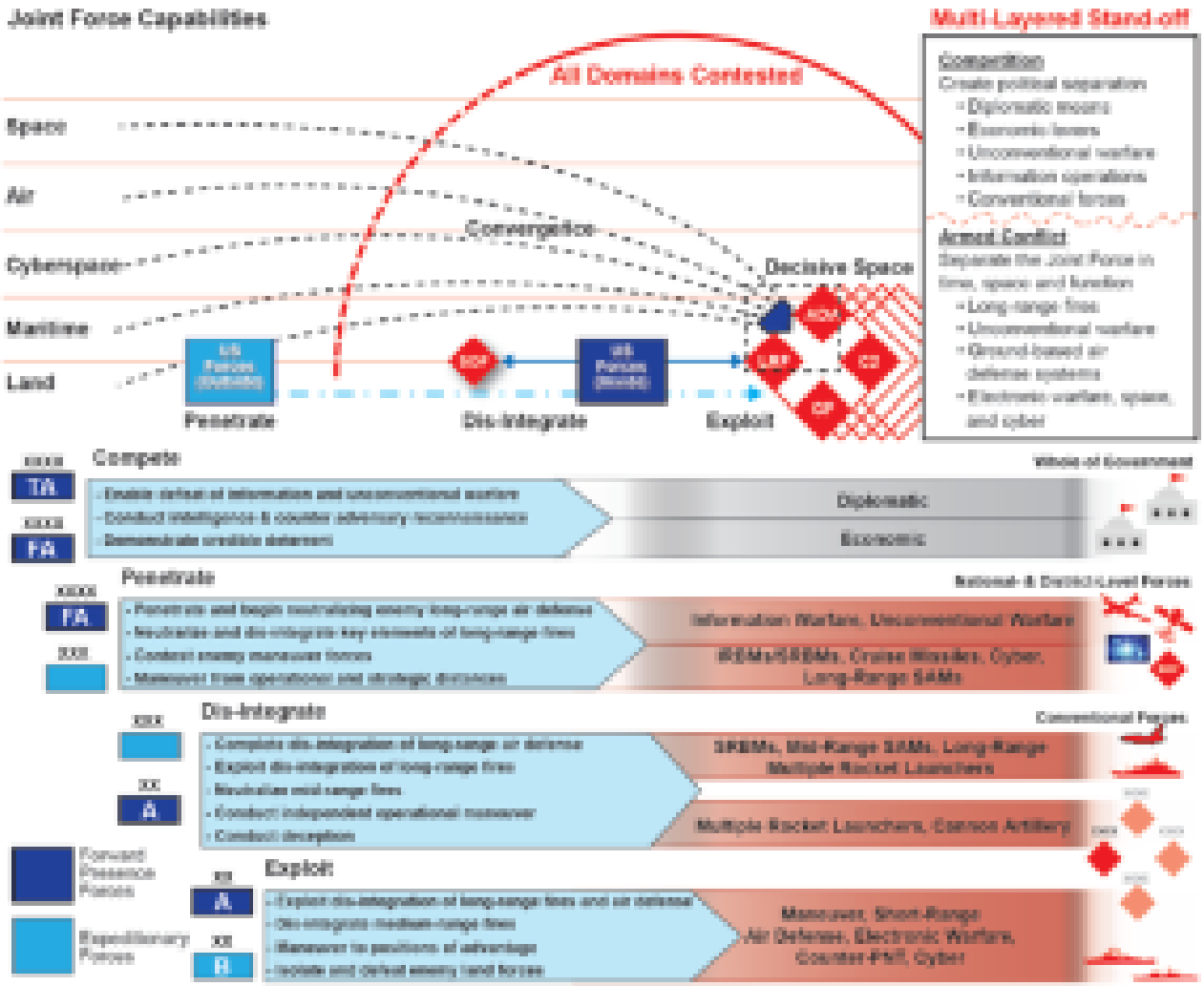
Source: (TP 525-3-1)

Figure 11-32: Convergence Generating Cross-Domain Synergy and Layered Options



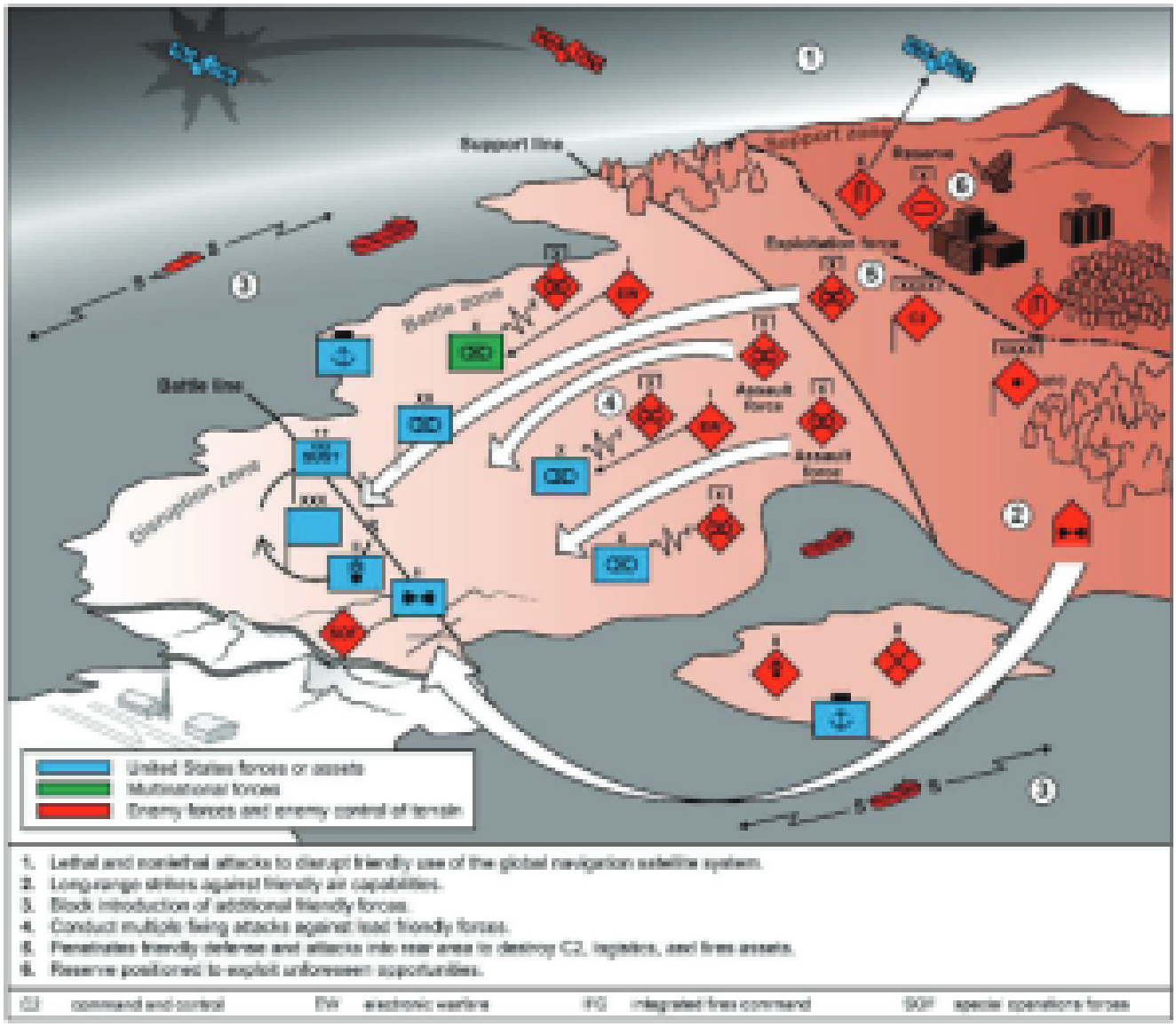
Source: (TP 525-3-1)

Figure 11-33: MDO Solutions



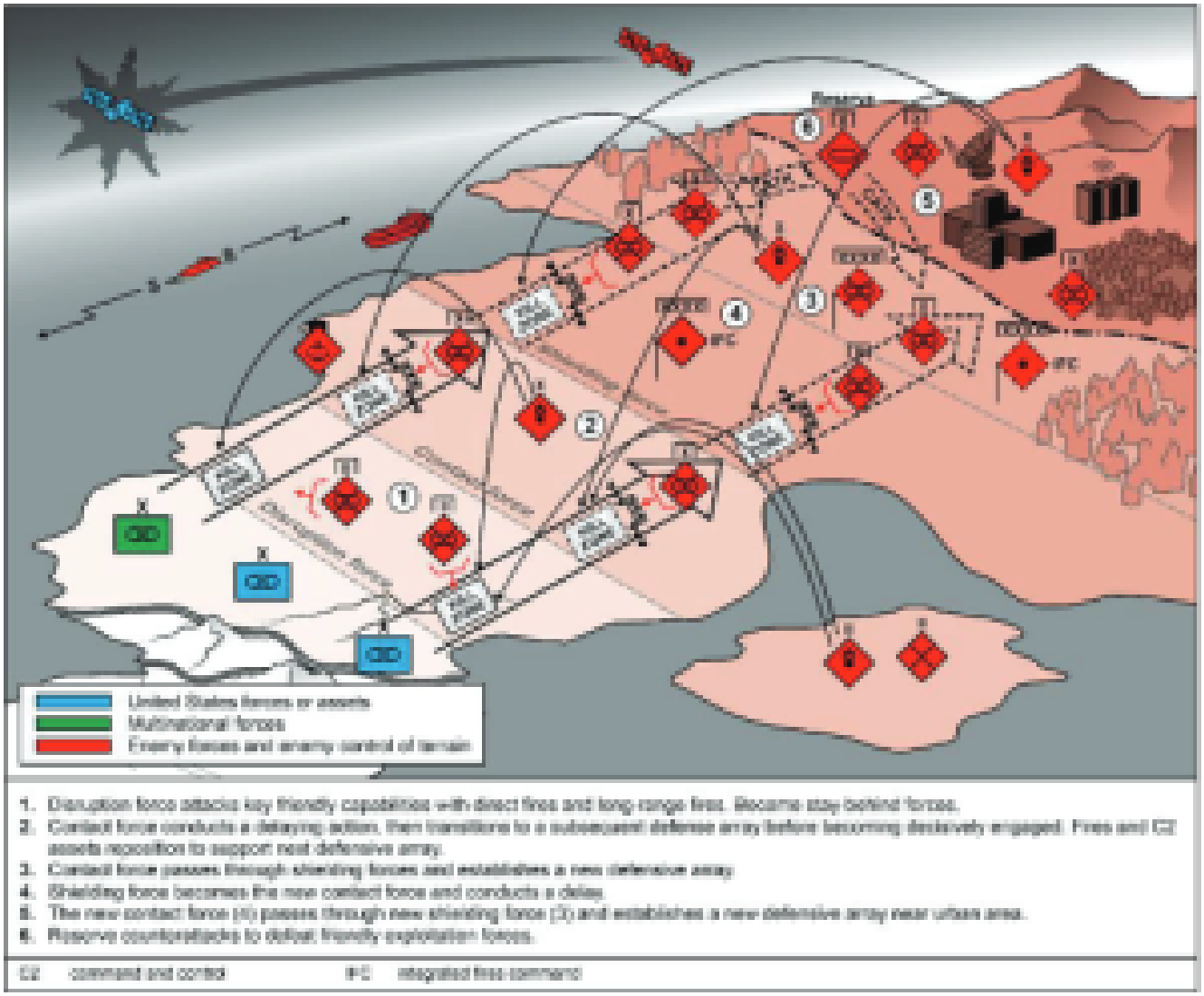
Source: (TP 525-3-1)

Figure 11-34: Notional Enemy Offensive Operation



Source: (FM 3-0, 2022)

Figure 11-35: Notional Enemy Maneuver Defense



Source: (FM 3-0, 2022)

Thinking back to MDMP as a decision-making framework, the MDO operational concept now requires Army staff officers to model a variety of threats in all five domains, simulate large-scale combat, and compare the results of multiple courses of action. As a result, the space domain cannot remain solely an operational and strategic concern for military planners. With the publication of the US Army's MDO concept, space modeling and simulations is now a tactical-level responsibility in the wargaming process, requiring a modern solution of toolsets widely proliferated among planners. While sufficient for simulating interactions between ground, air, and maritime order of battle units, the adaptive tabletop wargaming methods may no longer be capable of capturing the complexities of actions in space and cyberspace.

MODELING AND SIMULATION FRAMEWORK

Previously in this chapter, we identified a definition for simulation specific to the Apollo space program use case. Taking a more holistic look at models and simulations across various aerospace use cases, it is helpful to characterize these terms more generally. In a Johns Hopkins APL Technical Digest, James Coolahan defined a model as "a physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process" and simulation as "a method for implementing a model over time" (Coolahan, 2003). Models in a space context may account for a single shuttle, a hypersonic missile, or the totality of satellites orbiting Earth with free-floating debris. Similarly, simulations must account for several situations, from a shuttle launch to large-scale combat operations, showing the progression of hundreds of missiles, electronic warfare effects, aircraft, satellites, etc.

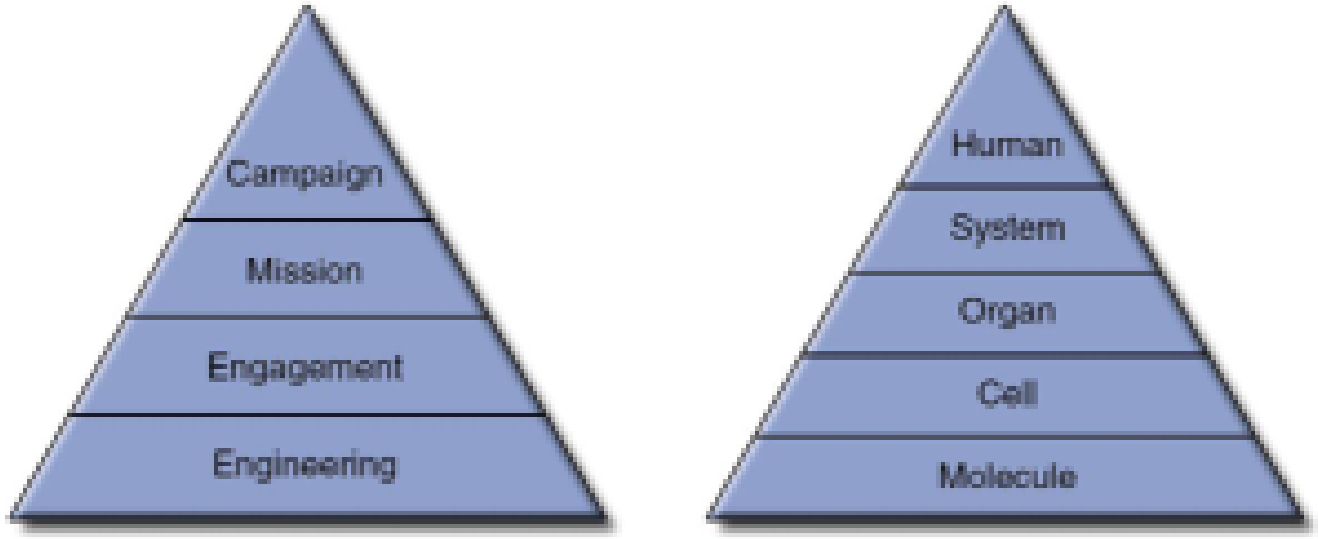
There are multiple ways of categorizing models and simulations, but Coolahan's four viewpoints fit the space use cases described in this chapter. In many cases, models and simulations will have one or more of the following categories and components.

1. Application Domain – Captures a specific problem area within a model or simulation, including space physics, a battlefield's geographic area (potentially in the maritime, air, land, space, and cyber domains), or a transportation network.
2. Resolution Level – Identifies the amount of detail and the extent of aggregation within a given model or simulation. As an example, a satellite may have propulsion, actions of maneuvering surfaces, and power generation aggregated together in a single model at a particular level of resolution (See Figure 11-36 for further examples of military and physiological resolution levels).
3. Role – The function a specific model or simulation is built to accomplish. An example could be to evaluate a hypersonic missile's flight performance, analyze a joint firepower strike against multiple satellites, or train a space crew on their duties in the spacecraft.
4. Technique – The method a given model or simulation uses to accomplish its purpose. Examples include a static display of a lunar vehicle, a dynamic, constructed environment simulating a space launch, or a model of hardware system components interacting.

Figure 11-37 provides a graphic depiction of Coolahan's four viewpoints and additional sample characteristics.

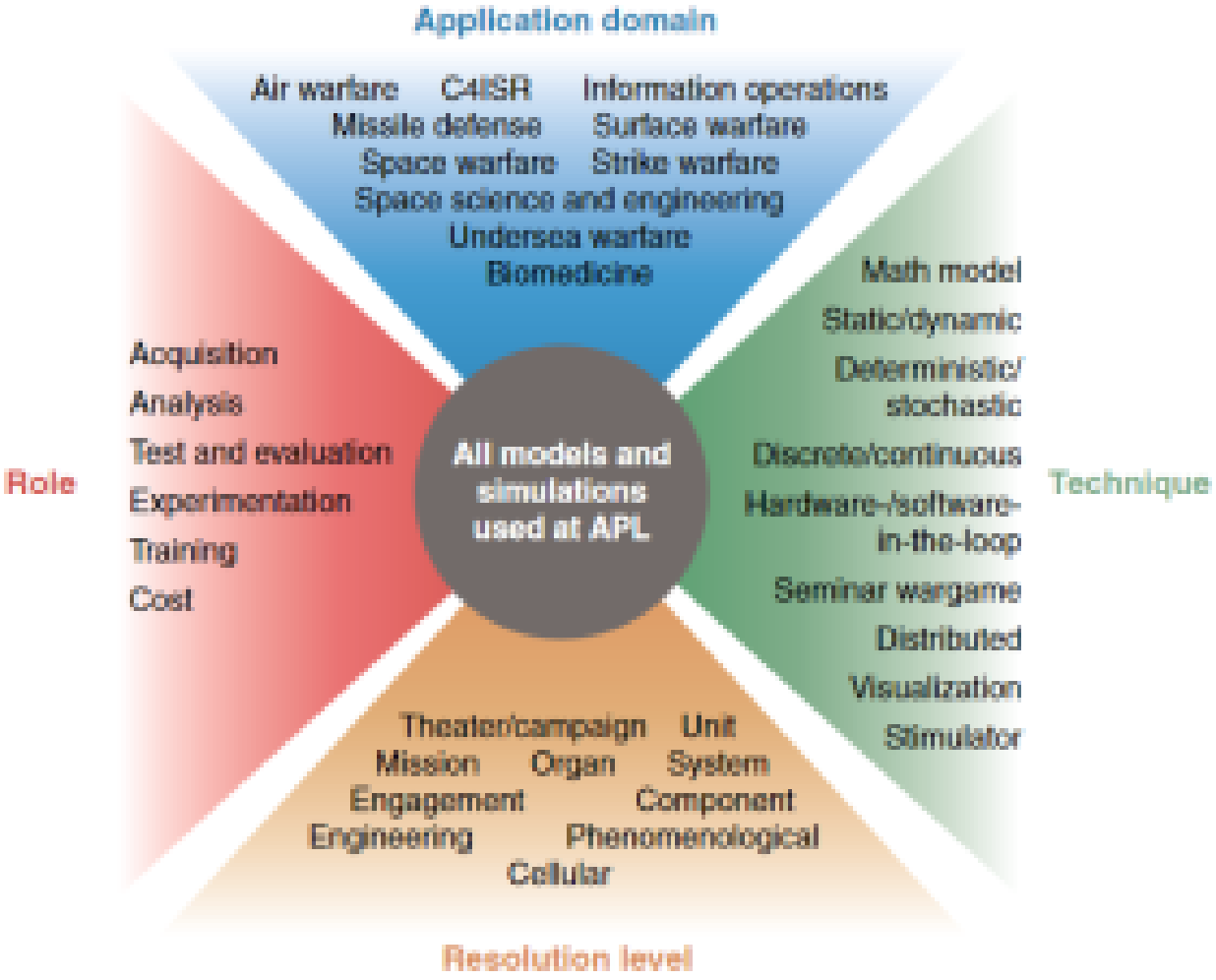
Given the threat context and mass proliferation of space-based capabilities described earlier in this chapter, models and simulations must not be constrained to highly technical users. To be successful, models and simulations must be widely used and accepted within the community of interest they support, have a framework that is effective when applied in practice, be available across a large user base, be affordable to the organizations that need it, and be accessible for users to adopt (West & Birkmire, 2020). Models both improve the chances of success for a mission during execution and reduce the overall costs of capability development.

Figure 11-36: Examples of Modeling and Simulation Resolution Levels: (left) Military Simulations and (right) Physiological Models



Source: (Johns Hopkins APL Technical Digest, Volume 26, Number 4 | Credit: James Coolahan)

Figure 11-37: A Potential Taxonomy for Models and Simulations Used at APL: Four Views and Sample Characteristics



Source: (Johns Hopkins APL Technical Digest, Volume 26, Number 4 | Credit: James Coolahan)

MODELING AND SIMULATION TOOLS

The following list of tools is just a tiny sample of the instruments available for modeling and simulating space effects. Casual gamers may note that there are dozens of realistic space flight simulators on the Steam marketplace as of the publication of this document, many of which are not captured here. DoD employees may also recognize that well-known tools are not included in this list, primarily due to classification and usefulness to an academic audience. There are also customized space simulators, like those developed by NASA for the space shuttle program and SpaceX for commercial purposes, which are proprietary and not publicly available. Nonetheless, this list demonstrates the potential for computer-based modeling today and dozens of use cases for both military and civil purposes.

For an overview of the mechanics (inputs) used to model a spacecraft's trajectory or satellite's orbit, please refer to Chapter 10 (Nichols, et al., 2023).

IMPROVED MANY ON MANY (IMOM)

IMOM is a commonly used modeling and simulation tool developed by the Air Force Electronic Warfare Center (AFEWC). This software's specific purpose is to simulate the routing of an attack aircraft as it penetrates enemy air defense systems, including radars and surface-to-air weapons, providing planners insight into the vulnerability of detection, tracking, and engagement of friendly aircraft along a specific route. Self-protection and stand-off jamming are also critical components of the IMOM simulation. IMOM is customizable to meet user needs and can ingest various classified and unclassified data sets (Ormesher, 1993). Although there are few use cases where IMOM could be used to model activities in the space domain, it provides an example of critical data points to consider in the simulation process for military planners seeking to model aerial flight against a complex enemy air defense (Diebold, 2023).

A combat simulation in IMOM requires a scenario containing an Electronic Order-of-Battle (EOB), terrain mapping, radar, threat, and jammer databases (Ormesher, 1993). The EOB file should provide IMOM with the names and locations of threat radars, weapons, and jammers on Earth's surface, which can then be modified individually or linked to databases of standardized military equipment (Ormesher, 1993). A sample EOB is depicted in Figure 11-38, further identifying radars with the North Atlantic Treaty Organization (NATO) name, Electronic Intelligence Notation (ELNOT), Personal Identification Number (PIN), and type of radar (further described in the radar database portion of this chapter).

Figure 11-38: Sample EOB Listing

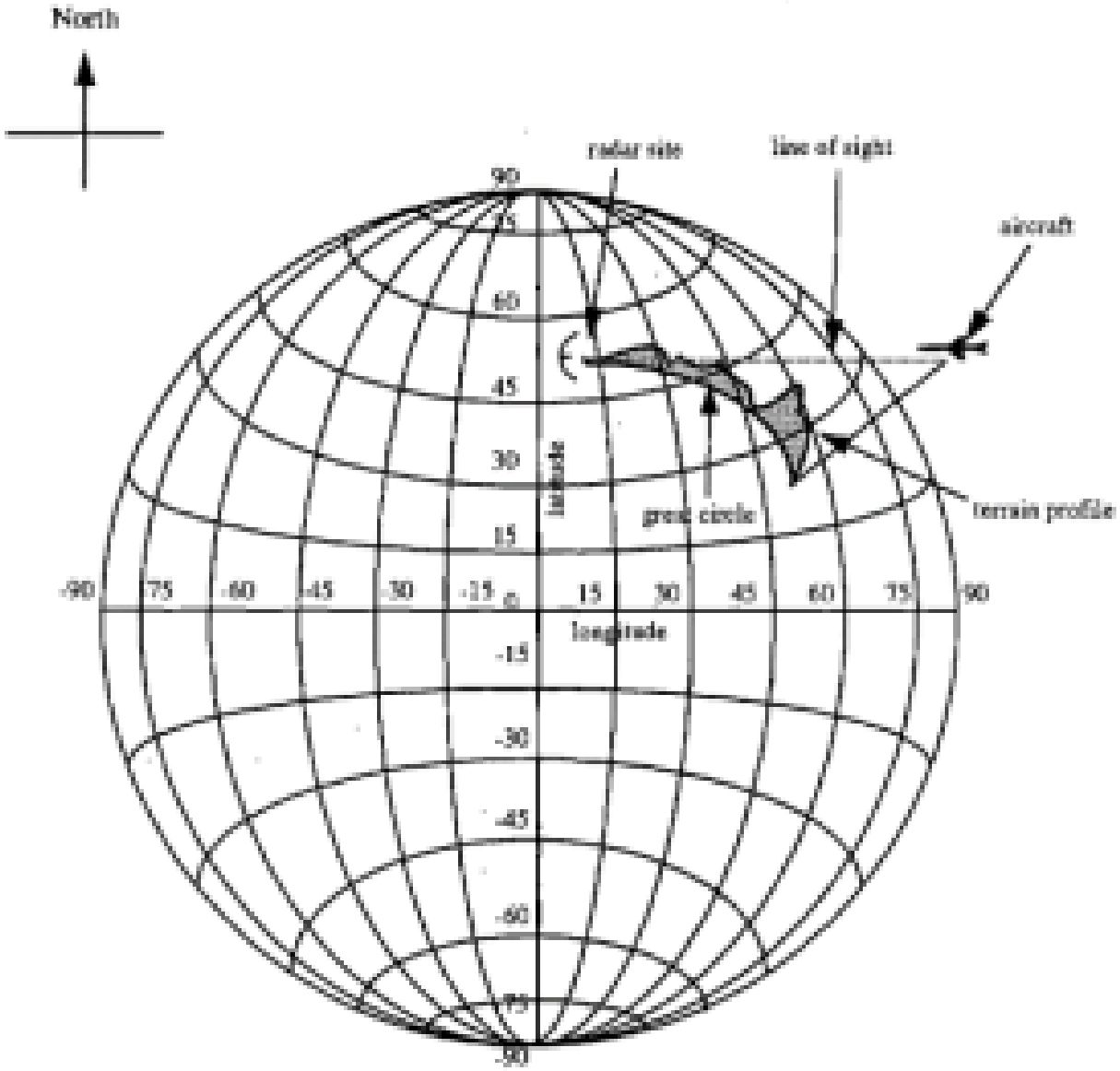
Table 1: Sample EOB listing

Latitude	Longitude	NATO Name	ELNOT	Type	PIN (optional)	Weapon
943000N	705000E	BIGBOY	RAD1	TA	00000	
201000N	1043000E	BIGBOY	RAD1	TA	00000	
140000N	1100000E	TALLBOY	RAD03	HF	00000	
100000N	1100000E	BIGBOY	RAD1	TA	00000	
040000N	1030000E	TALLBOY	RAD03	HF	00000	
150000N	1100000E	FATBOY	RAD02	TT	00000	FATS
123000N	1010000E	FATBOY	RAD02	TT	00000	FATS

Source: (Richard C. Ormesher)

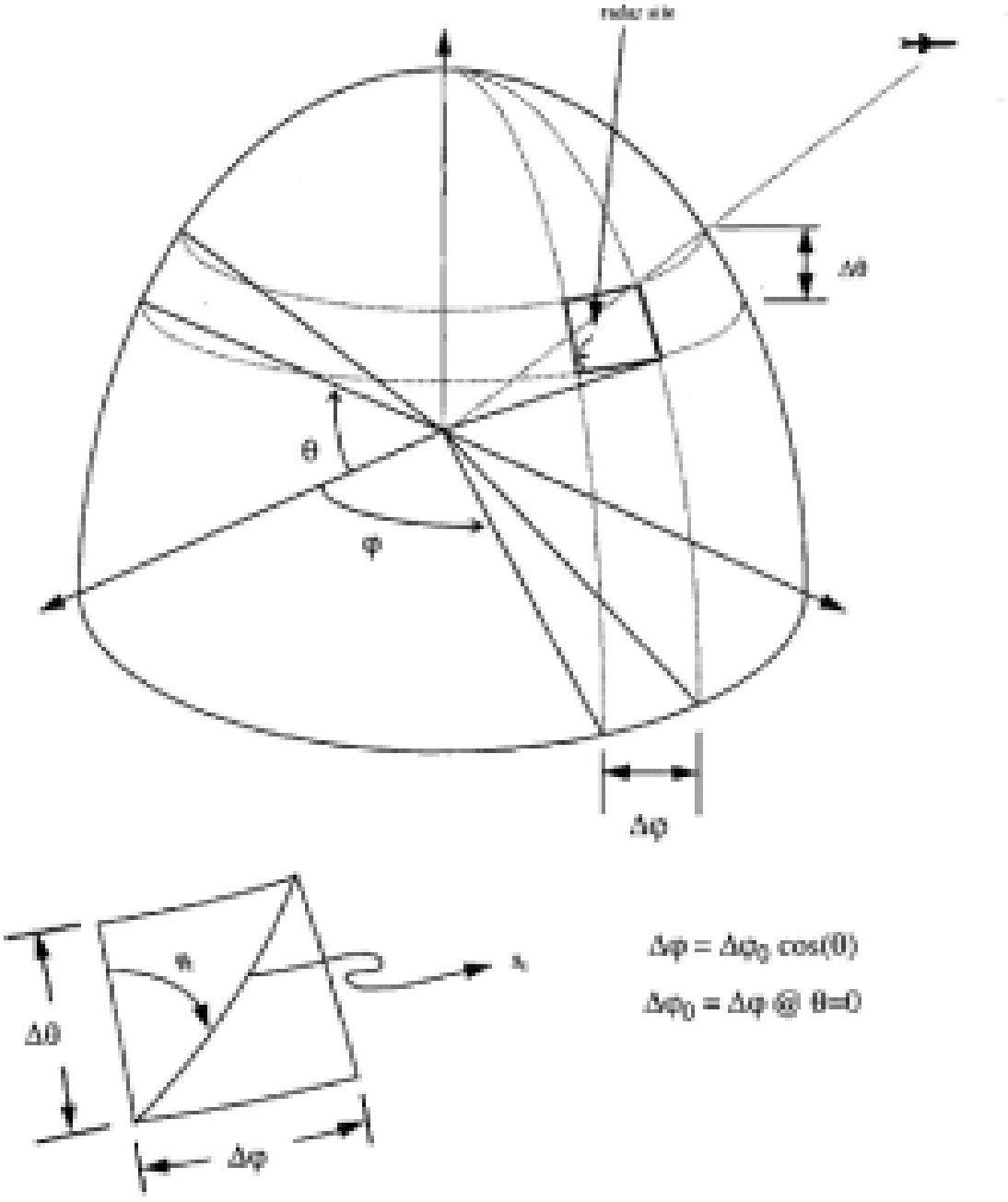
The terrain file ingested into IMOM typically only captures elevation, but the resolution level in the file is essential to consider (Ormesher, 1993). For example, there are three standardized levels of post spacing when using Digital Terrain Elevation Data (DTED). DTED level 0 has a post spacing of 30 arc seconds (~1km between cells), where DTED level 1 has a post spacing of three arc seconds (~100m), and DTED level 2 is at one arc second (~30m) (VTP, n.d.). The higher the DTED level, the more accurate the line-of-sight analysis. However, there is a tradeoff in simulation time, which takes much longer to complete when using more detailed terrain data (higher levels of DTED) given the additional computation required (Diebold, 2023). Figures 11-39 to 11-41 graphically depict how IMOM calculates line of sight from a radar to an aircraft and how terrain data factors into the output (whether a particular radar can see an aircraft).

Figure 11-39: ROUTE Coordinate System Showing Radar, Line of Sight, Aircraft, and Terrain Profile



Source: (Richard C. Ormesher)

Figure 11-40: Ground Distance and Azimuth Direction from Radar to Aircraft



Source: (Richard C. Ormesher)

Figure 11-41: Slant Range and Elevation Angle from Radar to Aircraft

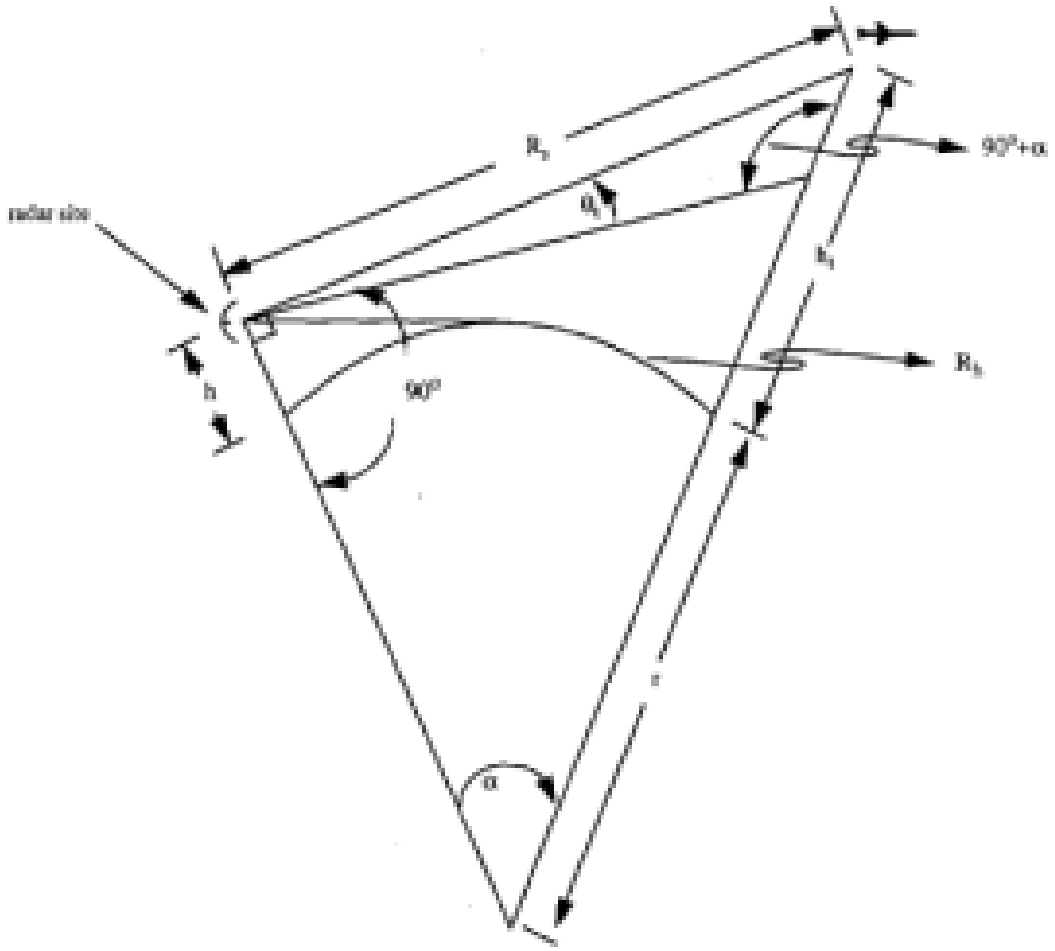
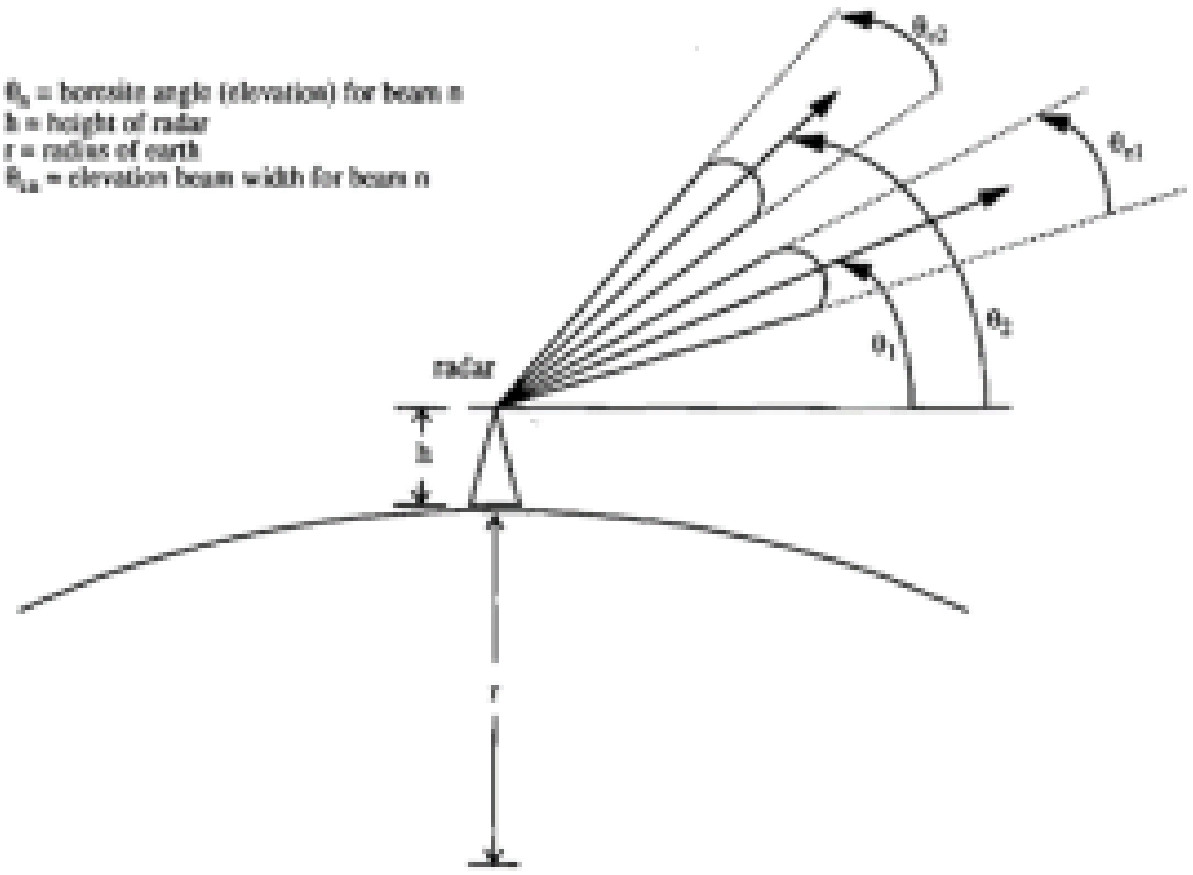


Figure 11. Slant range and elevation angle from radar to aircraft

Source: (Richard C. Ormesher)

The radar database file lists parameters to model each specific enemy radar, including power levels, beam widths, antenna gains, and receiver losses. Radars are also characterized by type, with Early Warning (EW) or Target Acquisition (TA) assumed to have vertical beams scanning horizontally and Fire Control (FC), Target Tracking (TT), and Height Finding (HF) assumed to be non-scanning beams pointed at an aircraft (Ormesher, 1993). Figures 11-42 to 11-43 show how IMOM calculates a radar's beam look angle and range while Figure 11-44 shows how IMOM determines the slant distance from the radar to an aircraft.

Figure 11-42: Diagram Showing Radar Beam Look Angle (in Elevation)



Source: (Richard C. Ormesher)

Figure 11-43: Simple Radar Range Calculation

$$R = \frac{10^{((RCONST + \sigma') \times 0.25/10)}}{1000}$$

Source: (Richard C. Ormesher)

Figure 11-44: Slant Distance from Radar to Aircraft Calculation (Credit: Richard C. Ormesher)

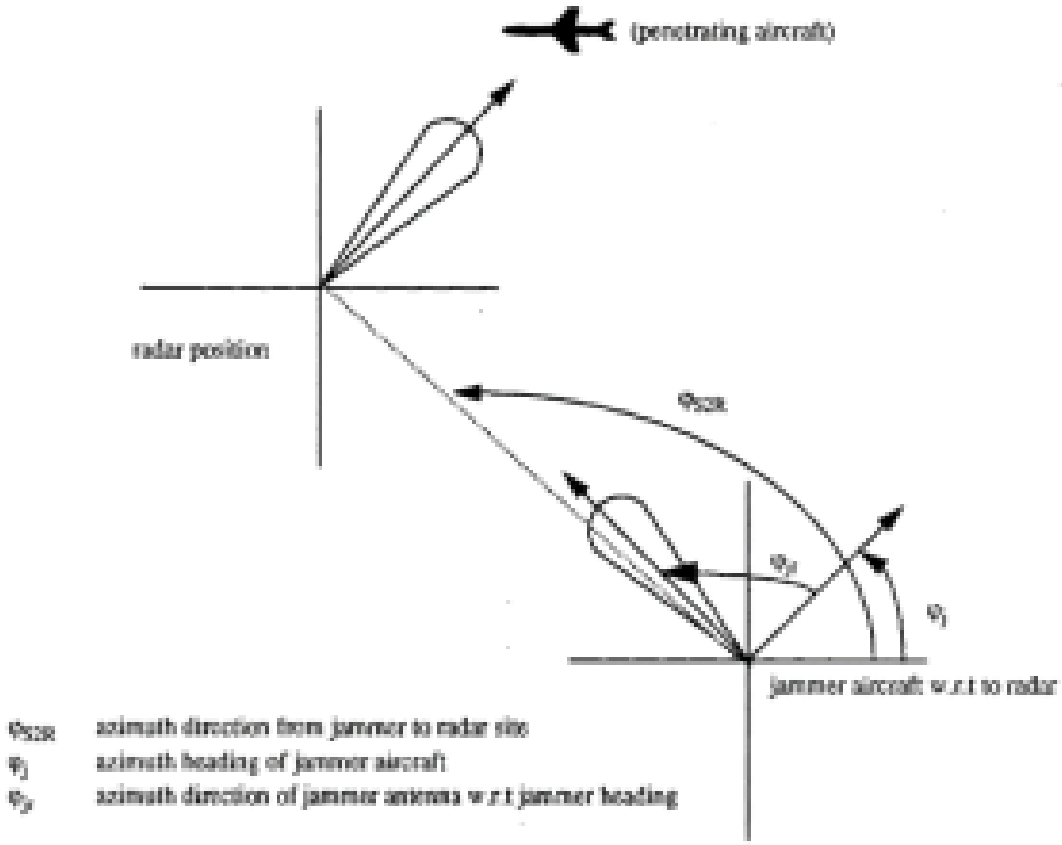
$$ACRNGE = \frac{\sqrt{ACDIST^2 + ALTUDE^2}}{1000}$$

Source: (Richard C. Ormesher)

The threat database file lists parameters linked or unlinked to the performance characteristics of weapon systems associated with radar systems (Ormesher, 1993). The primary attributes of a surface-to-air weapon system are the maximum and minimum engagement altitude and the maximum, minimum, and recommended intercept ranges. Although IMOM does not always incorporate seeker types, munition speeds, and their probability of success against specific airframes based on exposure time, this can be considered for windows of vulnerability after a holistic IMOM analysis (Diebold, 2023).

The jammer file simply contains the specific parameters for modeling standardized jammers and their configurations (Ormesher, 1993). Figure 11-45 graphically shows how IMOM models the geometry of a jammer with respect to a radar and aircraft in the simulation. When performing calculations to determine a jammer's effectiveness, IMOM considers the overlapping frequencies between radar signals and jammer transmitters in addition to geometry.

Figure 11-45: Geometry of Radar, Penetrating Aircraft, and Stand-Off Jammer

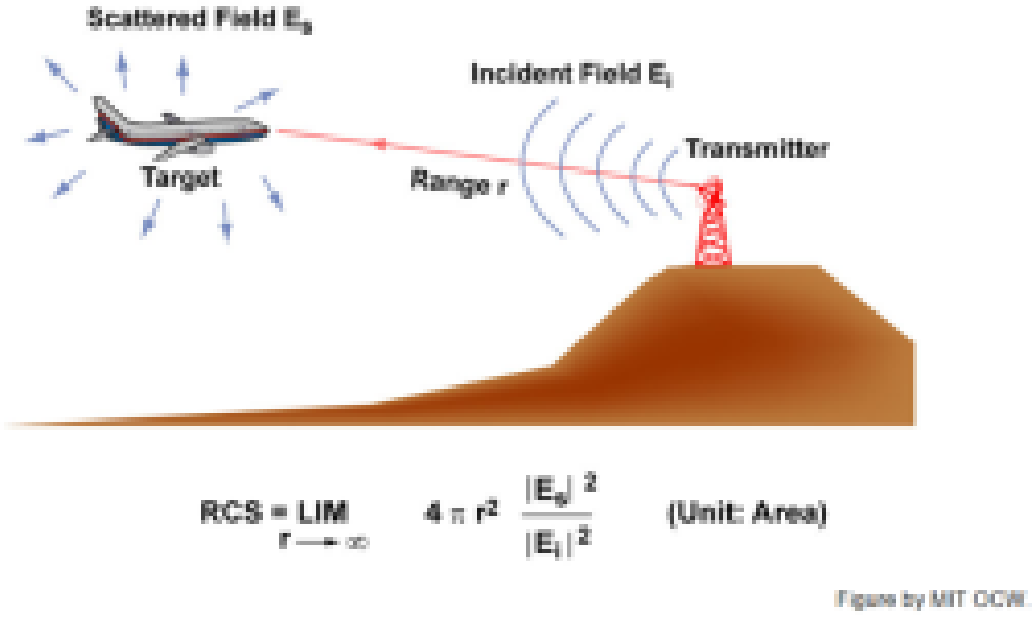


Source: (Richard C. Ormesher)

Beyond the threats and operational environment models, IMOM also models the friendly aircraft and the route it will attempt to fly. When modeling the aircraft, the most important input is the Radar Cross Section (RCS), often measured in decibels (dB) (Diebold, 2023). MIT defines an RCS as the area intercepting that amount of power which, if radiated isotropically, produces the same received power in the radar (See Figure 11-46 for a graphic depiction of RCS). Many factors, including the aircraft's size, shape, orientation, and materials contribute to its RCS (See Figure 11-47), but the three main contributors are structural, propulsion, and avionics (See Figure 11-48) (MIT Lincoln Laboratory, 2018). IMOM can simplify RCS by applying a constant value (usually the highest value across all aircraft or missile orientations), or it can create a 3D pattern for calculations that will account for the look angle of each radar and the aircraft's orientation for detection (Ormesher, 1993). The most critical inputs along the aircraft's route are speed and altitude, which when calculated with position, also allows for orientation to the radar to be factored in (See Figure 11-49 and 11-51). These inputs contribute to how individual radar and weapon systems interpret a friendly aircraft or missile and could impact a threat's ability to see it all together, even if all other variables in IMOM's calculations suggest

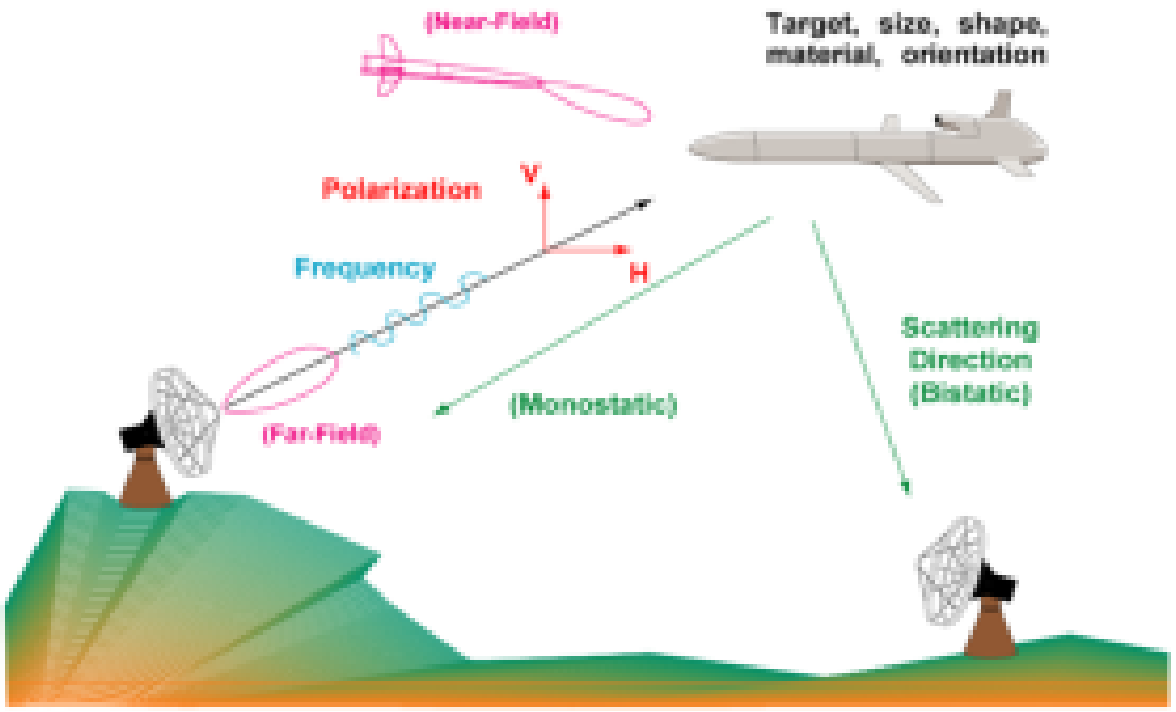
it should be able to. Without external contributing factors (such as a jammer or weather), RCS is the primary variable that friendly forces can influence in a detection decision (See Figure 11-50) (Diebold, 2023).

Figure 11-46: Definition of RCS



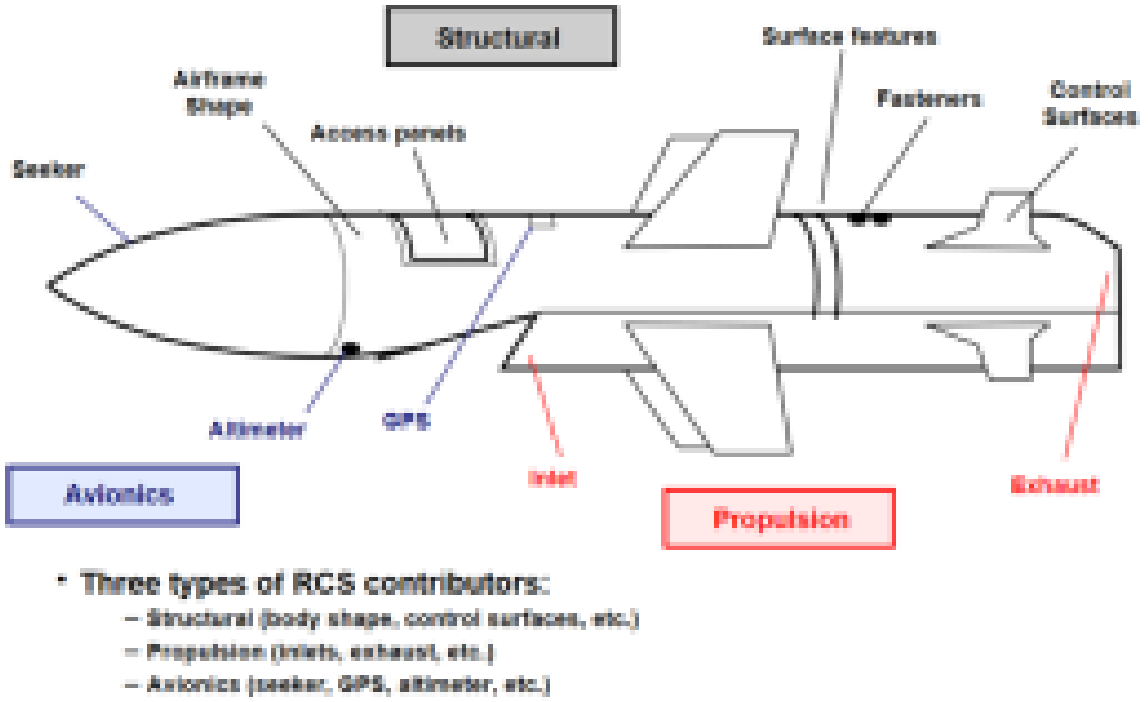
Source: (MIT Lincoln Laboratory)

Figure 11-47: Factors Determining RCS



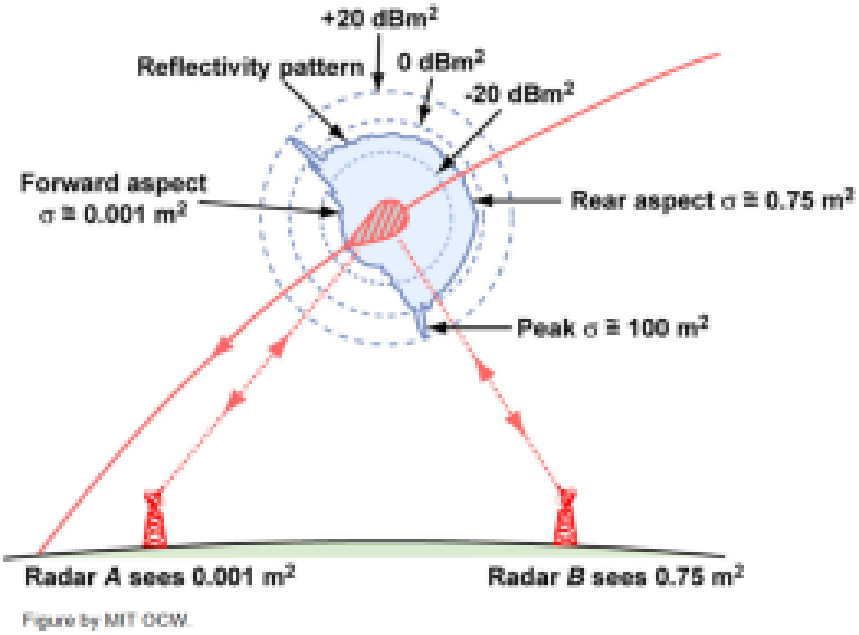
Source: (MIT Lincoln Laboratory)

Figure 11-48: Components of Target RCS



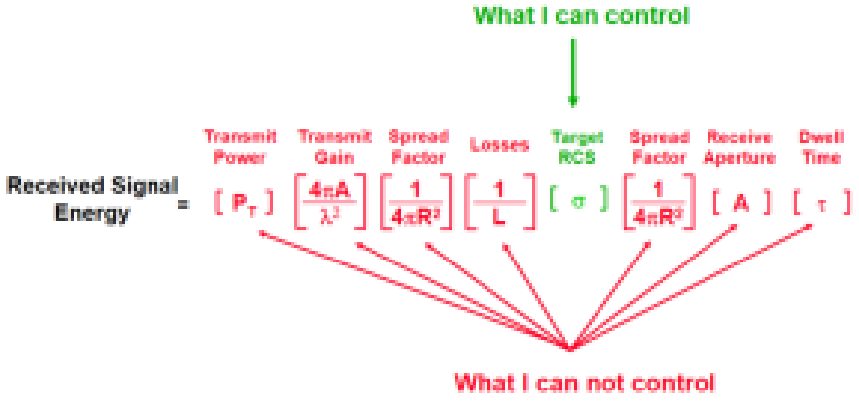
Source: (MIT Lincoln Laboratory)

Figure 11-49: RCS Example



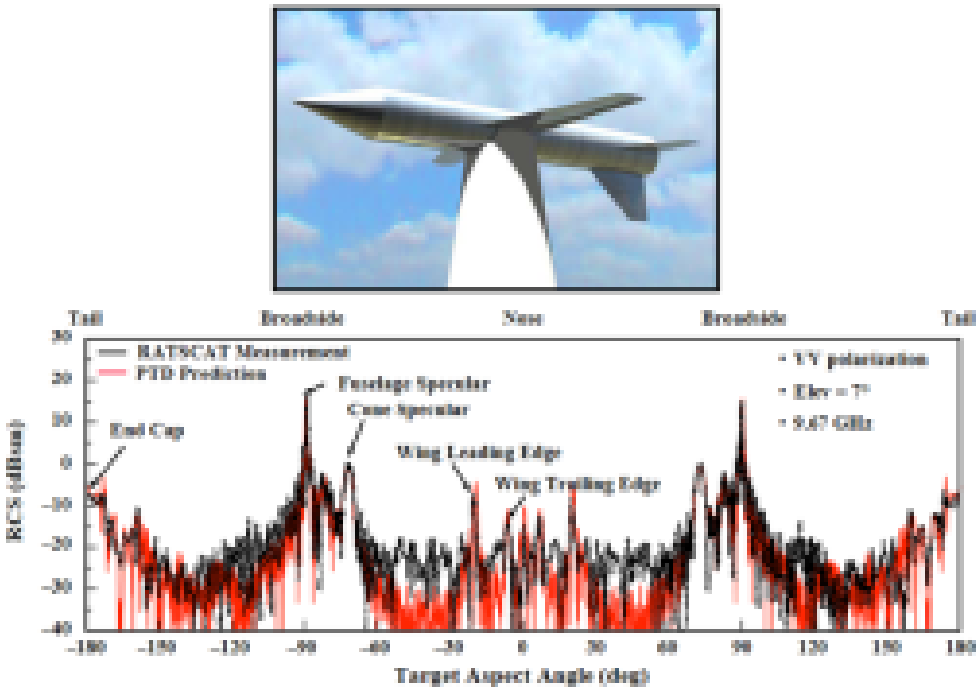
Source: (MIT Lincoln Laboratory)

Figure 11-50: Threat's View of the Radar Range Equation



Source: (MIT Lincoln Laboratory)

Figure 11-51: Measured and Calculated RCS of Johnson Generic Aircraft Model



Source: (MIT Lincoln Laboratory)

IMOM's output is both a graphic display and summary file that indicates the effectiveness of radar (Figure 11-52 depicts the baseline algorithm for determining a radar's range with respect to aircraft RCS) against an aircraft along its route. The simplest and the most important check that IMOM performs is a comparison of the aircraft, radar, and terrain position and height along a route. This is most comparable to a line-of-sight analysis, which can show if an aircraft is terrain masked effectively while in range of a radar or weapon system. When an aircraft is detected at a specific time and place along the route, IMOM checks the jammer profile to determine whether radar effects should be negated. The user can then compare an aircraft's position when the vulnerability was identified to the potential weapon systems that could perform an engagement (Ormesher, 1993). Figure 11-54 describes the IMOM ROUTE algorithm in detail, showing how all previously mentioned data sets are incorporated into determining an aircraft's level of detection (See Figure 11-55) along each point in its flight path.

Figure 11-52: ROUTE Algorithm for Calculating the Radar-Range Equation

$$R^4 = \frac{P_t G_t G_r I \sigma c^2}{(4\pi)^3 F_n B f^2 (SNR) L k T_o}$$

where

P_t	is the peak transmitted power of the radar signal in Watts
G_t	is the transmitting antenna power gain
G_r	is the receiving antenna power gain
I	is the receiver integration gain
σ	is the radar cross section of the aircraft in square meters
c	is the velocity of light
F_n	is the radar receiver's noise figure
B	is the receiver bandwidth in Hertz
f	is the radar frequency in Hertz
SNR	is minimum signal-to-noise ratio based on P_d and P_f
L	is the radar receiver loss
k	is Boltzmann's constant 1.38×10^{-23} Watts per Hertz per Kelvin
T_o	is the absolute temperature (290 K)

Source: (Richard C. Ormesher)

Figure 11-53: Radar Parameters Used in Radar-Range Equation

Table 2: Radar parameters used in radar-range equation

Parameter	Unit
P_t	kW
B	Hz
I	dB
L	dB
F_n	dB
SNR	dB
f	GHz
G_r	dB
G_t	dB

Source: (Richard C. Ormesher)

Figure 11-54: IMOM ROUTE Algorithm Description

Color	Level of Detection
Light Blue	Detection by EW, TA, or HF radars is probable
Green	Placement of SOJ against an EW, TA, or HF radar is probably effective in an area where the radar would normally detect the target aircraft
Red	The target aircraft is within a lethal weapon system envelope of a TT or FC system. Self-protection jamming probably has little or no effect on the tracking radar if used
Magenta	Placement of SOJ against the tracking radar on a TT or FC system is probably preventing the system from locking on to the target aircraft
Yellow	Self-protection jamming is probably degrading the TT or FC system by 35 to 70%
Grey	Self-protection jamming is probably degrading the TT or FC system by 70 to 100%
White	The aircraft is probably out of effective range of any of the threat systems
Dark Blue	The aircraft is probably terrain-masked from all threat systems

Source: (Richard C. Ormesher)

Figure 11-55: Color Code for Radar Detection

Color	Level of Detection
Light Blue	Detection by EW, TA, or HF radars is probable
Green	Placement of SOJ against an EW, TA, or HF radar is probably effective in an area where the radar would normally detect the target aircraft
Red	The target aircraft is within a lethal weapon system envelope of a TT or FC system. Self-protection jamming probably has little or no effect on the tracking radar if used
Magenta	Placement of SOJ against the tracking radar on a TT or FC system is probably preventing the system from locking on to the target aircraft
Yellow	Self-protection jamming is probably degrading the TT or FC system by 35 to 70%
Grey	Self-protection jamming is probably degrading the TT or FC system by 70 to 100%
White	The aircraft is probably out of effective range of any of the threat systems
Dark Blue	The aircraft is probably terrain-masked from all threat systems

Source: (Richard C. Ormesher)

As mentioned at the beginning of this section, IMOM was not designed for modeling space domain entities. However, the same inputs required to model an aircraft or missile flying in the atmosphere could be extrapolated for other space-centric use cases, such as space electronic warfare or unmanned aircraft satellite communication link analysis (Diebold, 2023) (Drew, 2023).

ADVANCED FRAMEWORK FOR SIMULATION, INTEGRATION, AND MODELING (AFSIM)

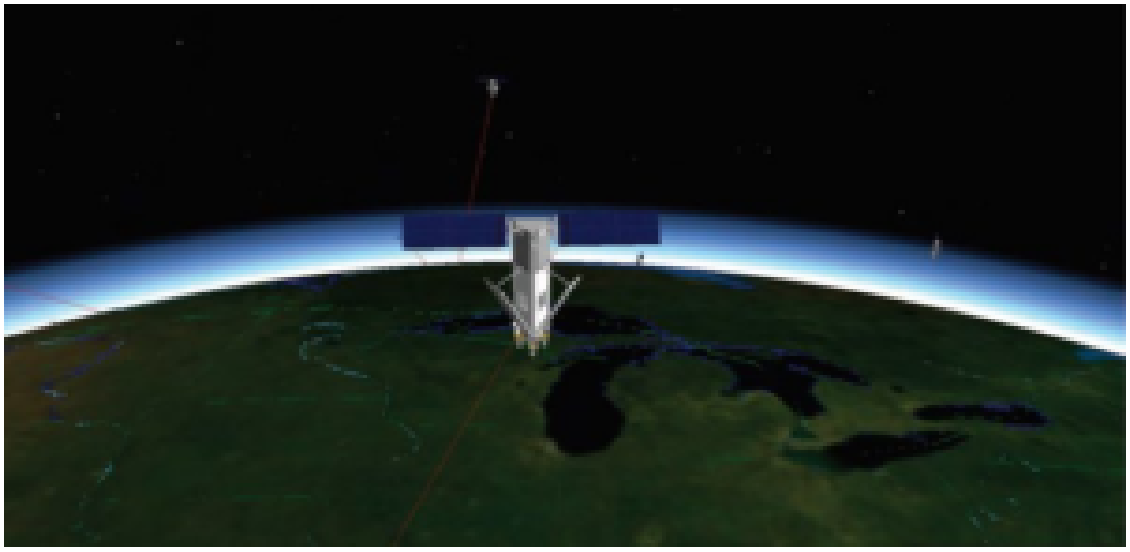
AFSIM was created by the Air Force Research Laboratory (AFRL) to make modeling and simulation ubiquitous in the weapon system concept development process, providing a framework for military simulations that seek to analyze, experiment, and wargame. Although developed by the Air Force, AFSIM is a multi-domain toolset capable of modeling land, air, sea, and space-based platforms such as tanks, helicopters, submarines, and satellites. The software also enables users to create their models for implementation if the standard toolkit does not provide the specific entity that a user needs (West & Birkmire, 2020).

AFSIM can model all four resolution levels described by Coolahan, capturing each by complexity and time

scale (See Figure 11-57 and 11-58). This allows users to focus on the factors most relevant to the decisions that need to be made from the outcome of the military simulation. For example, at the engagement and engineering levels, a user may be able to answer which satellites a hypersonic missile would need to interact with for positioning, navigation, and timing or communications during an intercontinental flight from launch to impact, factoring in terrain obscuration, jamming effects, and weather. At this level, it may highlight when the communication windows with satellites would be optimal across the flight path or if a satellite needs to push a boosted signal at a specific time and place to achieve an effect. On a larger scale, such as a mission or campaign, AFSIM could highlight the impact of an electronic warfare effect delivered from space on hundreds of units conducting large-scale conflict in a less precise manner (West & Birkmire, 2020).

AFSIM is produced at both the UNCLASSIFIED and SECRET classification levels, with the primary differences being the number, type, and fidelity of the models available for simulation (West & Birkmire, 2020). In the SECRET simulation, approved models for weapon systems and the operational environment are generated from classified intelligence provided by multiple DoD agencies, much like IMOM. For national security, it is common for DoD agencies to protect specific intelligence, such as the performance characteristics of models in AFSIM, to ensure the sources of that information and methods used to collect it remain protected. Therefore, for users with the requisite need to know and clearance to use this information, AFSIM can provide more accurate outputs (Diebold, 2023).

Figure 11-56: AFSIM Application Screenshot



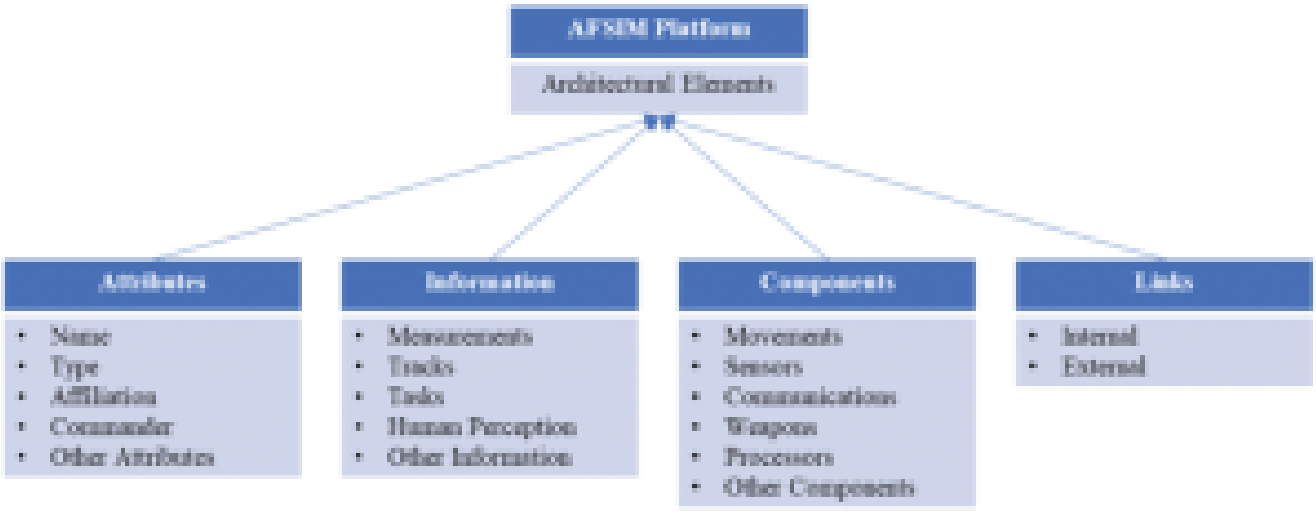
Source: (CSIAC | Credit: Col Timothy West and Brian Birkmire)

Figure 11-57: AFSIM Levels of Wargaming Simulations

Simulation Level	Complexity Scale	Time Scale
Campaign	Many v. Many	Days
Mission	Several v. Several	Hours
Engagement	One v. One	Minutes
Engineering	Subsystem Interaction	Seconds

Source: (CSIAC | Credit: Col Timothy West and Brian Birkmire)

Figure 11-58: AFSIM Architectural Elements



Source: (CSIAC | Credit: Col Timothy West and Brian Birkmire)

EXTENDED AIR DEFENSE SIMULATION (EADSIM)

EADSIM is a system-level simulation developed by the U.S. Army Space and Missile Defense Command (USASMDC) focused on air, space, and missile warfare. EADSIM enables analysts to model performance and predict the effectiveness of ballistic missiles, surface-to-air missiles, aircraft, and cruise missiles for operational-level commanders in multiple environments and scenarios. While AFSIM can simulate all four resolution

levels, EADSIM is best suited for the campaign (many on many) and mission levels (few on few). Each system in the simulation is individually modeled to include its command and control, sensors, jammers, networks, flight characteristics, and the effects of terrain and attrition. (U.S. Army Space and Missile Defense Command)

EADSIM has many use cases in the space domain. USASMDC advertises the capability to model and simulate an active defense, passive defense, attack operations, battle management, command, control, communications, and intelligence (BM/C3I), Integrated Air and Missile Defense (IAMD), and Cyber Electromagnetic Activities (CEMA). (U.S. Army Space and Missile Defense Command)

Figure 11-59: EADSIM Application Screenshots

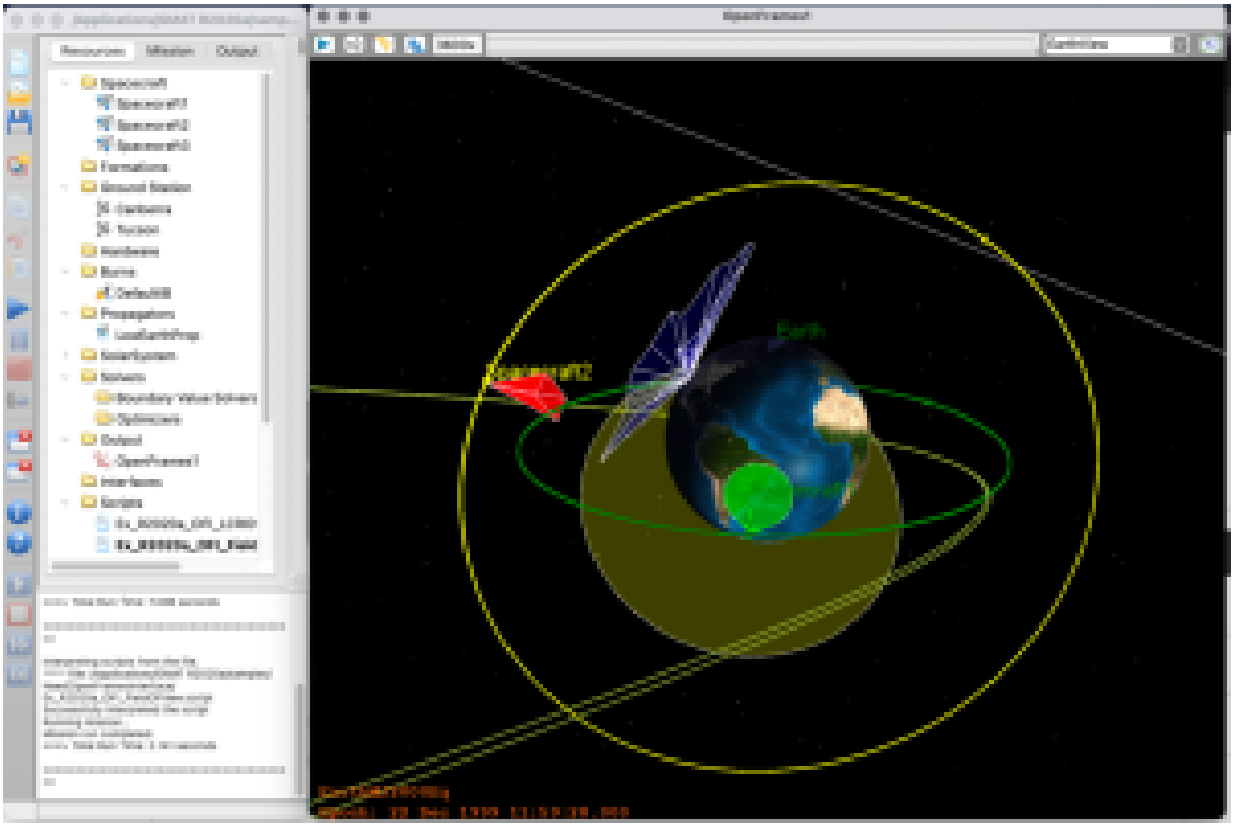
Source: (USASMDC EADSIM Fact Sheet)

GENERAL MISSION ANALYSIS TOOL (GMAT)

GMAT is an open-source space mission analysis tool developed by NASA, private industry, and many individual contributors intended to aid in real-world engineering design studies. Unlike the previous tools, GMAT was not designed specifically for military use cases. Instead, it was built to model, optimize, and estimate spacecraft trajectories in flights ranging from LEO to deep space missions. (GMAT Wiki, n.d.)

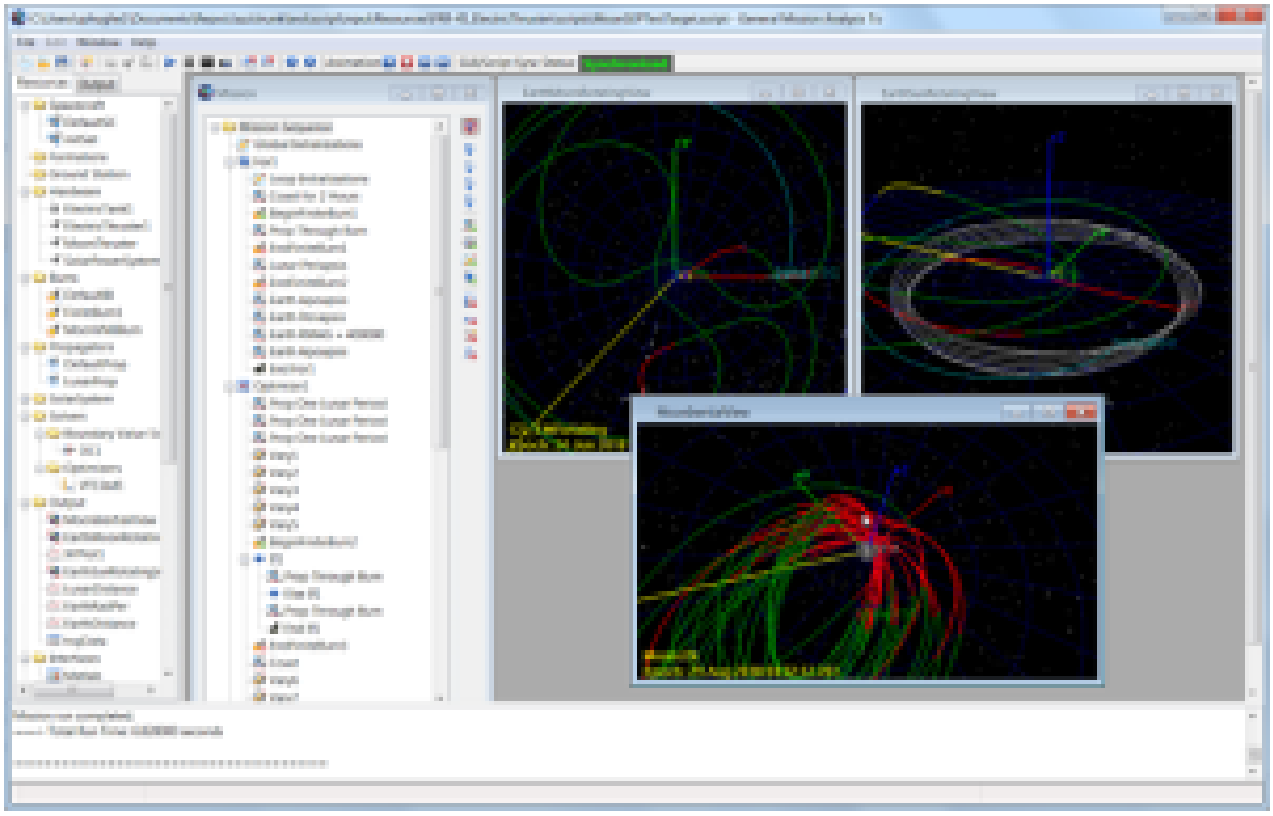
GMAT contains resources that can be broken down into physical models and customized to meet user requirements. These include spacecraft, thrusters, tanks, ground stations, formations, impulsive and finite burns, planets, comets, and asteroids. (GMAT Wiki, n.d.)

Figure 11-60: GMAT Project Sample Screenshot



Source: (SOURCEFORGE)

Figure 11-61: Sample GMAT Illustration Using a Low Thrust Propulsion System and Cube-Sat for a Lunar Mission



Source: (GMAT Wiki)

SYSTEMS TOOL KIT (STK)

Ansys developed STK to provide a physics-based modeling environment for analyzing platforms and payloads for the aerospace, defense, and telecommunications industries in a realistic mission context. In the premium space version, STK includes advanced orbit design and maneuver planning to improve a user's understanding of system performance. (Ansys, n.d.)

STK's capabilities include.

- high-fidelity orbit propagation
- deep space trajectory design
- rendezvous and proximity operations
- conjunction analysis
- orbit maneuver planning
- attitude modeling
- power generation, storage, and consumption modeling
- satellite constellation design
- launch window analysis

- space environment effects

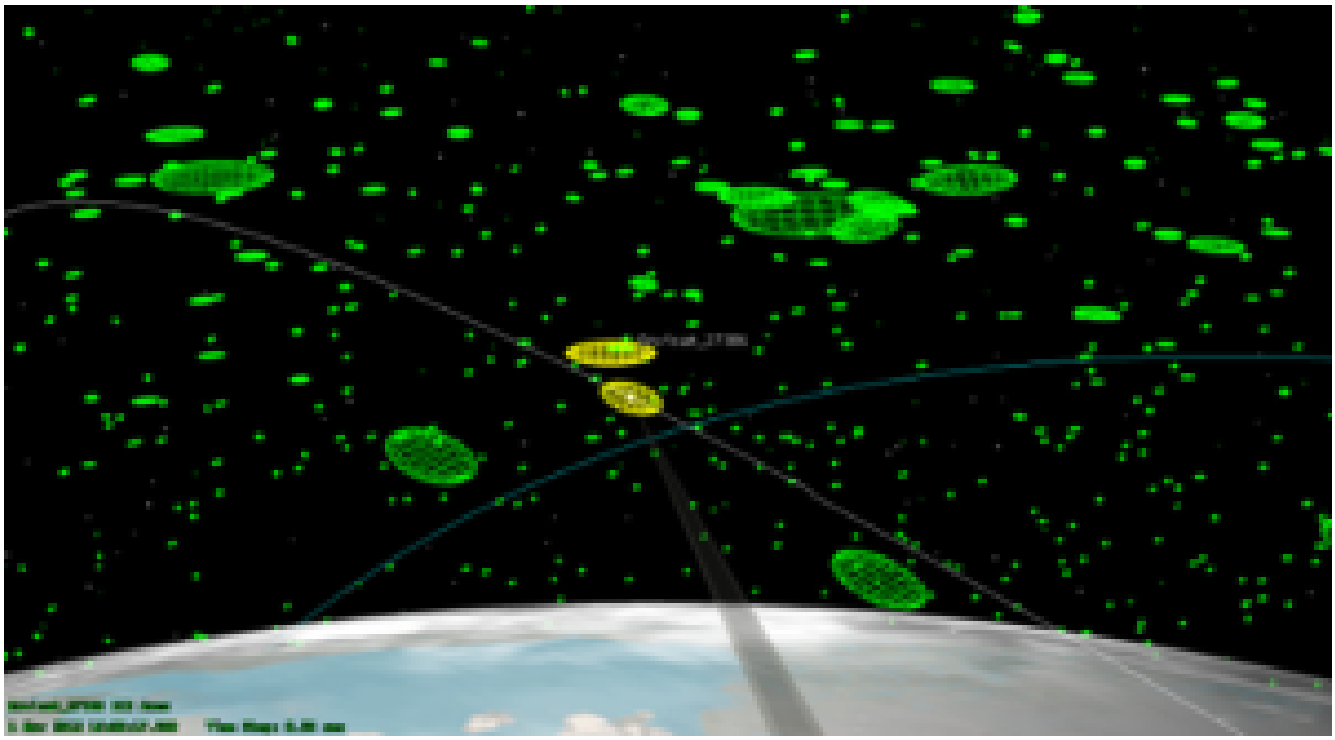
In the space-based systems modeling capabilities, STK has several core programs. The Astrogator assists mission planners in developing, optimizing, and validating flight-ready trajectory solutions for deep space operations. SatPro allows users to model a satellite's surface area, mass, and solar panel configuration, among other characteristics, to analyze its mission profile strengths and weaknesses. The Space Environment Effects Tool adds variables in the near-Earth space environment to orbit modeling, calculating exposure to ionizing particles, thermal radiation, and space debris. The Conjunction Analysis Tool includes threat analysis to detect potential collisions in space, providing users with a probability of collision, optimal launch windows, and even blackout times when a ground-based laser would affect an object in space. The Analyzer and Optimizer integrates engineering analysis to understand better factors like fuel usage, satellite coverage, and signal-to-noise ratio.

Real-Time Tracking Technology, Distributed Simulation, and Electro-Optical/Infrared (EOIR) models are the most impressive capabilities for military users. These tools allow users to monitor a live simulation in STK and incorporate common data feeds such as Link 16, NATO's Digital Motion Imagery Standard, and NATO's Ground Moving Target Indicator Format. EOIR models the detection, tracking, and imaging performance of electro-optical and infrared sensors on satellites, factoring in variables such as atmospheric weather, thermal and optical properties of celestial bodies, and Earth's surface. (Ansys, n.d.)

Figure 11-62: Sample STK Screenshot Demonstrating Advanced Modeling of Space-Based Platforms and Payloads

Source: (Ansys STK Premium Space Brochure)

Figure 11-63: Sample STK Screenshot Demonstrating the Space Environment Effects Tool

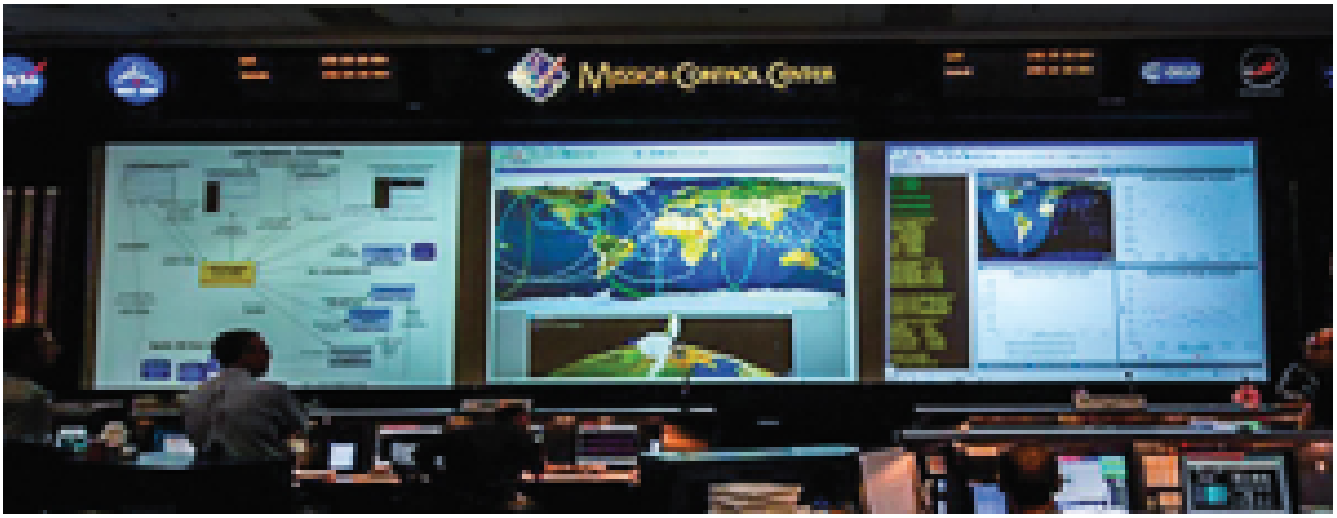


Source: (Ansys STK Premium Space Brochure)

FREEFLYER

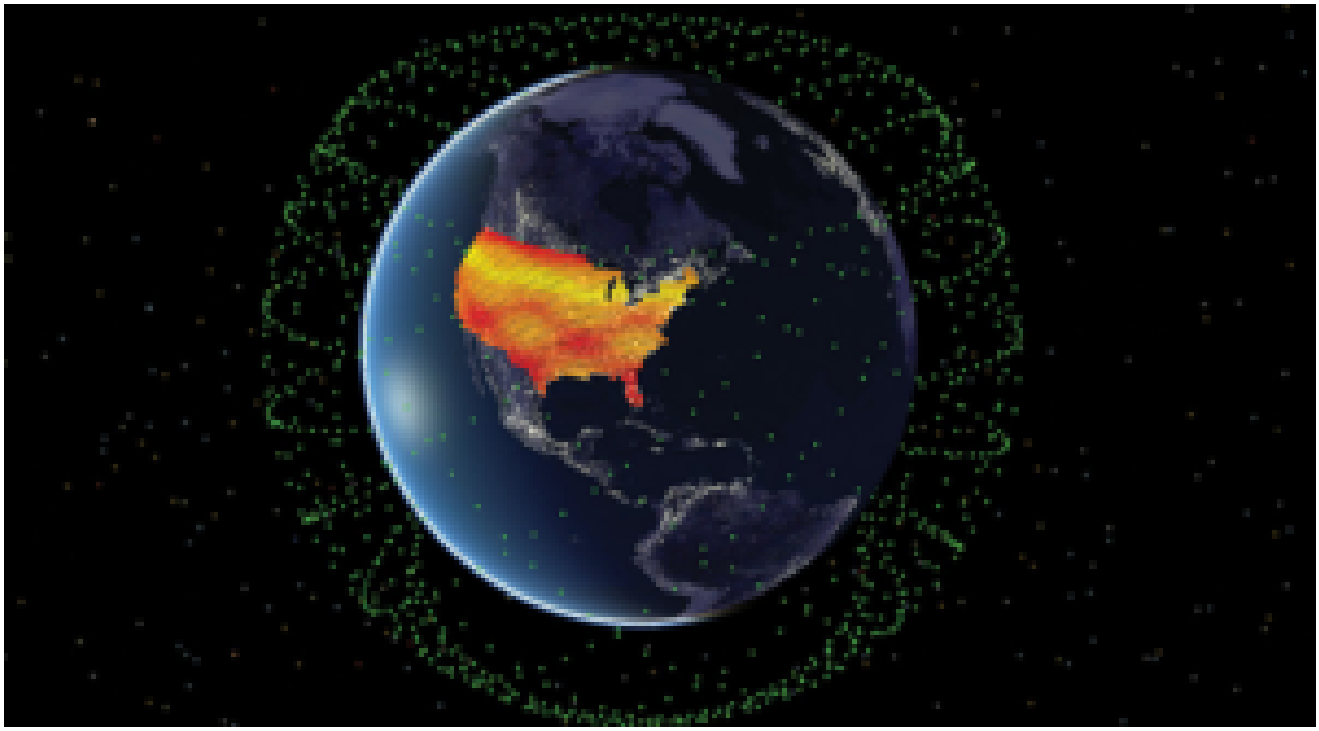
AI solutions developed FreeFlyer as a commercial off-the-shelf software application for space mission design, analysis, and operations. Its core functions include spacecraft propagation, coverage and contact analysis, maneuver modeling and targeting, orbit determination, attitude modeling, and terrain analysis. The primary use cases for FreeFlyer include space domain awareness, orbital debris collision avoidance, ground system integration, automated operations, mission design and analysis, wargame strategies, and constellations and clusters. Like AFSIM, the documentation suggests that FreeFlyer has a classified software version for use by government agencies with the appropriate clearance and requirements. (a.i. solutions, n.d.)

Figure 11-64: FreeFlyer Used in the ISS NASA Mission Control Center at Houston, TX



Source: (a.i. solutions FreeFlyer Capabilities Brochure)

Figure 11-65: Sample FreeFlyer Screenshot Demonstrating Analysis of Constellations



Source: (a.i. solutions FreeFlyer Capabilities Brochure)

CONCLUSIONS

Throughout this chapter, we explored various topics related to space modeling and simulations. In the beginning, this chapter described space operations from the advent of NASA and the first moon landings in 1969 through the modern space environment that now includes thousands of operational satellites from 75 countries. Next, we covered the evolving strategic context through the lens of civilian, commercial, and military space users, especially the growing aerospace defense problem posed by emerging technology. Finally, this chapter examined a framework for models and simulations and the tools and use cases.

More than at any point in history, there is a need for accurate and precise space models and simulations to predict the outcome of any aerospace operation. The space domain has rapidly expanded to impact aspects of civilian life, generated extensive revenue in the commercial sector, and proven to be a warfighting domain extraordinarily relevant to US national security. With the extensive and growing list of tools available, even the average user can learn to take advantage of capabilities in space through an enhanced understanding of complex system interactions. Using this knowledge, we can apply space models and simulations to use cases in any facet of personal life, public service, business, or national defense.

REFERENCES

(Coolahan, 2003) (Goddard Space Flight Center, n.d.) (a.i. solutions, n.d.) (U.S. Army Space and Missile Defense Command)

a.i. solutions. (n.d.). *FreeFlyer Astrodynamics Software*. Retrieved from a.i. solutions: https://ai-solutions.com/freeflyer-astrodynamic-software/

Ansys. (n.d.). *Ansys Systems Tool Kit (STK) – Software for Digital Mission Engineering and Systems Analysis*. Retrieved from https://www.ansys.com/products/missions/ansys-stk

Arms Control Association. (2022, November). *Seven Countries Join ASAT Test Ban*. Retrieved from Arms Control Association: https://www.armscontrol.org/act/2022-11/news-briefs/seven-countries-join-asat-test-ban

Badham, J. (Director). (1983). *WarGames* [Motion Picture].

Balachandran, A., Rabuya, L. C., Shinde, S., & Takalkar, A. (n.d.). *Simulation and Modeling Team.* Retrieved from University of Houston: https://uh.edu/~lcr3600/simulation/contents.html

Blatt, T. M. (2020, May 26). *Anti-Satellite Weapons and the Emerging Space Arms Race*. Retrieved from Harvard International Review: https://hir.harvard.edu/anti-satellite-weapons-and-the-emerging-space-arms-race/

Brockmann, K., & Schiller, M. (2022, February 4). *A matter of speed? Understanding hypersonic missile systems*. Retrieved from Stockholm International Peace Research Institute: https://sipri.org/commentary/topical-backgrounder/2022/matter-speed-understanding-hypersonic-missile-systems

Bugos, S. (2021, December). *Russian ASAT Test Creates Massive Debris*. Retrieved from Arms Control Association: https://www.armscontrol.org/act/2021-12/news/russian-asat-test-creates-massive-debris

Caffrey, M. (2000, April 27). *Toward a History Based Doctrine for Wargaming*. Retrieved from Air University: https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/caffrey.pdf

Chakrabarti, S. (2021, September 25). *How many satellites are orbiting Earth?* Retrieved from space.com: https://www.space.com/how-many-satellites-are-orbiting-earth

Clausewitz, C. v. (n.d.). *On War*.

Congressional Research Service. (2023, February 13). *Hypersonic Weapons: Background and Issues for Congress (R45811).* Retrieved from https://sgp.fas.org/crs/weapons/R45811.pdf

Congressional Research Service. (2023, March 16). *The Army's Multi-Domain Task Force (MDTF).* Retrieved from congress.gov: https://crsreports.congress.gov/product/pdf/IF/IF11797

Coolahan, J. E. (2003). Modeling and Simulation at APL. *Johns Hopkins APL Technical Digest, Volume 24, Number 1*.

CSIS. (2023, February 16). *Space Environment: Total Launches by Country*. Retrieved from CSIS Aerospace: https://aerospace.csis.org/data/space-environment-total-launches-by-country/

CSIS Missile Defense Project. (2021, August 2). *Minuteman III*. Retrieved from Missile Threat: https://missilethreat.csis.org/missile/minuteman-iii/

CSIS Missile Defense Project. (2021, April 12). *Missiles of China*. Retrieved from https://missilethreat.csis.org/country/china/

CSIS Missile Defense Project. (2021, August 10). *Missiles of Russia*. Retrieved from https://missilethreat.csis.org/country/russia/

CSIS Missile Defense Project. (2023, February 28). *Tomahawk*. Retrieved from Missile Threat: https://missilethreat.csis.org/missile/tomahawk/

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/

Diebold, C. (2023). Author's Personal Experience.

Drew, J. (2023, May 1). (C. Diebold, Interviewer)

Eckstein, M. (2017, April 7). *How the U.S. Planned and Executed the Tomahawk Strike Against Syria*. Retrieved from USNI News: https://news.usni.org/2017/04/07/us-planned-executed-tomahawk-strike

ESRI. (2022, January). *SatteliteXplorer*. Retrieved from ESRI: https://geoxc-apps.bd.esri.com/space/satellite-explorer/

(2018). *Fact Sheets: President Donald J. Trump is Unveiling an America First National Space Strategy.*

FCNL Education Fund. (2021, March). *Intercontinental Ballistic Missiles (ICBMs) Increase the Risk of Nuclear War.* Retrieved from https://www.fcnl.org/sites/default/files/2021-03/ICBMs%20Increase%20the%20Risk%20of%20Nuclear.FINAL_.pdf

Freedberg, S. J. (2019, June 4). *Army Wants Hypersonic Missile Unit by 2023: Lt. Gen. Thurgood*. Retrieved

from breakingdefense.com: https://breakingdefense.com/2019/06/army-wants-hypersonic-missile-unit-by-2023-lt-gen-thurgood/

GAO. (2022, June). *Missile Defense – Better Oversight and Coordination Needed for Counter-Hypersonic Development (GAO-22-105075).* Retrieved from gao.gov: https://www.gao.gov/assets/gao-22-105075.pdf

GMAT Wiki. (n.d.). *GMAT Wiki*. Retrieved from Confluence: https://gmat.atlassian.net/wiki/spaces/GW/overview

Goddard Space Flight Center. (n.d.). *Design and Integration Tools – General Mission Analysis Tool (GMAT) v.R2016a*. Retrieved from NASA TECHNOLOGY TRANSFER PROGRAM: https://software.nasa.gov/software/GSC-17177-1

Graham-Harrison, E. (2017, April 7). *A visual guide to the US missile strikes on a Syrian airbase*. Retrieved from The Guardian: https://www.theguardian.com/world/2017/apr/07/visual-guide-us-airstrikes-on-syria-donald-trump

Granai, C. (2015, January 3). *"A Complex and Volatile Environment": The Doctrinal Evolution from Full Spectrum Operations to Unified Land Operations.* Retrieved from https://apps.dtic.mil/sti/pdfs/AD1001386.pdf

Hadley, G. (2023, January 13). *Saltzman: China's ASAT Test Was 'Pivot Point' in Space Operations*. Retrieved from Air & Space Forces Magazine: https://www.airandspaceforces.com/saltzman-chinas-asat-test-was-pivot-point-in-space-operations/

Headquarters Department of the Army. (2001, June). *FM 3-0 Operations.* Retrieved from https://www.bits.de/NRANEU/others/amd-us-archive/fm3-0%2801%29.pdf

Headquarters Department of the Army. (2011, October). *ADP 3-0 Unified Land Operations.* Retrieved from https://www.army.mil/e2/downloads/rv7/info/references/ADP_3-0_ULO_Oct_2011_APD.pdf

Headquarters Department of the Army. (2012, May). *ADRP 3-0 Unified Land Operations.* Retrieved from https://www.lsu.edu/hss/milsci/resources/adrp3_0.pdf

Headquarters Department of the Army. (2022, October). *FM 3-0 Operations*. Retrieved from https://irp.fas.org/doddir/army/fm3-0.pdf

Heginbotham, E., Nixon, M., Morgan, F. E., Heim, J. J., Hagen, J., Li, S., . . . Morris, L. J. (n.d.). *The U.S.-China Military Scorecard – Forces, Geography, and the Evolving Balance of Power 1996-2017.* Retrieved from RAND Corporation: https://www.rand.org/paf/projects/us-china-scorecard.html

History.com Editors. (2009, November 18). *Bombing of Hiroshima and Nagasaki*. Retrieved from History.com: https://www.history.com/topics/world-war-ii/bombing-of-hiroshima-and-nagasaki

History.com Editors. (2022, November 9). *Atomic Bomb History*. Retrieved from History.com: https://www.history.com/topics/world-war-ii/atomic-bomb-history#:~:text=The%20atomic%20bomb%20and%20nuclear%20bombs%20are%20powerful,of%20World%20War%20II%2C%20in%20Hiroshima%20and%20Nagasaki.

Howell, E. (2021, October 3). *SpaceX's Inspiration4 all-civilian spaceflight: Here's what to know*. Retrieved from space.com: https://www.space.com/spacex-inspiration4-mission-explained

International Trade Administration. (n.d.). *Market Overview – Space Launch*. Retrieved from Commercial Space: https://www.trade.gov/commercial-space

Joint Chiefs of Staff. (n.d.). *Origin of Joint Concepts*. Retrieved from https://www.jcs.mil/About/Origin-of-Joint-Concepts/

Jomini, A. H. (n.d.). *The Art of War*.

Judson, J. (2021, October 7). *'Dark Eagle' has landed: US Army finishes equipping first unit with hypersonic capability — minus the missiles*. Retrieved from DefenseNews: https://www.defensenews.com/breaking-news/2021/10/07/dark-eagle-has-landed-us-army-finishes-equipping-first-unit-with-hypersonic-capability-minus-the-missiles/

Kim, S. E. (2021, August 25). *Can the World's First Space Sweeper Make a Dent in Orbiting Debris?* Retrieved from Smithsonian Magazine: https://www.smithsonianmag.com/science-nature/can-worlds-first-space-sweeper-make-dent-orbiting-debris-180978515/

Lopez, C. T. (2019, September 27). *Spacecom Built for Today's Strategic Environment.* Retrieved from U.S. Department of Defense: https://www.defense.gov/News/News-Stories/Article/Article/1973953/spacecom-built-for-todays-strategic-environment/

Missile Defense Advocacy Alliance. (2023, January). *China*. Retrieved from https://missiledefenseadvocacy.org/missile-threat-and-proliferation/todays-missile-threat/china/

Missile Defense Advocacy Alliance. (n.d.). *Russia*. Retrieved from https://missiledefenseadvocacy.org/missile-threat-and-proliferation/todays-missile-threat/russia/

MIT Lincoln Laboratory. (2018). *Introduction to Radar Systems – Target Radar Cross Section.* Retrieved from https://www.ll.mit.edu/sites/default/files/outreach/doc/2018-07/lecture%204.pdf

NASA. (2000, January 19). *NASA JOHNSON SPACE CENTER ORAL HISTORY PROJECT – BIOGRAPHICAL DATA SHEET – Carroll H. "Pete" Woodling.* Retrieved from NASA: https://historycollection.jsc.nasa.gov/JSCHistoryPortal/history/oral_histories/WoodlingCH/CHW_BIO.pdf

NASA. (2009, September 4). *Three Classes of Orbit*. Retrieved from NASA Earth Observatory: https://earthobservatory.nasa.gov/features/OrbitsCatalog/page2.php

NASA. (2018, April 2). *NASA History Overview*. Retrieved from NASA: https://www.nasa.gov/content/nasa-history-overview

National Air and Space Museum. (2017, May 23). *Ask an Explainer*. Retrieved from How Things Fly: https://howthingsfly.si.edu/ask-an-explainer/what-speed-required-launch-object-space

Neuman, S. (2023, March 9). *Russia is firing hypersonic missiles into Ukraine that are nearly impossible to stop*. Retrieved from npr.org: https://www.npr.org/2023/03/09/1162185287/hypersonic-missiles-ukraine-russia

Nichols, R., Carter, C., Diebold, C., Drew, J., Farcot, M., Jackson, M., . . . & Toebes, J. (2023). Space Electronic Warfare. In R. Nichols, *CYBER HUMAN SYSTEMS, SPACE TECHNOLOGIES AND THREATS* (p. Chapter 10). Manhattan: New Prairie Press. Accepted for Publication, 2023; NPP#TBN.

Olivier, S. S. (2008, September 15). *A Simulation and Modeling Framework for Space Situational Awareness.* Retrieved from https://www.osti.gov/servlets/purl/945663

Ormesher, R. C. (1993, April). *Improved Many-On-Many ROUTE Software Description.* Retrieved from National Technical Information Service: https://ntrl.ntis.gov/NTRL/dashboard/searchResults/titleDetail/DE93013961.xhtml

P., N. R. (2014, July 1). *The World's first guided missiles : V1 and V2*. Retrieved from defencyclopedia: https://defencyclopedia.com/2014/07/01/the-worlds-first-guided-missiles-v1-and-v2/#:~:text=The%20V1%20has%20the%20distinction%20of%20being%20the,and%20flew%20at%20a%20speed%20of%20640%20km%2Fhr.

Page, E. H. (n.d.). Modeling and Simulation, Experimentation, and Wargaming – Assessing a Common Landscape. Retrieved from https://www.mitre.org/sites/default/files/publications/16-2757-modeling-and-simulation-experimentation-and-wargaming.pdf

Panda, A., & Silverstein, B. (2022, April 20). *The U.S. Moratorium on Anti-Satellite Missile Tests Is a Welcome Shift in Space Policy*. Retrieved from Carnegie Endowment for International Peace: https://carnegieendowment.org/2022/04/20/u.s.-moratorium-on-anti-satellite-missile-tests-is-welcome-shift-in-space-policy-pub-86943

Precedence Research. (n.d.). *Simulation Software Market*. Retrieved from https://www.precedenceresearch.com/simulation-software-market

Skibba, R. (2021, November 17). *The US Space Force Wants to Clean Up Junk in Orbit*. Retrieved from Wired: https://www.wired.com/story/the-us-space-force-wants-to-clean-up-junk-in-orbit/

Skinner, D. W. (1988, September). *Airland Battle Doctrine.* Retrieved from https://apps.dtic.mil/sti/pdfs/ADA202888.pdf

Smith, M. (2022, August 10). *Anti-satellite weapons: History, types and purpose*. Retrieved from space.com: https://www.space.com/anti-satellite-weapons-asats

SOURCEFORGE. (2023, January 26). *General Mission Analysis Tool (GMAT)*. Retrieved from sourceforge.net: https://sourceforge.net/projects/gmat/

Staff. (2023). *Oxford Dictionary.* London: Oxford Dictionary.

Tate, K. (2021, November 3). *How Intercontinental Ballistic Missiles Work (Infographic)*. Retrieved from Space.com: https://www.space.com/19601-how-intercontinental-ballistic-missiles-work-infographic.html

Tchorowski, N., Murawski, R., Manning, R., & Fuentes, M. (n.d.). Modeling and Simulation of Phased Array Antennas to Support Next-Generation Satellite Design.

Tellis, A. J. (2019, April 15). *India's ASAT Test: An Incomplete Success*. Retrieved from Carnegie Endowment for International Peace: https://carnegieendowment.org/2019/04/15/india-s-asat-test-incomplete-success-pub-78884

The Editors of Encyclopedia Britannica. (2023, March 28). *Cruise Missile*. Retrieved from Britannica: https://www.britannica.com/technology/cruise-missile

The Editors of Encyclopedia Britannica. (n.d.). *go*. Retrieved from https://www.britannica.com/topic/go-game

The International Institute for Strategic Studies. (2022, February). *China's 2021 orbital-weapon tests*. Retrieved from IISS.org: https://www.iiss.org/publications/strategic-comments/2022/chinas-2021-orbital-weapon-tests#:~:text=In%20mid-2021%2C%20China%20launched%20two%20unprecedented%20test%20weapons,the%20atmosphere%2C%20which%20hit%20targets%20on%20Chinese%20territory.

Tingley, B. (2022, December 12). *US Air Force launches 1st operational hypersonic missile.* Retrieved from space.com: https://www.space.com/us-air-force-launches-first-hypersonic-missile

Title 10 USC Ch 6: Combatant Commands. (n.d.). Retrieved from https://uscode.house.gov/view.xhtml?path=/prelim@title10/subtitleA/part1/chapter6&edition=prelim

Tzu, S. (n.d.). *The Art of War*.

U.S. Army Space and Missile Defense Command. (n.d.). *Extended Air Defense Simulation (EADSIM).* Retrieved from https://www.smdc.army.mil/Portals/38/Documents/Publications/Fact_Sheets/EADSIM.pdf

University of Florida Department of Mechanical & Aerospace Engineering. (n.d.). *History of Cruise Missiles.* Retrieved from https://mae.ufl.edu/~uhk/CRUISE-MISSILES.pdf

US Army Training and Doctrine Command. (2018, December 6). *TP 525-3-1 The U.S. Army in Multi-Domain Operations 2028.* Retrieved from https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-1.pdf

US Space Force. (n.d.). *United States Space Force History*. Retrieved from https://www.spaceforce.mil/About-Us/About-Space-Force/History/

VTP. (n.d.). *DTED files (Digital Terrain Elevation Data)*. Retrieved from http://vterrain.org/Elevation/dted.html

Wampler, R. L., Centric, J., & Salter, M. S. (1998, January). *The Military Decision-Making Process (MDMP): A Prototype Training Product.* Retrieved from U.S. Army Research Institute for the Behavioral and Social Sciences: https://apps.dtic.mil/sti/pdfs/ADA343154.pdf

Watts, J. T., Trotti, C., & Massa, M. J. (2020, August). *Primer of Hypersonic Weapons in the Indo-Pacific Region.* Retrieved from Atlantic Council Scowcroft Center for Strategy and Security: https://www.atlanticcouncil.org/wp-content/uploads/2020/08/Hypersonics-Weapons-Primer-Report.pdf

Wellerstein, A. (2022). *Nukemap 2.72*. Retrieved from nuclearsecrecy.com: https://nuclearsecrecy.com/nukemap/

West, T. D., & Birkmire, B. (2020, January 9). *AFSIM: The Air Force Research Laboratory's Approach to Making M&S Ubiquitous in the Weapon System Concept Development Process.* Retrieved from Cybersecurity & Information Systems Information Analysis Center: https://csiac.org/articles/afsim-the-air-force-research-laboratorys-approach-to-making-ms-ubiquitous-in-the-weapon-system-concept-development-process/

Woodling, C., Faber, S., Van Bockel, J. J., Olasky, C. C., Williams, W. K., Mire, J. L., & Homer, J. R. (1973,

March). *Apollo Experience Report – Simulation of Manned Space Flight for Crew Training*. Retrieved from NASA: https://www.hq.nasa.gov/alsj/tnD7112Simulators.html

ENDNOTES

[1] Operational variables refer to the PMESII acronym in joint US military doctrine including Political, Military, Economic, Social, Information, and Infrastructure. The mission variables refer to the acronym METT-TC including Mission, Enemy, Terrain, Troops Available (extrapolated to mean resources), Time, and Civilian Considerations.

[2] Translated: "A glance that takes in a comprehensive view." (Staff, 2023)

[3] DoD and Open-Source documentation varies on the advertised capabilities of the Tomahawk, likely due to the numerous variants.

12.

DEEP SPACE WARFARE AND SPACE DOMINANCE [NICHOLS]

PURVIEW

As of this writing (February 14, 2023), multiple intelligence balloons or UFOs from unknown sources have traversed the United States and penetrated the Air Defense Systems (ADS). It took more than a week for POTUS to shoot down a Chinese spy balloon. (Gustaf Kilander, 2023)[1] The DoD reported that its first shot was missed by a defensive F-16 at a UFO over Lake Huron. [2] Chinese surveillance balloons have been detected over the Middle East according to USAF LTG Alexus Grynkewich. (Paul Best, 2023)

Since 2018, KSU Wildcat author teams have explored the Risks, Vulnerabilities, Impact, and Countermeasures for US ADS, specifically for Unmanned Aircraft Systems (UAS). (Nichols & al, Space Systems: Emerging Technologies and Operations, 2022), (Nichols & Sincavage, 2022), (Nichols & al., Unmanned Vehicle Systems and Operations on Air, Sea, and Land, 2020), (Nichols R. K., 2020), (Nichols R. K., 2020), (Nichols R. K.-P., 2019)

Their conclusions and ISSUES identified were:

THREAT: The RISK of *success of terrorist attacks* on Air Defense Systems (ADS) via UASs / SUAS is higher and improving with commercial capabilities and accessibility. (Nichols R. K., 2020)

HOW: Advanced small drones capable of carrying sophisticated imaging equipment, significant and deadly (WMDD) payloads are readily available to the civilian market. (Nichols & Sincavage, 2022)

WHO? A range of nation-state, terrorist, insurgent, criminal, corporate, and activist threat groups have demonstrated the ability to use civilian drones and gather intelligence.

ISSUES – ADS optimized for missiles and AC at high altitudes & speeds.

- **Data fusion works better with larger targets.**
- **Reactive for longer ranges.**
- **Close reactive requirements sub-optimal.**

ADS Vulnerabilities to sUAS

- **SUAS launched into action close to target(s) – ~ 1 mile. Small Radar signature.**
- **Reactive dictates quick response near target. Slow flight. LOW flying avoiding Radar**

identification.

- **Electric motors are both quiet and limited thermal signatures.**
- **Make difficult detection in noise. The urban sphere presents additional problems & potential collateral damage.** (Nichols R. K., DRONE WARS THREATS, VULNERABILITIES AND HOSTILE USE of UAS, 2017)

Keeping in mind the apparent deficiencies in the DoD, USAF, and POTUS responses to simple *balloon* incursions into our earthly ADS, we now take the fascinating mental jump to Deep Space and potential battles far beyond the constraints of Earth. What might the logistics and forces require to fight in deep space? (What is Deep Space, 2023) Can we imagine a *weaponized space domain* where military vessels and robotic machines fight force-on-force battles thousands of miles above the surface of the Earth?

Rather than the Sci-Fi notions of "Alien versus Human" in such movies as *Aliens, Mars Attack, District 9, Independence Day, Avatar, Star Wars, and Battlestar Galactica,* in reality, space warfare is already upon us. It is restricted to orbital activities near and around Earth. It is not beyond imagination that humans will make First Contact with another sentient life capable of competing with us on an interplanetary scale.[3] This does not consider that our first battles in space will be with ourselves (other humans). Commercial firms like Space X, Virgin Galactic, Blue Origin, Boeing, and Lockheed Martin are making huge progress in space tourism.

It is reasonable to assert that state-on-state conflict will be humans' first open space warfare experience. (Wright, 2020)[4]

Ye author's sense is that space warfare will look more like and require staged training of forces similar to *Enders Game*. What that movie should have addressed (and we will) is the *logistics* problem.

OBJECTIVES

This is an introductory chapter to a fascinating science – the conquest of deep space. It encompasses so many disciplines: materials, logistics, military science, weapons, tactics, operations, HAZMAT, navigation, safety, security, survival, forces and gravity, hostile environment, politics, First Contact and so many additional topics. The objective is to give the student a small flavor of some of the key concerns to building a naval–structured space force that might be able to colonize territory in deep space. This would not be a civilian operation but likely a military one guided by strategic, survival, and political goals.

Open sources focus on astrophysics, new discoveries, and public information about US Space Force Command technologies/budget/organization. Both approaches focused on some of the harsh realities of traveling into deep space and then launching operations to take territory. Two resources did provide enough strategy and thought to yield challenges to our readers, and we lean heavily on their experiences. (Wright, 2020) (Szymanski, How to Fight and Win the Coming Space War, 2019) Treat this chapter as a match to light further dreaming and thinking. Make yourself an Admiral and think how you would prepare your fleet to sail millions of miles into space to set up a forward base for future military endeavors. Along the way, you might

come into contact with a non-human sentient species that has similar ideas to Earth as its base. Is it a game of GO or Chess you are about to play?

INTERSTELLAR BASICS

In 1961, Frank Drake created a theoretical equation to determine the number of civilizations in the Milky Way capable of emitting detectable EM emissions. The equation was rife with assumptions that drastically affected the calculations. Drake's conjecture was about 340 spacefaring civilizations that could sustain life and be detectable by Earth technology. (Drake, 2023)

Conflict has existed since the first day that man evolved on Earth. I can picture Adam and Eve having a heated discussion about dinner. I don't know how it was settled. Conflict occurs because political units use power to ensure their survival and this use of power affects different political units unevenly. Military force is a key instrument of national power to ensure behavior and the right to survival. Unfortunately, humanity has always reserved the right to use violence and coercion. In nice terms, this is called international relations as using force to obtain political objectives.

Outer Space Treaty, formally the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, is a multilateral treaty that forms the basis of international space law. Negotiated and drafted under the auspices of the United Nations, it was opened for signature in the United States, the United Kingdom, and the Soviet Union on January 27, 1967, entering into force on October 10, 1967. As of February 2022, 112 countries are parties to the treaty—including all major spacefaring nations—and another 23 are signatories. (Wiki, 2023) Unfortunately, only political power can enforce or reject a claim; only conflict can ensure the final decision. Distances between stellar objects and logistical difficulties in supplying space forces mean a preponderance of military power in one area or near a particular supply object force the de facto arbiter of that object's security and access. (Wright, 2020)

ANARCHICAL ENVIRONMENT

Space comprises extreme distances between unfamiliar stellar bodies, which are or can be assumed hostile to human life. [5] Any territorial claims will be backed by political negotiations that hold interest in them and are prepared to maintain, supply, and protect their claims. In maritime Earth situations, it is incumbent on vessels to answer and assist in rescue operations for a vessel in distress. The law of salvage is a principle of maritime law whereby any person who helps recover another person's ship or cargo in peril at sea is entitled to a reward commensurate with the value of the property saved. (Wright, 2020)

Maritime law is inherently international, and although salvage laws vary from country to country, generally, there are established conditions to be met to allow a salvage claim. The vessel must be in peril, either immediate or forthcoming; the salvage vessel must act voluntarily and under no pre-existing contract; and the salvage

vessel must be successful in their efforts, though payment for partial success may be granted if the environment is protected. (Wiki, 2023) Because space is a self-help system, claimant states cannot rely on other political units to safeguard their claims. (Wright, 2020)

Space is a unique environment. Territorial claims share three characteristics: Technological sophistication, complications, and vulnerability. The deep space environment is hostile, unbelievably hostile to habitation and creating a permanent base or settlement. The logistics of supply are a nightmare in a horror show. The equipment in a simple research lab would require sophistication and stand-alone computing capabilities of 5-G networks available on Earth. Supply vessels would need to be escorted by military vessels. Communications would need to be the best that Earth engineers could offer. If a supply vessel arrived late – what would be the consequences to the lab? Everything must be designed for duplication, accuracy, uniqueness, security, survivability, replacement, longevity, and balance. It requires technical sophistication.

Space territorial claims would be complicated. They would be in 4-dimensions (three physical and time). Stellar phenomena are in motion according to their body and gravity's influence. Think miles cubed rather than square miles like Earth's territorial claims. Reference points protected air space, and boundaries could be at the heart of every disagreement.

Claims in space are, by nature, vulnerable. Space and maritime domains share the problem of pinpoint location. The extreme distances between claims and the slow speeds of space-going vessels mean the territorial claim will be unprotected for long periods. (Wright, 2020)

SPACE DISTANCE

Space is so big and vast that it defies our best measurement capabilities. Basic dimensions are measured as distances between stars and by listing the quantity (or estimate of) the number of stars themselves. Let's expand on a maritime example of MOB [6] or deserter from a ship at sea. Both swimmers in the water spot what they think is land, perhaps 1-2 nm from their location. They make this calculation with their head above water and in the sea where they are in motion with current and waves. They start swimming. The actual land mass might be as far as 5 nm. Estimates in water are usually 200% or more under stress conditions. [7]An average swimmer in 70oF water temperature, average wave conditions, and no sharks is 32.24 minutes across all ages and genders. (Anonymous, 1 Mile Swim Times: Swimming Standards By Age and Ability, 2023) Assuming our MOB or deserter is off by 3 nm, his total time would be 161 min for the 5 nm if not exhausted. Let's change the water temperature to 40oF. See Figure *12-1 Life Expectancy Following Cold Water Immersion.* Our MOB / Deserter has about 1 hour to have a 50% chance to live. Above 90 minutes, his life expectancy is zero. Even with an exposure suit, [8]Our MOB/Deserter would be in great danger as the nm increases. *See Figure 12- 2 Life Expectancy Following Cold-Water Immersion (Exposure Suit).* Errors in maritime situations are quite dependent on distance and environment and can quickly become life-threatening.

Now we put our play in space where the baseline temperature of outer space is based on the radiation of the Big Bang at -455 oF. (Wiki, 2023) Why is deep space this cold? The distance between gas and dust

particles grows, limiting their ability to transfer heat. Leaving a space vessel for any reason is fatal – immediately. Protective gear has its limitations, as well as the ability to carry oxygen. BTW, A body will decompose in space. Although there are no insects, fungi, or external organisms to break down the body, we still carry plenty of bacteria with us. Left unchecked, they would rapidly multiply and cause the putrefaction of a corpse on board the shuttle, ISS, or vessel. (Anonymous, Would a Corpse decay in space?, 2023)

Figure 12-1 Life Expectancy Following Cold Water Immersion

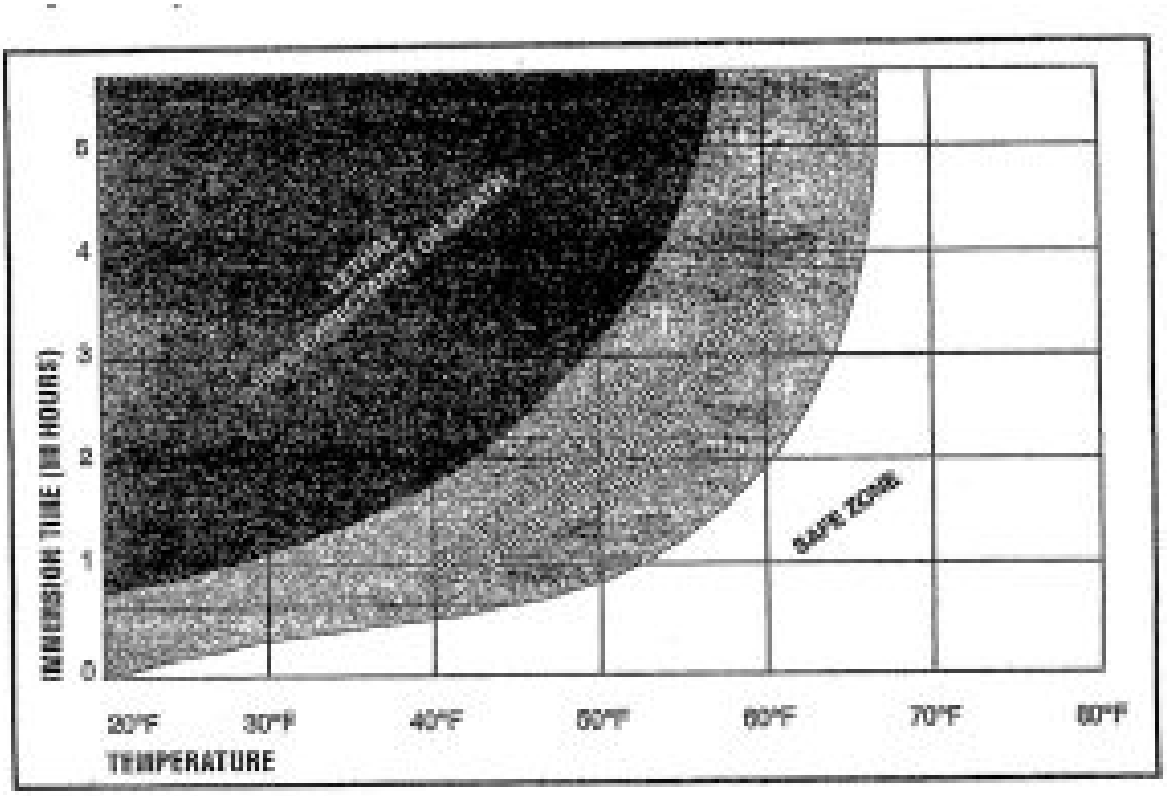


Figure 13-2. Life Expectancy Following Cold-Water Immersion.

Source: Reprinted from Figure 13-2 courtesy of (USAF, 2003)

Figure 12-2 Life Expectancy Following Cold-Water Immersion (Exposure Suit)

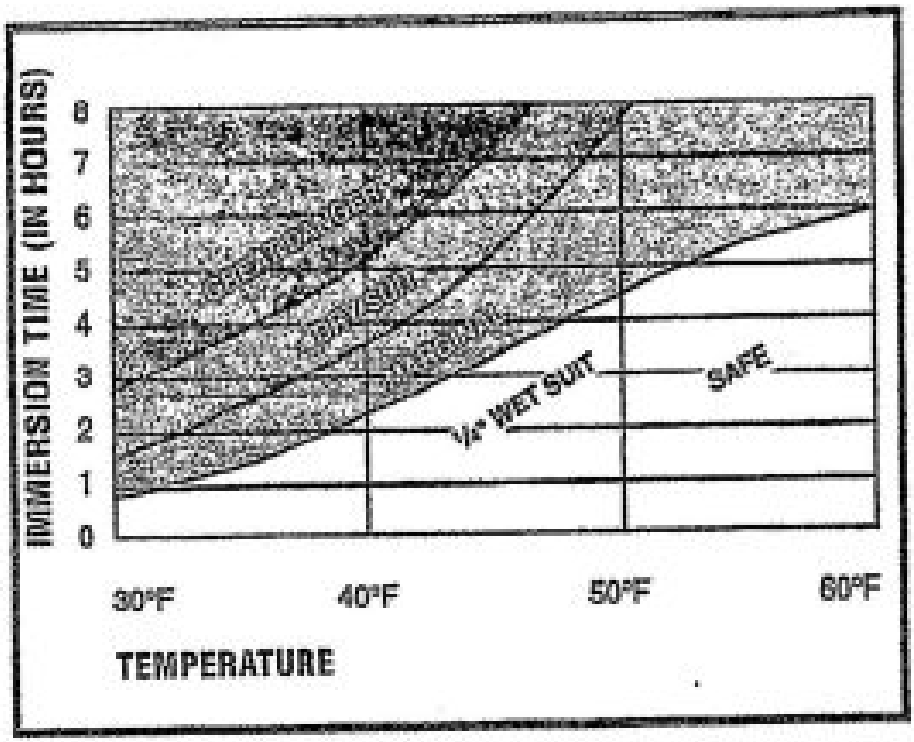


Figure 13-3. Life Expectancy Following Cold-Water Immersion (Exposure Suit).

Source: Reprinted from Figure 13-3 courtesy of (USAF, 2003)

Distances associated with space flight are brain-busters. Traveling at light speed (which is not possible yet) would take four years to reach our closest neighboring star, Alpha Centauri. Safely equipping a fleet-sized for deep space travel would be critical to any force hoping to traverse the galaxy. Planners must provide additional supplies, replacement parts, a machine shop, excess fuel, excess weapons, hazard protections, machinery duplication, backup communication, and navigation equipment. Multiple navigational hubs and protected lanes of travel would be required. (Wright, 2020)

DARK ENERGY AND DARK MATTER

There is so much mystery in the universe. Two components of the universe that have been studied but we really need to comprehend are dark energy and dark matter. Before contemplating sending a space force to engage with a combatant competitor, we must know more about these. Dark Energy (DE) appears to be accelerating

the universe's expansion with time. Discovered in the 1990s from observations of distant supernovas, this expansion observation contradicted the prevailing theory of cosmos decelerating. (Saikia, 2023) See Figure 12-3.

Figure 12-3 Hypernova

Source: (Saikia, 2023)

The explanation is that DE forces space to expand and gross less dense, thereby driving galaxies and other structures apart. From a space force POV, [9]waypoints and navigation sets are not constant.

Dark Matter (DM) does not interact with light or conventional matter. It was initially deduced from its gravitational effects on visible matter, such as the spinning and grouping of galaxies. DM is believed to constitute approximately 85% of the universe's matter, although scientists have yet to discover it directly. DM is the network glue for revealing enormous clusters and filaments of galaxies. This has been confirmed with modern telescopes and gravitational wave detectors. (Saikia, 2023) The relationship between DM and DE is being explored by NASA to identify the evolution of DE over time and space and how DM interacts with regular matter and other kinds of energy. See Figure 12-2 NASA Rendition of DE interactions with other energy forms.

FIGURE 12-4 A simulated drawing of a large black hole emitting high-energy atomic jets. Elements of this image furnished by NASA.jpg

Sources: NASA, (Saikia, 2023)

NAVAL MODEL

(Szymanski, How to Fight and Win the Coming Space War, 2019) presents a military lexicon of tactics, strategies, and objectives to be considered in near space (to GEO altitudes) against terrestrial competitors. DM and DE are less important in the direct altitudes over Earth's surface. However, our concern is with Deep space. (Wright, 2020) considers the environment and technologies available for an interstellar space force. DM and DE come into play big-time.

Forces serving in space would be comprised of forces structured similarly to our navies on Earth. [10] The nature of space travel means long, isolated, and unforgiving movement over vast distances. This is akin to ocean-going terrestrial navies. The cold and lifeless environment outside is to space vessels as the ocean is to submarines. (Wright, 2020) Space is a three-dimensional environment, and the occupant of any space vessel is at the mercy of zero gravity.

Vessels must be large enough to contain supplies, personnel, and equipment needed for spaceborne missions. Ships must carry spare and standby equipment to make repairs underway; space will swallow the unprepared or undersupplied. Terrestrial, naval ships do this regularly. Classic naval discipline will be required to protect provisions and personnel over long voyage times. Establish rank, traditions, and command mesh well with spaceborne forces.

SPACE RPO

Dr. Paul Szymanski is an SME on Space Rendezvous and Proximity Operations (RPO) and Contingency Planning. He teaches Satellite Warfare classes and is a US Space Forces consultant. [11] His writings are prolific, and three of his more interesting ones are "How to Fight and Win the Coming Space War" (Szymanski, How to Fight and Win the Coming Space War, 2019) "Space Operational Art and Design (SOAD)," (Szymanski, Space Operational Art, and Design (SOAD), 2020) and "Space Warfare Analysis Tools (SWAT) – Summary." (Szymanski, Space Warfare Analysis Tools (SWAT) Summary, 2020) [12]

ALL OR NOTHING

Major Wright and Dr. Szymanski agree that Deep Space Warfare would be "All or Nothing." They also believe that the model of Naval maritime engagements has analogs to space warfare. Naval and airborne battles will tend to be *All or Nothing*. They will win and live or lose and die. (Wright, 2020) Why? Operating in an extremely hostile environment means that the slightest mechanical or life support problem would lead to losing the entire vessel to the vacuum of space. Technological advantages like terrestrial naval combat tend to be decisive and tower over obsolete naval technology. Naval forces that press their weight upon the opposition will produce cascading destruction exponentially on the weaker force. Rescue and personnel recovery is unlikely in space because both the hostile environment and the battle are still active. The longer a battle rages in space, the more the losing side loses. (Wright, 2020)

SUPPLYING SPACE FORCES – A LOGISTICS NIGHTMARE

Dr. Szymanski presents a detailed discussion of space warfare implications for the Principals of War with a comparison of terrestrial and space considerations for each of the nine principles in Table 12-1. *Principles of Space War.* ***Dr. Szymanski's vision of space warfare is confined to the upper regions of satellites and space stations where their electronic signals or weapons reach down to or up from Earth. The potential combatants are political and known. Major Wright's vision encompasses deep space where First Contact is possible, distances are great, and the environment so hostile that rescue is unlikely. Combatants may be human or not. Combat is All or Nothing, and protecting territorial claims are in play. Those claims might be as big as another planet or mining section on a planet /star/asteroid or extended waypoint where supplies and personnel are prepositioned.***

TABLE 12-1 Principles of Space War[13]

1	Objective
2	Offensive
3	Mass
4	Economy of Force
5	Maneuver
6	Unity of Command
7	Security
8	Surprise
9	Simplicity

Source: (Szymanski, How to Fight and Win the Coming Space War, 2019)

We have two space war visionaries presenting their views of the implications of the Principles of Space War (Table 12-1). Their purview is different in terms of distance and logistics from the Earth. Dr. Szymanski considers the questions raised if space war is limited to the edge of satellites and space stations. Major Wright is concerned with deep space and dominance over humans and First Contact sentient or non-sentient beings. We can integrate/differentiate their KEY positions based on Table 12-1. See Table 12-2 for the author's synchronization of ideas based on two primary references and KSU's Wildcat research. (Szymanski, How to Fight and Win the Coming Space War, 2019) (Wright, 2020) (Nichols & al, Space Systems: Emerging Technologies and Operations, 2022) (Nichols, et al., 2023) Remember many questions can be raised about each of the implications of formal Principles of Space War. Questions give rise to more questions and debates. Our effort here is to find the nub of both visions. The doctrinal quotes have several sources. (Tzu, 2006) (USA, 2020) (Clausewitz, 2003) (Wright, 2020)

Table 12-2 Comparison and Interpretation of Space Warfare Visions grounded in Principles of Space War

Principle of Space War (Szymanski)	Terrestrial (Szymanski)	Space (Szymanski) from Earth to ISS[14]	Deep Space (Wright)[15]
Objective	"Direct every military operation toward a clearly defined, decisive, and attainable objective with measurable effects."	To take out one or more satellites supported by satellites and ground stations. What level of information denial can be achieved?	In deep space (DS), objectives must be crystal clear. DS's harsh environment immediately pits any military operation, of any size, against the clock. DS warfare is, first and foremost, to achieve a political objective. Are the forces available enough to achieve the "end result"
Offensive	"Seize, retain, and exploit the initiative."	Is there a political will to start a space war? Are US Forces setting the space battle's time, place, and terms?	When in battle in DS, it is ALL or NOTHING. They win and live or lose and die. Newer technology tends to be decisive against older technology or weapons. A Naval space force tends to press its weight until the weaker force begins to cascade exponentially.
Mass	"Mass the effects of overwhelming combat power at a decisive place and time."	Are there sufficient weapons to achieve continuous or sustained space control? How will the weapons cache be supplied? Can the weapons be synchronized for simultaneous and coordinated attacks?	DS resembles a maritime environment. Once sunk on Earth, a naval ship has a chance of rescuing some of its complement. In DS rescue is unlikely, and the entire complement is lost.
Economy of Force	"Employ all combat power available in the most effective way possible; allocate minimum essential combat power to secondary efforts."	Are all space control efforts and weapon systems integrated into one deployment/ employment plan? Are they purposefully in delay, limited, or deception operations that focus the enemy's attention away from the main space attack at all times of the conflict?	Taking on a planet or even a small star is measured in miles cubed, not square miles like on Earth. Allocation of forces where the space flight distances are mind-numbing presents far greater problems than minimizing forces. Further, a consideration of the makeup of those forces (Hybrid / robotic) is a force multiplier.
Maneuver	"Place the enemy in a position of disadvantage through the flexible application of combat power."	Are there critical orbits/time, phasing/launch, corridors /communications paths worldwide contributing to the battlefield that needs space superiority consideration?	The same principles hold, BUT Spaceborne forces may find themselves blasting each other without mercy like in a previous era of capital ships. Conceivably an entire fleet could be lost in a single engagement. Forces may engage less often because of Risk factors.

Unity of Command	"for every objective, seek a unity of command and unity of effort."	Is there adequate space/info war delineation of a chain of command and decision responsibility? Are target lists traceable back to objectives?	DS is an Anarchical Environment. Territorial claims will require technological innovation/ sophistication; they will be complicated and vulnerable.
Security	"Never permit the enemy to acquire unexpected advantage."	Have OPSEC concerns been met? Have choke points, centers of gravity (TT&C), [16]Have logistics and command structures been identified and protected?	Security has two distinct features in DS. OPSEC, COMSEC, and facilities security will be paramount. However, security is also a political consideration, especially when dealing with other non-Earth sentient beings.
Surprise	"Strike the enemy at a time or place or in a manner for which he is unprepared."[17]	The timing and tempo of space weapons use can be a surprise even if their existence is known. Threats of weapon use, even if the weapon doesn't exist, can effectively surprise.	Taking a planet is no mean feat. Surprise is difficult to achieve with long-range Intel, MASINT, and EW. A planetary assault would require 4 stages: Blockade; Siege; BW & CW deployment; orbital insertion, and space drop of sufficient troops – perhaps as many as five million. Surprise is not an option.
Simplicity	"Prepare clear, uncomplicated plans and concise orders to ensure thorough understanding."	How complex are space weapons and their deployment?	Planetary invasion is a logisticians' nightmare. What number of troops is necessary to beat a planet into submission? Planning for a several million-mile supply line is a horror. How about life support on the planet for sustaining forces? How about weapons, spare parts, medical supplies, casualties, hybrid components, and withdrawal if necessary. The headaches keep coming.

Sources: (Szymanski, How to Fight and Win the Coming Space War, 2019) (Wright, 2020) (Nichols & al, Space Systems: Emerging Technologies and Operations, 2022) (Nichols, et al., 2023) See Endnotes 12 & 13 regarding distances firewalling these visions.

FIRST CONTACT

The scale of the universe and our slow technological reach for the stars suggests an extraterrestrial (ET) sentient competitor "out there." It is only a question of when we make First Contact (FC). What would FC look like? How would FC behave – especially if FC is more advanced than us? Little green men? Bugs? EM impulses? Carbon-based? More than 1000 scientific movies have produced all kinds of ETs / FC. We, as a population and especially movie-making bodies of Japan, Russia, and Hollywood – come to mind – always assume that FC is bad or wants to use us for food or steal Earth's resources.

Shifting into the FC playground of deep space, it is reasonable to think of potential military confrontations and countermeasures from a military strategy perspective. FC scenarios carry with them unpredictability and danger. Is our first assumption to murder the FC (because we expect them to do the same to us)? There is no riskier adventure for either party than to reveal its presence, nature, or interests of one civilization to the other. The very presence of an alien intelligence can have serious ramifications on the progress and character of a civilization. The Orville, Season 2, Episode 5, "All the World is a Birthday Cake," has the crew meet a humanoid race on Regor 2 in the Gamma Velorum system. Regorians' FC with the Planetary Union abruptly ends when two Union officers are arrested because they are Gilia's (wrong birthday). Regor 2 is governed by a race that has taken astrology to the extreme. In that same cool series, Commander Kelly is seen as a Goddess of Healing in Season 1, Episode 12, "*Mad Idolatry*," because she revealed her presence in a technologically infantile and multi-dimensional civilization. Her status throughout later generations caused acts in her name that were hardly defined as healing. (Wiki, 2023)

FC considerations generate questions such as what intelligence is known about the target species? What are the interests of both parties? Why is FC being initiated? How will it be accomplished (safely)? Who goes first? Is communication possible? What will be the long-term influence on both species? And on and on. Nothing will be understandable for both species on FC.

However, War is universal. The only consideration in conflict with another species is scale. We will naturally distrust any non-human civilization. If FC is planned, one side will sortie with force greater than the counterpart to ensure survival and to intimidate a potential rival from future aggression. Sortieing without a preponderance of force would be foolhardy and even risk our civilization's survival. Diplomacy and niceness can come second. Unplanned FC is totally unpredictable. Both civilizations will find any military battle or accidental damage or loss of life difficult to ignore, especially when diplomacy comes into play. (Wright, 2020)

LOGISTICS – SUPPLYING SPACE FORCES

The greatest challenge to any spaceborne force is its maintenance and resupply in DS. Foraging will not be an option. Historically, fielded armies needed to carry things that could not be obtained locally: ammunition, artillery, cooking gear, camp tools, sleeping bags, water, etc. This is not possible in DS. Depending on mission and scale, any space force might be larger than anything humanity has previously needed. Care and feeding of human assault troops, officers, crew, spare parts, and specialized troops to care for the automated forces over vast distances and cruise times border on the unimaginable.

The numbers and types of supplies involved with an armed force of any size go far beyond ammunition (amount, types, crews) and food. Everything an individual soldier might need during the day, including clothing, personal care, camping tools, to body bags, must be planned in detail. Beyond substance, fuel is a major supply issue, as well as oxygen, spare parts, and replacements.

SPACE FORCES OPTIONS

Table 12-3 shows the abbreviated pros and cons of three options for manning a space armada. Further explanation may be found in (Wright, 2020)

TABLE 12-3 Abbreviated Pros And Cons Of Three Different Options For Manning A Space Armada

FORCE	PROS	CONS
Terrestrial – human officers & crew, traditional supply function	Familiarity, Maximum operational flexibility, Maximized Morale, Limited investment, Maximizes ingenuity and adds to survivability, Rapidly adjustable in size, Experienced forces act as success multipliers	Catastrophe is extremely costly, Inefficient compared to automated forces, Frequent resupply, and transfers limit a force's range, Limited by human capacity, rest, boredom, Likely unsuitable for conscription.
HYBRID – Robots, Cyborgs, Exoskeletons, Nanobots, & Humans	Less personnel is required for a full crew complement, Less support is needed than completely human crews, Provides a secondary catastrophic point of failure, Very advanced AI could aid mission completion and combat performance	Eliminates the human element, Malfunctions require more expertise to repair, Malfunctions carry an increased risk of mission-ending failure, Onboard priorities could force crew members to sacrifice themselves for the good of automation.
TOTALLY AUTOMATED – No humans	Completely removes the need for life support and organic supply, Vessels can theoretically operate with minimal rest or refit, Preparation time is limited only by the speed of the industry, Machine-only forces cost considerably less than manned ones, if truly unmanned, Can traverse dangerous areas that manned spacecraft cannot, Advances in AI could mean automated space forces capable of learning from their mistakes and experiences, No human life was lost in a disaster, Reliable onboard systems decrease the chances of failure.	The human element is completely removed, Entirely automated forces are at the mercy of the weakest component reliability, Repair and refit will be difficult to diagnose and respond to, Totally automated forces are completely reliant on command-and-control signals from a distance – a critical vulnerability, Incapable of diplomatic discourse if encountering another sentient species, Complete conquest of a territory unlikely due to local control, Most contingencies must be considered beforehand for programming purposes – another critical vulnerability.

Source: (Wright, 2020)

When you think about the logistics problem, there is no guarantee that the chosen battlefield will possess the minimum requirements to support human life. Any assault force assembled must bring everything needed to support life, including housing. The force must create an environment suitable to human life and breathing conditions. Even if the planet is life-capable and supports respiratory organisms, it cannot *ab initio* be assumed to be compatible with our oxygen-nitrogen atmosphere. So, life support and breathing apparatus will be required. Filtering systems would need to be supplied for every space soldier. Filtering out what? A foreign atmosphere might contain unknown bacteria, hostile organisms, and unknown chemical or radiological substances. This precludes trusting a foreign atmosphere until we are certain the atmosphere is safe.

Breathing is not the only hostile environment. Lifeless balls of gas and rocks circle the suns and moons of some planets. The size of the chosen battlefield may be a serious problem if the target is both hostile to human life and populated with the enemy.

ATMOSPHERIC CONCERNS

A hostile atmosphere will fight the space force. The impact of fighting in a 100% poisonous atmosphere complicates the fighting and necessitates a fully pressurized suit (subject to tears caused by enemy weapons). Every piece of equipment facility and HAZMAT suits will be at risk of contamination, decay, damage, sabotage, or decompression, causing catastrophic support system failure. Local weather – extreme temperature ranges, radiation levels, and winds hinder any assault force. Sleeping, eating, resting, bathroom, and soldiering in a locked pressure suit would make the crowded spaces on a submarine feel like a theme park ride.

GRAVITY

Depending upon its location in the solar system, the target planet or battlefield in question may have significantly different gravity levels than our terrestrial-based forces might be able to endure. Gravity is a function of the distance of a body from other bodies and also a function of its mass. Equation 12-1 gives this relationship.

$$\mathbf{F = G\ [\ m^1 \times m^2 / r^2\ ]} \qquad \mathbf{G = 6.067\ X\ 10^{-11}} \qquad \mathbf{Eq.\ 12\text{-}1}$$

Where: F is the force due to gravity, between two masses (m^1 x m^2), which are a distance r apart; G is the

gravitational constant, N x m^2 / kg^2 ; N= Newtons. A Newton is defined as the force necessary to provide a mass of one kilogram with an acceleration of one meter per second per second.[18]

There is no conceivable limit to gravitational conditions under which a potential non-human sentient rival could evolve. (Wright, 2020)

SPACE DOMINANCE

The concept of Space Dominance (SD) has been studied by military analysts and scientists alike. Both (Szymanski, How to Fight and Win the Coming Space War, 2019) and (Wright, 2020) agree that it refers to a "preponderance of space weapons, vessels, and other space-going instruments of war which enables a localized predominance of military power." (Szymanski, Space Operational Art, and Design (SOAD), 2020) and (Szymanski, Space Warfare Analysis Tools (SWAT) Summary, 2020) goes into serious detail for planning a campaign to create SD and presents tools to measure the logistics, objectives, timing, planning, risk assessment, and battle damage assessments for an SD campaign. [19] Space dominance goes beyond the normal terrestrial or air domain definitions. They seek to *seize the initiative*, *maintain control, and a broad-reaching mandatory objective for space force assault. SD means m*aximizing *both coercive power and control and the ability to deploy forces at the time and place of their choosing.*(Wright, 2020)

The stronger space force in a battle, predominantly in space naval superiority and strength, is the key to space dominance. Space dominance is the first priority. Encircling enemy forces and territory should be a primary activity. It is tactically sound to totally destroy the enemy force in an "all or nothing" engagement in an extremely hostile environment. Space Dominance should be thought of as a game of GO,[20] NOT chess. In the former, the opponent aims to encircle (strangle) the opponent and deny him his strategic maneuver capability; in the latter, the opponent aims to completely deprive him of individual pieces (assets) or prevent defensive movement so that he can slaughter his ruler (king). (Wright, 2020)

SPACECRAFT CARRIER

Hollywood thinks space combat will mirror naval combat in terrestrial terms. Further, that opposing fleets will clobber each other from a distance, and at the center of their strategies are Spacecraft Carriers. The analogous Spacecraft Carrier battle group to a naval aircraft carrier group is that both require adequate defenses by concentric layers of other naval vessels to maximize the delivery punch of the Carrier. They depend upon other air or space defense vessels and escort capital ships and submarines to find, track, and destroy adversary air and underwater threats. We don't know what the equivalent submarine would be in space. Carrier-based fighters and bombers could be leveraged to deliver large weapons payloads to enemy fleets. Because of gravity and the weightless environment, there is a special payoff in space. Strike craft are not limited by wing length,

fuel considerations beyond target range, or bomb load except spaced on the craft. Newton's Laws of Motion favor the strike craft because of limited inertial counterforce acting on the craft. (Wright, 2020)

TARGETING AND PRIORITIES

The final topic of this chapter deals with targeting. What or how do we prioritize space targets? Targets are selected first for their strategic effect/value. (USJCS, 2023) Operation Desert Storm in 1991 provides a useful case for the study of target selection. USAF Colonel Edward C. Mann III describes the options. (III, 1995)

OPTION 1 – Equal Value

The first option is to attack targets in a series with no regard for their individual value. The strategic result is a sum of the targets destroyed. The planner needs only to focus on the level of destruction required for each target, then select the best weapon and delivery system available to insure a high probability of destruction. The target order is not important. (III, 1995)[21]

OPTION 2 – Value

A second option is to assess targets based on their strategic or tactical value. Determining the strategic or tactical results when they are destroyed is possible based on a weighted scale. Targets are assigned a value based on priority, with higher-valued targets being destroyed sooner increasing the impact on the enemy for a longer period. This approach is still serial targeting if the targets are destroyed sequentially rather than simultaneously. (III, 1995)

OPTION 3 – *Instant Thunder*

Developed by USAF Colonel John Warden called *Instant Thunder* is termed exponential strategic impact targeting. (III, 1995) By attacking multiple specific targets against key enemy installations or systems simultaneously, planners seek to induce a "catastrophic failure" rather than waiting for progressive system failures under the serial targeting scheme. If successful, the effect is to induce "*strategic paralysis*." (III, 1995) Instant Thunder [22] simultaneous strikes in Iraq on communications, power generation, and command and control facilities blinded Iraqi leadership to the battlefield realities and temporarily paralyzed Iraqi decision-making. Further strikes induced panic, fear, and hopelessness in Iraqi leadership and fielded forces. (III, 1995)

OPTION 3 could be used effectively in interstellar and interplanetary deep space warfare to destroy all targets strategically important and cause strategic paralysis of the enemy.

CONCLUSIONS

While we do not know yet how the U.S. approach to space and space warfare will take over the next two-five decades, we do know one thing to be true: space combat is coming, as is space mining, exploration, lunar and interplanetary settlements, and possibly First Contact. Only two nations appear capable of reaching this goal; The United States and the People's Republic of China. These countries have different governments, policies,

economics, innovation capabilities, and values. Their approaches to Space Dominance are NOT collaborative. Our first space warfare may be with existing terrestrial competitors.

REFERENCES

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

Anonymous. (2023, February 15). *1 Mile Swim Times: Swimming Standards By Age and Ability.* Retrieved from swimminglevel.com: www.swimminglevel,com

Anonymous. (2023, February 15). *Would a Corpse decay in space?* Retrieved from space: www.sciencefocus.com

Clausewitz, C. v. (2003). *Principles of War.* NY: Dover Publications.

Drake, F. (2023). *Drake Equation.* Retrieved from Wiki: https://en.wikipedia.org/wiki/Drake_equation

Gustaf Kilander. (2023, February 4). *US Shoots down suspected Chinese Spy Balloon over Atlantic Ocean.* Retrieved from Independent: independent.co.uk.com

III, E. C. (1995). *Thunder and Lightening: Desert Storm and the Airpower Debates.* Maxwell AFB, AL: Air University Press.

Nichols, Carter, Diebold, Drew, Farcot, Hood, & Jackson, J. J. (2023). *Cyber Human Systems, Space Technologies, and Threats.* Manhattan: NPP # TBA.

Nichols, R. &. (2022). Space Electronic Warfare, Jamming Spoofing, and ECD. In R. Nichols, & e. al, *Space Systems: Emerging Technologies and Operations* (pp. 112 – 232). Manhattan, KS: New Prairie Press #47.

Nichols, R. K. (2017, October 4). DRONE WARS THREATS, VULNERABILITIES, AND HOSTILE USE of UAS. *Presentation at WSU Technology Symposium, Rev 15A*. Wichita, KS, USA.

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

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

Nichols, R. K., & 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. (2022). *Space Systems: Emerging Technologies and Operations.* Manhattan, KS: New Prairie Press # 47.

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

Paul Best. (2023, February 13). *Chinese surveillance balloons have been detected over the Middle East.* Retrieved from Fox News Digital: fox.com

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

Saikia, R. (2023, Feb 18). *The Elusive Universe: The Hunt for Dark Energy and Dark Matter Continues.* Retrieved from https://www.linkedin.com/: https://www.linkedin.com/feed/update/urn:li:activity:7032779998088376321/

Szymanski, P. (2019). *How to Fight and Win the Coming Space War.* Retrieved from https://satellitewarcom-my.sharepoint.com/: https://satellitewarcom-my.sharepoint.com/personal/paul_szymanski_satellitewar_com/_layouts/15/onedrive.aspx?id=%2Fpersonal%2Fpaul%5Fszymanski%5Fsatellitewar%5Fcom%2FDocuments%2FPrime%20Briefs%2FHow%20to%20Fight%20and%20Win%20the%20Coming%20Space%20War%20

Szymanski, P. (2020, Jan 27). *Space Operational Art and Design (SOAD).* Retrieved from https://www.dropbox.com: https://www.dropbox.com/s/9jlrjxgbigm7lsv/Space%20Operational%20Art%20and%20Design%20(SOAD)%20-%202020-01-27.xlsx?dl=0

Szymanski, P. (2020, Feb 7). *Space Warfare Analysis Tools (SWAT) Summary.* Retrieved from https://satellitewarcom-my.sharepoint.com/: https://satellitewarcom-my.sharepoint.com/:p:/g/personal/paul_szymanski_satellitewar_com/EYdnXVqvalxPjR6hzOp-C60B9ujGIyIWXtRHWn-5mwaJsw?rtime=Aoc78-sP20g

Tzu, S. (2006). *The Art of War.* Washington, DC: Holden-Crowther Organization for Asian Studies, Filiquariam Publishing, LLC.

USA, J. C. (2020). *Joint Publication 5-0, "Joint Planning" Doctrine.* Washington: JCS.

USAF. (2003). *USAF Search and Rescue Survival Training USAF AFR 64-4.* NYC: Barnes & Noble.

USJCS. (2023, February 20). *Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/.* Retrieved from www.jcs.mil/: https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/

What is Deep Space? (2023, February 2). Retrieved from Wikipedia: https://www.quora.com>what's the difference between 'space,' 'outer space, 'deep space

Wiki. (2023, February 14). *Law_of_salvage.* Retrieved from Wiki: https://en.wikipedia.org/wiki/Law_of_salvage

Wiki. (2023, February 15). *Outer Space.* Retrieved from Wiki: https://en.m.wikipedia.org

Wiki. (2023, February 14). *Outer_Space_Treaty.* Retrieved from Wiki: https://en.wikipedia.org/wiki/Outer_Space_Treaty

Wiki. (2023). *The Orville Season 1, Episode 12, The World is a Birthday Cake, and Season 2, Episode 5, Mad Idolatry.* Retrieved from Wiki: wikipedia.com

Wright, J. C. (2020). *Deep Space Warfare: Military Strategy Beyond Orbit.* Jefferson, NC: McFarland & Company.

ENDNOTES

[1] To add insult to injury, The Chinese only public statement was that they wanted their balloon back.

[2] AIM-9x missiles cost $400,000 and are super accurate.

[3] It is unscientific and unsound to strategically assume we are the only sentient species in the universe. Rather than not plan, it is at least prudent to consider the real biological possibilities of encountering another space-traveling species.

[4] A "state" can mean a country, a government, or a political authority. It means absolute control over a fixed territory on Earth.

[5] Except maybe Drake's 340.

[6] MOB = Man Overboard – a very serious situation for a Captain,

[7] For MOB, the boat leaves (especially a capital ship). For the deserter, he is trying to escape security forces which might put a few holes in his buoyancy ability. A far worse situation would be a child whose survival would be imperiled from the minute he/she entered the water.

[8] How many MOB cases have exposure suits before they go over the railing?

[9] POV = Point of View

[10] Ye author is a licensed Captain of a moderate power cruiser 38′. Many issues (supply, water, mechanical, repairs, safety of passengers, navigation accuracy, communications, food, training, EPIRB, lights, refrigeration, logging, sonar, radar, waste removal, entertainment, and security) are all the responsibility of the Captain. We cruise a known body of water, the Chesapeake. The depths are known, and the entire Bay has been mapped: NOAA Map 12270, Chesapeake Bay Eastern Bay, and South River. Ye author has also captained a sailboat. So, the environment is controlled, and crew capabilities are known on defined voyages. This is tiny responsibility compared to a Captain of a spaceborne capital vessel.

[11] Dr. Szymanski's linked profile is: www.linkedin.com/in/PaulSzymanski

[12] The author would love to take a class Dr. Szymanski and Major Wright taught. What a pair of brilliant visionaries they are.

[13] Dr. Szymanski was part of the decision team under USJCS to establish the US Space Command.

[14] The International Space Station is 254 miles above Earth. The Geostationary orbits (GEO) are used for

TV and communication satellites and cover most of the Earth at 22,223 miles. It is assumed that the edge of Szymanski's vision stops (for purposes of Table 12-2) at the edge of the GEO range and covers everything to the Earth's surface.

[15] Venus is 38 million miles from its closest neighbor Earth. Jupiter is 778,600,000 miles from Earth. Neptune is 2 Billion miles from Earth. Our Sun is 93 million miles from Earth. Astronomers have found a gas giant planet OGLE-2014-BLG-0124L at 13,000 light-years from Earth. 1 light-year = 5.879 x 1012 miles!

[16] TT & C = Tracking, Telemetry, and Control.

[17] This was the famed tactic of CSA Gen Andrew "Stonewall" Jackson. On May 5, 1863, his most famous maneuvering was to defeat Northern General Hooker's Army by a long flanking march to surprise and defeat Hooker's right during the Chancellorsville Campaign. Unfortunately, Jackson's units became jumbled because of the Wilderness underbrush and terrain. Jackson was shot by friendly fire and died from complications of amputation and pneumonia on May 10. He was known as a superb commander for execution with elements of speed, maneuver, initiative, audacity, and singleness of purpose and determination.

[18] A simple way to think of Newton is the force of Earth's gravity on an apple with a mass of about 102.0 grams. 5 apples = 5 Newtons. It gets more complicated when we leave Earth's gravitational pull because we deal with vectors (accelerating masses each in a specific direction).

[19] Dr. Szymanski's space warfare work and experience are extensive, much CLASSIFIED, and brilliant efforts for the OPEN-Source materials delivered. He teaches courses and consults for the DoD and USJCS. His profile is on Linkedin. Most of his work is beyond the scope of this introductory chapter.

[20] AKA wei qi or baduk in Chinese and Korean, respectively.

[21] This is known as serial targeting or one-by-one destroying targets.

[22] Also called "shock and awe."

PART III

PART 3: WARFARE, HYPERSONICS, AND MATERIALS

13.

PROGRESS IN HYPERSONICS MISSILES AND SPACE DEFENSE [SLOFER]

STUDENT OBJECTIVES

- Understand how advancements in different disciplines, such as metallurgy, semiconductors, and Artificial Intelligence, are being used to improve existing challenges in hypersonic technology.
- Obtain an appreciation for tactical and strategic concerns associated with advancements in hypersonic technology.
- Gain an appreciation of the technical considerations to create such weapons and a greater appreciation for the science and how the facts measure up to the challenges of the hype.
- How such weapons require changes to existing strategies

OVERVIEW

From the sword to the rocket, weapons have played a crucial role in warfare and conflict throughout history. Their continued evolution has often been driven by the need to gain an advantage over one's enemies or develop countermeasures to protect and create a balance of power that could potentially deter a preemptive strike from one's adversaries because of the retaliatory consequences.

Over the past decade, numerous advancements in many scientific disciplines have created more sophisticated weapons, which require more sophisticated defense systems and a different way to view offensive and defensive strategies. As illustrated in

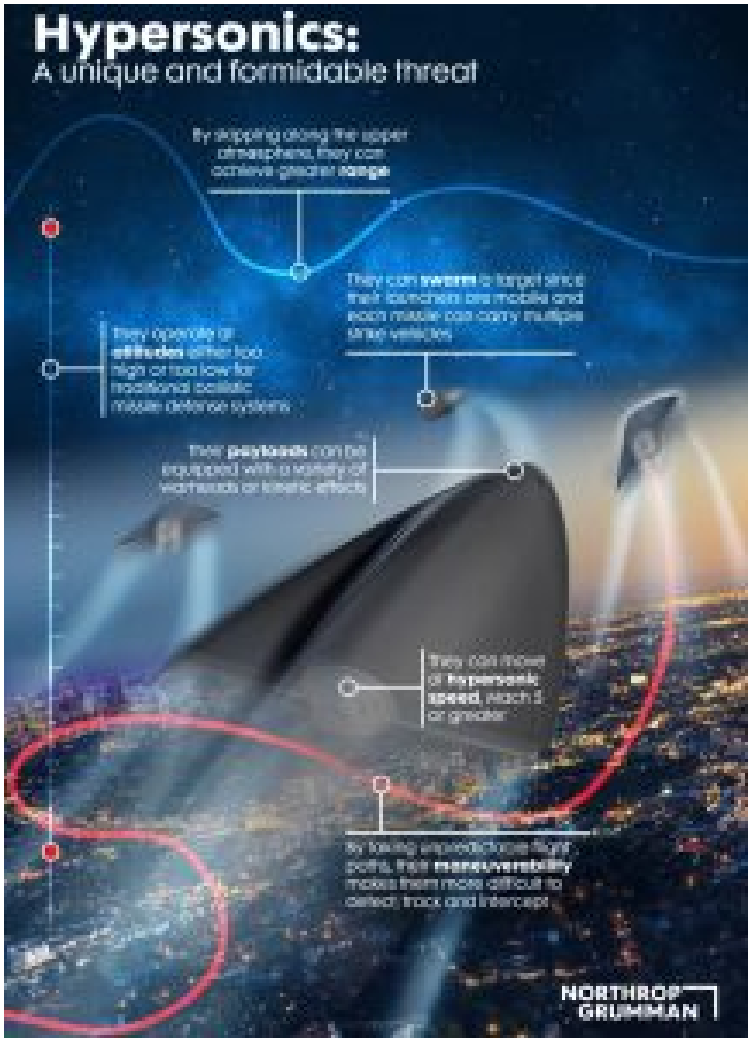
Book 6 – Drone Delivery of CBRNECy – DEW Weapons WMDD (Nichols, et al., 2022)

Book 7 – Space Systems – Emerging Technologies and Operations (Nichols, et al., 2022)

the same has proven true with the evolution of rocketry, which has led to the development of hypersonic missiles, now traveling faster than five or more times the speed of sound (Mach 5+), which is the minimum for Hypersonics. This technology is considered a game changer because of its speed and maneuverability. In addition, such weapons have changed the detection paradigm since they do not follow the anticipated launch signatures or flight characteristics of Inter-Continental Ballistic Missiles (ICBM), which most defense systems are calibrated to defend against. This, therefore, makes existing systems obsolete and causes delays in the observation/detection phase and, therefore, reducing the time for Observation, Orientation, Decide, and Act

processes, also known as the OODA Loop, a methodology allowing commanders and political leadership to make decisions in a quickly changing situations and act upon them.

Figure 13-1
Hypersonic Weapons, An Enviable Asset Or Formable Foe



Source: (Northrop Grumman, 2023)

This chapter will provide an overview of some advancements in the areas of semi-conductor, Real-Time-Operating-Systems (RTOS, Artificial Intelligence, metallurgy, airframe construction, and improved Guidance Systems, along with cooling technology and how improvements in the individual disciplines can lead to the advancement of more lethal hypersonic weapon systems.

THE SPEED SPECTRUM

This evolution of hypersonic weaponry is changing how weapon delivery systems are created, launched, controlled, detected, and defended against. This technology will alter how technicians, strategists, and diplomats view their existing doctrines, policies, and strategies and the navigating the complexities of revising offensive and defensive approaches necessary to address this disruptive technology.

To appreciate the concept of hypersonic speed, it is necessary to understand various parts of the speed spectrum and how they relate to the speed of sound. Two reasonably common examples of speed notation are:

- 1) **The speed of light** or light-speed, indicated by light-years or approximately 670,616,629 miles per hour in a vacuum (NASA, 2019)
- 2) **The speed of sound**, which is denoted as Mach speed.

These short-hand notations identify an object's speed between any two points. Mach 1 will be the baseline for the speed of sound calculated by the formula.

Vs – 643.855 x (T/273.15)0.5 Eq 13-1

Where:

Vs = Velocity of Sound (Knots)

T = temperature (Kelvin)

643.855 = Calculated speed of sound (N.O.A.A., (n.d.))

In general terms, "On Earth, the speed of sound at sea level — assuming an air temperature of 59 degrees Fahrenheit (15 degrees Celsius) — is 761.2 mph (1,225 km/h)." (Science Daily, 2021)

The generally accepted sonic spectrums are divided into Subsonic, Supersonic, and Hypersonic for aeronautical use. To provide additional perspective, the table below identifies types of aircraft that operate within the various parts of the sonic spectrum and the approximate speed ranges:

Table 13-1
Comparison Of The Various Aircraft And Speed Ranges In The Sound Spectrum

Category	Aircraft type	Approx. speed (mph)	Mach
Subsonic	Helicopters, General Aviation, and generally Commercial aircraft	0 – 580	N/A
Supersonic	Fighter jets	1,453 – 2,500	Mach 2.5+
Hypersonic	X-15, Space Shuttle, and manned space capsules (on reentry)	3,806 - 17,500+	Mach 5 - Mach 25+

Sources: (Aero Corner , 2021) (Smithsonian National Air and Space Museum, 2022)

Sources: (Aero Corner , 2021) (Smithsonian National Air and Space Museum, 2022)

TIME IS EVERYTHING

Weapons operating in the Hypersonic realm have the advantage of speed which can be an asset if used as a preemptive or first-strike weapon in which the weapon will have arrived on target before the opposition can respond. Likewise, if used as a retaliatory response, the aggressor may need to be more capable of adequately defending against a counterstrike. For example, if we use the below table, a Hypersonic Missile traveling at Mach 8 can reach a target 1000 miles away in approximately 9.85 minutes. The same Mach 8 missile fired at an aircraft carrier from a plane, ship, or shore point at a range of 200 miles could reach its target in less than 2 minutes (1.97). This virtually eliminates any reaction time for the command and crew of a ship to react to the attack.

Table 13-2
HYPERSONIC SPEEDS AND THE TIME TO COVER 1000 MILES TO A TARGET

Mach Speed	Miles/Hr.	Miles/ Sec.	Travel time 1K miles (min.)	Mach Speed	Miles/Hr.	Miles/ Sec.	Travel time 1K miles (min.)
1	761.20	0.21	78.82	16	12,179.20	3.38	4.93
2	1,522.40	0.42	39.41	17	12,940.40	3.59	4.64
3	2,283.60	0.63	26.27	18	13,701.60	3.81	4.38
4	3,044.80	0.85	19.71	19	14,462.80	4.02	4.15
5	3,806.00	1.06	15.76	20	15,224.00	4.23	0.25
6	4,567.20	1.27	13.14	21	15,985.20	4.44	0.27
7	5,328.40	1.48	11.26	22	16,746.40	4.65	0.28
8	6,089.60	1.69	9.85	23	17,507.60	4.86	0.29
9	6,850.80	1.90	8.76	24	18,268.80	5.07	0.30
10	7,612.00	2.11	7.88	25	19,030.00	5.29	0.32
11	8,373.20	2.33	7.17	26	19,791.20	5.50	0.33
12	9,134.40	2.54	6.57	27	20,552.40	5.71	0.34
13	9,895.60	2.75	6.06	28	21,313.60	5.92	0.36
14	10,656.80	2.96	5.63	29	22,074.80	6.13	0.37
15	11,418.00	3.17	5.25	30	22,836.00	6.34	0.02

Adapted from: (Drone Delivery of CBNRECy, 2022)

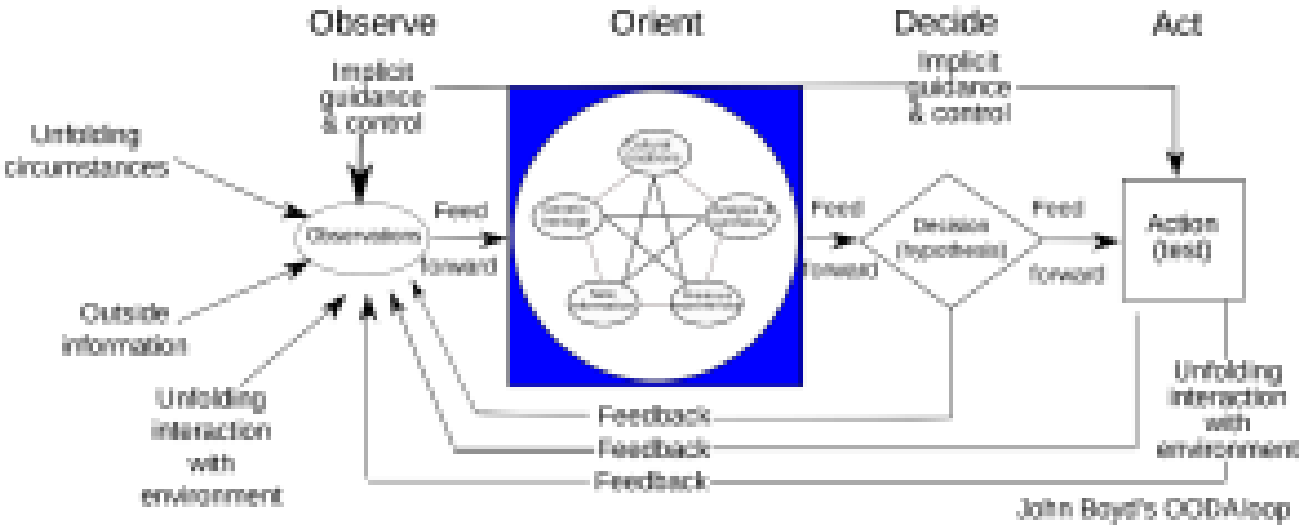
Adapted from: (Drone Delivery of CBNRECy, 2022)

Time is the critical component, and as eloquently stated by Michael E White from the Office of the Undersecretary of Defense for Research and Engineering, "...the adversaries have increasingly focused on systems that dramatically compress the timelines and the timescale of a tactical battlefield. These systems — including ballistic missiles, ballistic missiles with maneuvering reentry vehicles, and vehicles that are increasingly hypersonic in nature — give adversaries the ability to hold our forces at risk from hundreds, even thousands, of miles away, with flight times that are measured in minutes." (Cronk, 2021).

As previously noted, a hypersonic missile traveling at Mach 8 can cover 1000 miles in less than 10 minutes. This leaves Command and Control little time to make a defensive countermeasure or counter-strike determination and implement/act on it. This extreme speed and the vast distance can be covered quickly, reducing the time needed to follow a process such as the Observe, Orient, Decide, Act (OODA) loop used for decision-making. Unfortunately, the defender will lose significant time at the beginning of the process,

where those under siege will spend critical time observing and attempting to orient themselves to the unfolding situation. This time absorption will severely reduce the defender's time to decide and act. It also infers that it will be necessary to recalibrate the cycle, which will also require time. The revised cycle will operate within an even more compressed loop, thus becoming a vicious cycle and a logistical nightmare for anyone attempting to defend against such an event.

Figure 13-2
The Observe. Orient. Decide. Act-Loop



Sourced from: (Wikipedia, 2003)

Technology, processes, and methodologies currently associated with a U.S. Inter-Continental Ballistic Missiles decision to launch reportedly require between 17-20 minutes from detection to launch decision (Blair, 2019). However, a hypersonic vehicle traveling at Mach 8 could have traveled approximately 1,725-2,030 miles by the time a decision was made. Assuming a first or preemptive strike situation, the missile speed has effectively reduced the time in the observation and orientation phases of the OODA loop. Likewise, defenders or opposing forces want technology that would provide early detection/observation capabilities and adequate, if not superior, countermeasures to provide a defense and enable an effective retaliatory strike capability to discourage a preemptive action.

Currently, multiple countries boast of having hypersonic-type weapons in their arsenal or are in a near-ready state.

Table 13-3
LIST OF COUNTRIES WITH ALLEGED HYPERSONIC DEVICES AND WITH ACCLAIMED SPEEDS AND DISTANCES

Country	Reported Vehicle	Claimed Mach Speed	Claimed range mi/km	Citations
Brazil	X-14	06.0	120 / 200	(Força Aerea Brasileira, 2021)
China	DF-17	10.0	1553 / 2500	(CSIS , 2021)
India	Shaurya	07.5	733 / 1180	(Military-Today, n.d.)
	Brahmos II	05.0	310 / 500	(CSIS, 2021)
North Korea	Hwasong 8	05.0	1988 / 3200	(Military-Today, n.d.)
Russia	Avangard (HGV)	20.0	3728 / 6000	(Nilsen, 2021)
	3M22 Zircon/Tsyrkon	07.0	621 / 1000	(Military-Today, n.d.)
USA	X-51A Waverider	05.0	460 / 724	(USAF, n.d.)

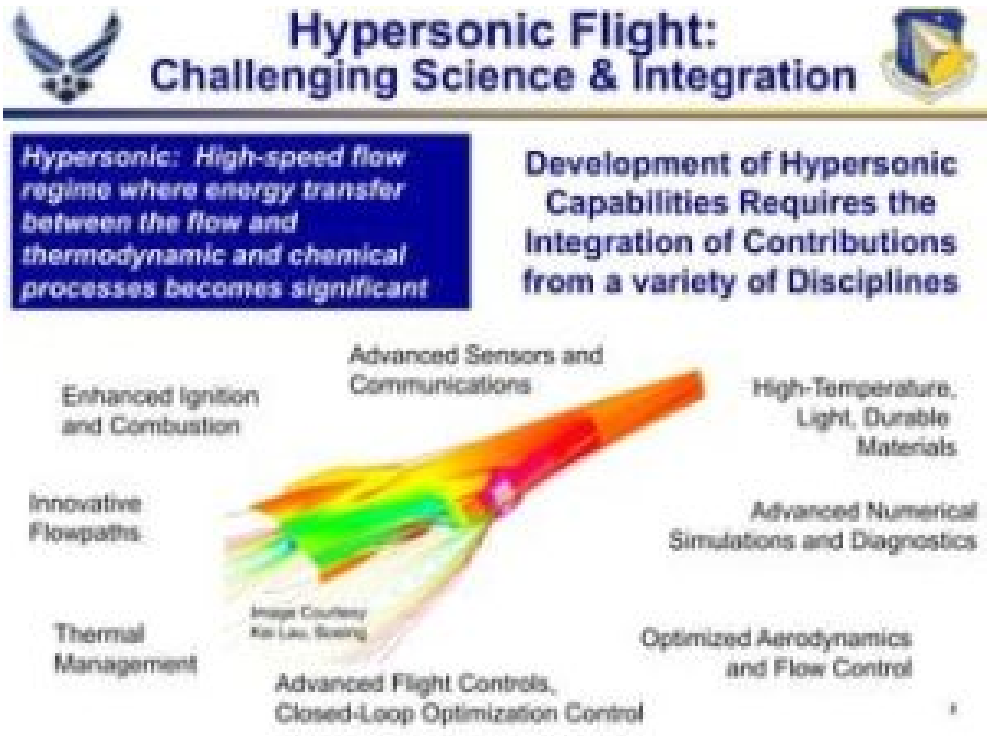
Note. The information is based on claims and may not be fieldable devices or have acclaimed speeds and distances.

Note. The information is based on claims and may not be fieldable devices or have acclaimed speeds and distances.

To continue developing weapons capable of faster hypersonic speeds than currently boasted comes with challenges and a price. Achieving these claims requires new technologies that must span multiple scientific disciplines.

Source: Author

Figure 13-3
Scientific Challenges Associated With Hypersonic Flight



Sourced from: (USAF Office of Scientific Research, 2011)

However, although numerous known technical difficulties are associated with creating a deployable weapon that meets the many boasted speeds and ranges, technical advancements in multiple fields of science are pushing today's myths and hype closer to reality. To appreciate the technological accomplishments, it is essential to understand the physiological and technological challenges and the complexities associated with faster hypersonic speeds.

PHYSICAL FORCES AND THE HUMANS

Unlike supersonic spy planes such as the SR-71, which carried a human pilot, hypersonic aircraft capabilities have exceeded human physiology's bounds due to the natural forces that occur at high-speed maneuvers. For example, G-force, short for gravitational force, is a measure of acceleration experienced by an object or person relative to gravitational pull and is commonly expressed in units of "G" which is equivalent to acceleration due to gravity (approximately 9.8 meters per second squared or 32.2 feet per second squared on Earth). G-forces can also be experienced during aviation maneuvers, space travel, cars, or amusement park rides. In these cases, the acceleration forces can be exerted in various directions, including vertical, lateral, or longitudinal, depending on the specific motion. The force's strength depended on the turn rate and the object's speed. Turns that require higher speeds and sharper turns will experience higher G-forces produced by centrifugal

force caused by the inertia of the object(s) trying to maintain a straight line while being forced into a turn. The following is a simple calculation to illustrate G-force changes based on changes in the objects speed:

$$g\text{-force} = (v^2 / (r * g)) + 1 \qquad \text{Eq. 13-2}$$

Where:

v is the velocity of the aircraft (in meters per second).

r is the radius of the turn (in meters).

g is the acceleration due to gravity (approximately 9.8 m/s^2)

Source: Derived from Newton's second law of motion and circular motion principles and centripetal acceleration.

Table 13-4
G-Force Comparison

Radius of turn (feet / meters)	15,840	4,828.03	equals 3 miles
Gravity ((f/s) / (m/s))	32	9.8	

Velocities			
Mach	**miles / hr**	**meters / sec**	**g-force**
0.5	380.5	170.1	1.6
1	761.2	340.3	3.4
2	1,522.4	680.6	10.8
5	3,806.0	1,701.4	62.2
10	7,612.0	3,402.8	245.7
15	11,418.0	5,104.2	551.6
20	15,224.0	6,805.5	979.9

Note: The table compares G-forces on the same object executing a turn within the same radius but at different speeds.

Note: The table compares G-forces on the same object executing a turn within the same radius but at different speeds.

The stress of g-forces on hypersonic vehicle structures increases astronomically with speed and as the turn rates increase. The same applies to the human body, where high G-forces can produce discomfort and, if maintained or increased, can result in severe physiological consequences and even death. This typically occurs when individuals are exposed to sustained G-forces greater than 4 to 7 Gs. It is important to note that "...fighter pilots often are exposed to higher G-forces of about 8 or 9 because of specialized G-suits and proper diet and hydration." (Venose, 2016). However, even such professionals will begin experiencing a loss of consciousness or G-LOC, resulting from blood being forced away from the brain and towards the lower extremities. If sustained for a prolonged period, it can result in brain damage and even death. If we reference the previous chart, a pilot initiating a turn at Mach 2 will experience 10.8 Gs,' but the same turn at Mach 5 would result in 62.2 Gs. This makes the human pilot a weak link in a situation where a hypersonic vehicle traveling at Mach 5+ was forced to take evasive actions. Execution of the evasion actions at that speed would almost certainly result in a death sentence for the pilot. This is a strong reason for most future military designs based on uncrewed vehicles. Therefore, the remainder of the chapter will focus on autonomous or remote-piloted vehicles.

Please note that the information in the Hypersonic speed and G-force comparison charts will be helpful as we continue to discuss hypersonic hype and improvements related to surface friction, structural integrity, and other areas.

AERODYNAMIC DRAG

Aerodynamic drag, or air resistance, refers to the force that opposes the motion of an object through the air (or a fluid). When an object moves through the air, it experiences resistance due to the collision of air molecules with its surface. This drag or resistance is influenced by several factors, including:

Shape: The shape of an object plays a significant role in determining the amount of drag it experiences. Streamlined objects or aerodynamic shapes, such as airplanes or race cars, are designed to minimize drag by reducing the frontal area and promoting smooth airflow around the object.

Surface roughness: Surface roughness can increase drag by creating turbulence and disrupting the smooth flow of air around an object. Smoother surfaces reduce drag by allowing air to flow more smoothly.

Velocity: The speed at which an object moves through the air affects the amount of drag it experiences. Drag increases with the square of the velocity, which means that doubling the speed of an object quadruples the drag force acting on it.

Air density: The density of the air also affects drag. Higher air density increases the number of air molecules colliding with the object's surface, resulting in more significant drag. As Hypersonic missiles move into the lower levels of the atmosphere, the air becomes denser and increases the amount of drag (as well as lift).

Viscosity: The viscosity of the air, or its resistance to flow, also influences drag. Higher viscosity leads to increased drag due to the stickiness of the air molecules.

Aerodynamic drag can be quantified using the drag coefficient (Cd), a dimensionless value representing the

object's aerodynamic efficiency. The drag force (Fd) acting on an object can be calculated using the following equation:

Fd = (1/2) * Cd * ρ * A * V^2 Eq. 13-3

Where:

Fd = is the drag force.

Cd = is the drag coefficient.

ρ (rho) = is the air density.

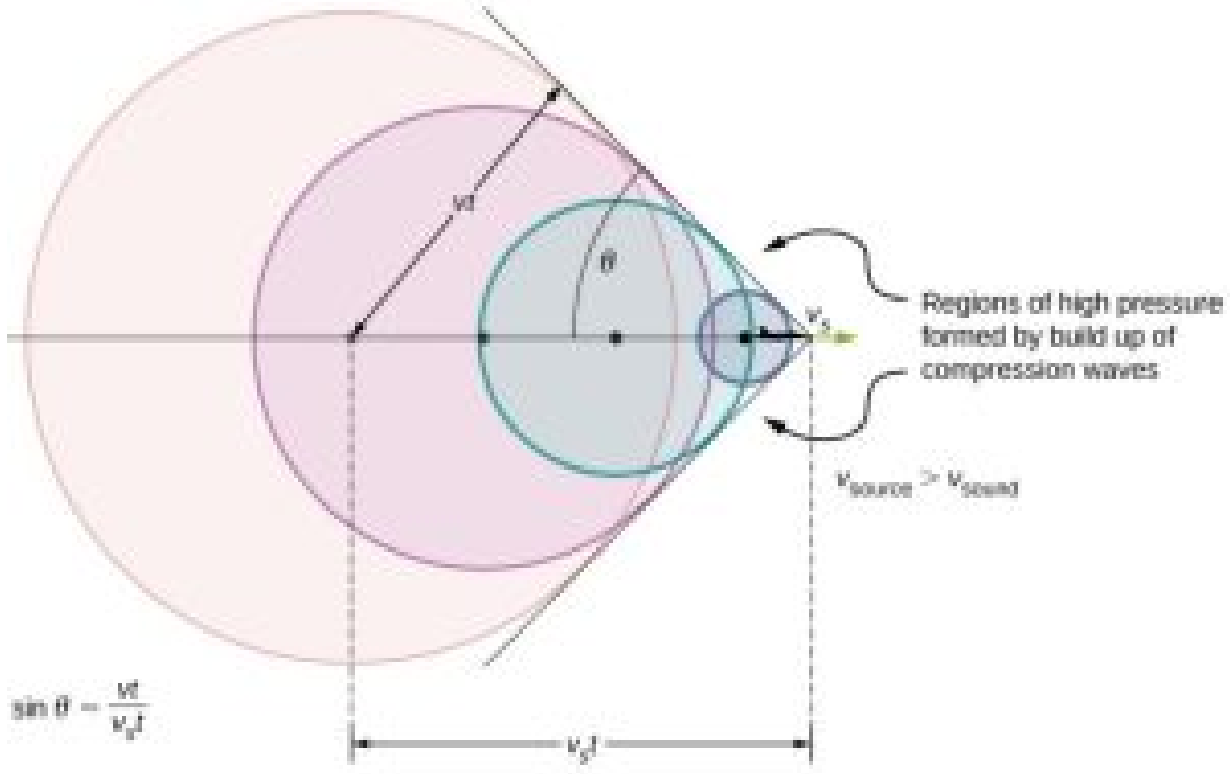
A = is the reference area (usually the frontal area) of the object.

V = is the velocity of the object relative to the air.

Source: (Drag Coefficient, n.d.)

At hypersonic speeds, aerodynamic drag becomes even more significant. It can substantially impact the performance of objects moving through the atmosphere and create additional forces such as "Wave Drag" and "bow shock waves," which are forms of drag that occur at high speeds when an object moves faster than the waves it creates in the surrounding air. Due to the high speeds involved, Shock waves play a significant role in hypersonic flows. By its nature, the shock wave is a compression wave that forms when an object moves through a fluid (such as air) faster than the speed of sound in that medium.

Figure 13-4
Shock And Compression Waves



Where:

t = time

s = source

v = velocity

Note: "Sound waves from a source that moves faster than the speed of sound spread spherically from the point where they are emitted, but the source moves ahead of each wave. Constructive interference along the lines shown (actually a cone in three dimensions) creates a shock wave called a sonic boom. The faster the speed of the source, the smaller the angle θ". (Lumen Learning, 2018)." .

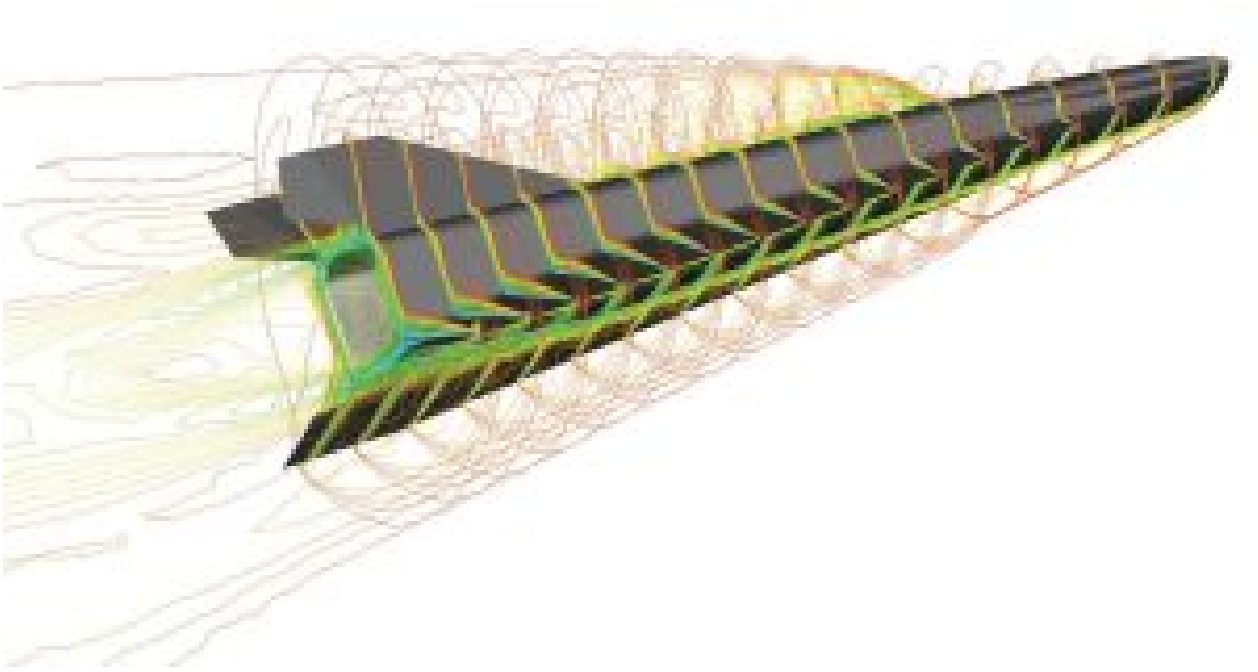
Sourced from: https://s3-us-west-2.amazonaws.com/courses-images/wp-content/uploads/sites/2952/2018/01/31201658/CNX_UPhysics_17_08_SBoom.jpg

When an object travels at hypersonic speeds, it generates a bow shock wave in front of it. This bow shock wave is a curved shock wave that forms as the object's leading edge compresses the air ahead of it and marks the boundary between the supersonic flow ahead of the object and the compressed, subsonic flow around it.

Behind the bow shock wave exists a compressed air region called the shock layer or shock wave boundary layer. This region experiences high temperatures and pressures due to the compression caused by the shock wave. The shock layer is characterized by sudden air density, temperature, and pressure increase.

In addition to the bow shock wave, hypersonic flight can also produce other shock waves depending on the shape and characteristics of the object. For example, if the object has sharp leading edges or prominent features, additional shock waves called detached shocks, or compression shocks can form at those locations.

Figure 13-5
Shock And Compression Waves



Note: "Passing the speed of sound compresses air flowing over an airfoil, creating a shockwave.- the "sonic boom" Waveriders use the shockwave to increase their lift, essentially surfing on a wave of pressurized air." " (U.S. Naval Institute, 2020)

Sourced from: https://www.usni.org/magazines/proceedings/2020/december/hypersonic-missiles-coming-hot

The presence of shock waves in hypersonic flight has several implications. First, shock waves contribute to thermodynamic heating, primarily caused by converting the object's kinetic energy into thermal energy as it pushes through the air. As the object moves faster than the speed of sound, it compresses the air in front of it, increasing air pressure and temperature. As the object's speed increases, this compression-heating effect becomes more pronounced.

The process of thermodynamic heating involves several factors:

Compressibility: At hypersonic speeds, the compressibility of the air becomes significant because the air cannot respond instantaneously to changes in pressure, resulting in local increases in temperature. This compression heating is related to the adiabatic heating of the gas as it is compressed.

Frictional Heating: The interaction between the object and the surrounding air generates frictional forces. These forces convert kinetic energy into thermal energy, leading to further heating. The heat generated by friction depends on the object's surface properties, such as its roughness and material composition, as well as the density of the material being traveled through, in this case, air.

Shock Wave Heating: Shock waves form when objects move at hypersonic speeds. These shock waves compress the air and create high-pressure and temperature regions, contributing to the object's overall thermodynamic heating.

The high temperatures resulting from the thermodynamics of heating created by hypersonic flight pose significant challenges to the design and materials used in and on such vehicles. For example, extreme heat can cause structural deformation, material degradation, comprise electronic components, and cause thermal stresses. Therefore, advanced materials, such as ceramics and Thermal Protection Systems (TPS), are often used to manage and dissipate heat, protecting the vehicle's structure. The following are some broad temperature ranges. Please note that these ranges will change based on vehicle design and other conditions:

Low Hypersonic Speeds (Mach 5 to Mach 7): At these speeds, the temperatures experienced can range from approximately 900°C to 1,500°C (1,650°F to 2,730°F). This range represents the compression heating and frictional heating effects caused by the object's interaction with the air.

Intermediate Hypersonic Speeds (Mach 7 to Mach 12): In this speed range, due to increased compression and frictional heating, temperatures can range from approximately 1,500°C to 2,500°C (2,730°F to 4,530°F). These temperatures are more demanding on coverings materials and airframes of hypersonic vehicles' and their thermal protection systems.

High Hypersonic Speeds (Mach 12 and above): At very high hypersonic speeds, temperatures can exceed 2,500°C (4,530°F) and can potentially reach up to 3,000°C (5,432°F) or even higher. The specific temperatures depend on the vehicle's design and the effectiveness of its thermal protection systems.

To help illustrate the heat intensity generated at these speeds, the following table provides the melting temperatures of various metals to act as a general reference to illustrate the heat generated by a hypersonic thermal activity.

Table 13-5
Melting temperatures of some common elements

Atomic #	Element	Melting Point (°C)	Melting Point (°F)
78	Platinum	1,768°C	3,214.90°F
26	Iron	1,538.00°C	2,800.00°F
28	Nickel	1,453.00°C	2,651.00°F
29	Copper	1,084.62°C	1,984.32°F
79	Gold	1,064.18°C	1,947.52°F
47	Silver	961.78°C	1,763.20°F
13	Aluminum	660.32 °C	1,220.58°F
12	Magnesium	650 °C	1,202.00°F
30	Zinc	419.53 °C	787.15°F
82	Lead	327.46°C	621.43°F
50	Tin	231.93°C	449.47°F

Source: (American Element, 2022)

Source: (American Element, 2022)

In addition to heating, shock waves can lead to increased drag and aerodynamic forces, affecting the vehicle's stability and control, which can also cause fluctuations in the aerodynamic forces and induce vibrations or buffeting, which must be carefully considered in the vehicle's design.

ADVANCEMENTS IN METALLURGY AND HEAT DISSIPATING MATERIALS

The thermodynamics introduced by compressibility, frictional drag, and shock wave heating occurring at hypersonic speeds make it imperative that hypersonic missiles be made from materials that can withstand the extreme heat and pressure generated by their extraordinary speeds. Recent advancements in materials science have led to the development of new compounds and compositions that can withstand many of these conditions. Over the past decade, there have been advancements in:

Carbon-Carbon Composite: Carbon-carbon composites are carbon fibers embedded in a carbon matrix.

They possess excellent thermal stability and can withstand temperatures up to 3,000 degrees Celsius (5,432 °F). These composites are lightweight, strong, and commonly used in aerospace applications.

Ceramic Matrix Composites (CMCs): CMCs combine ceramic fibers and a ceramic matrix. They exhibit high strength and excellent thermal resistance. CMCs can withstand temperatures exceeding 2,000 degrees Celsius (3,632 °F). They are lighter than traditional metals and are being researched for use in hypersonic vehicle structures.

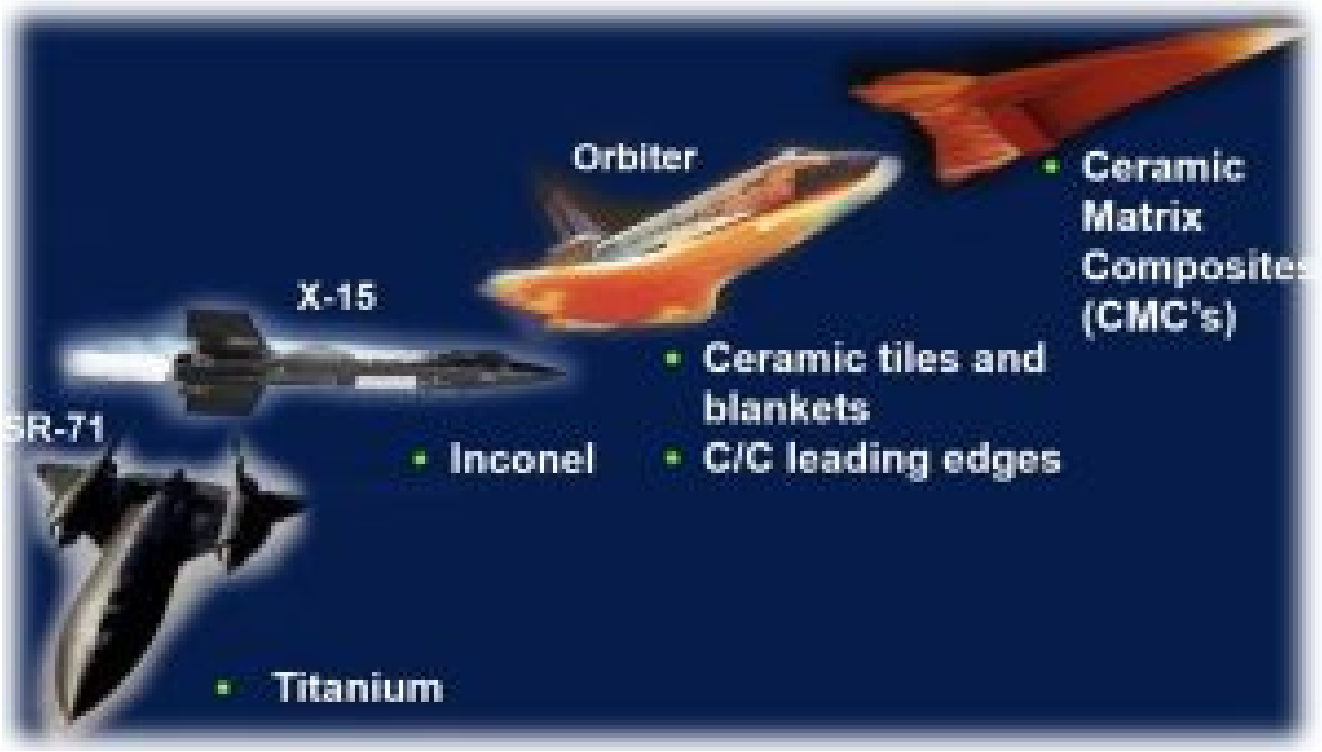
Refractory Metals: Certain refractory metals, such as tungsten and molybdenum, have high melting points and can withstand extreme temperatures. Tungsten, for example, has a melting point of approximately 3,400 degrees Celsius (6,152 °F). These metals are often used in aerospace applications requiring resistance to high temperatures.

Nickel-Based Superalloys: Superalloys are high-performance alloys that maintain strength at high temperatures. Nickel-based superalloys, such as Inconel and Hastelloy, display excellent resistance to heat and oxidation. They are commonly used in the hot sections of jet engines and can also be considered for hypersonic applications.

Graphene: Graphene is a single layer of carbon atoms arranged in a hexagonal lattice. It has exceptional mechanical, thermal, and electrical properties. Graphene can handle high temperatures and has excellent thermal conductivity. However, it is still in the early development and large-scale production stages.

If one were to review the history of high-speed flight, one could observe the changes that have occurred over time with the increase in speed and the need for improved materials.

Figure 13-6
Improvements In The Use Of Various Materials For Heat Dissipation



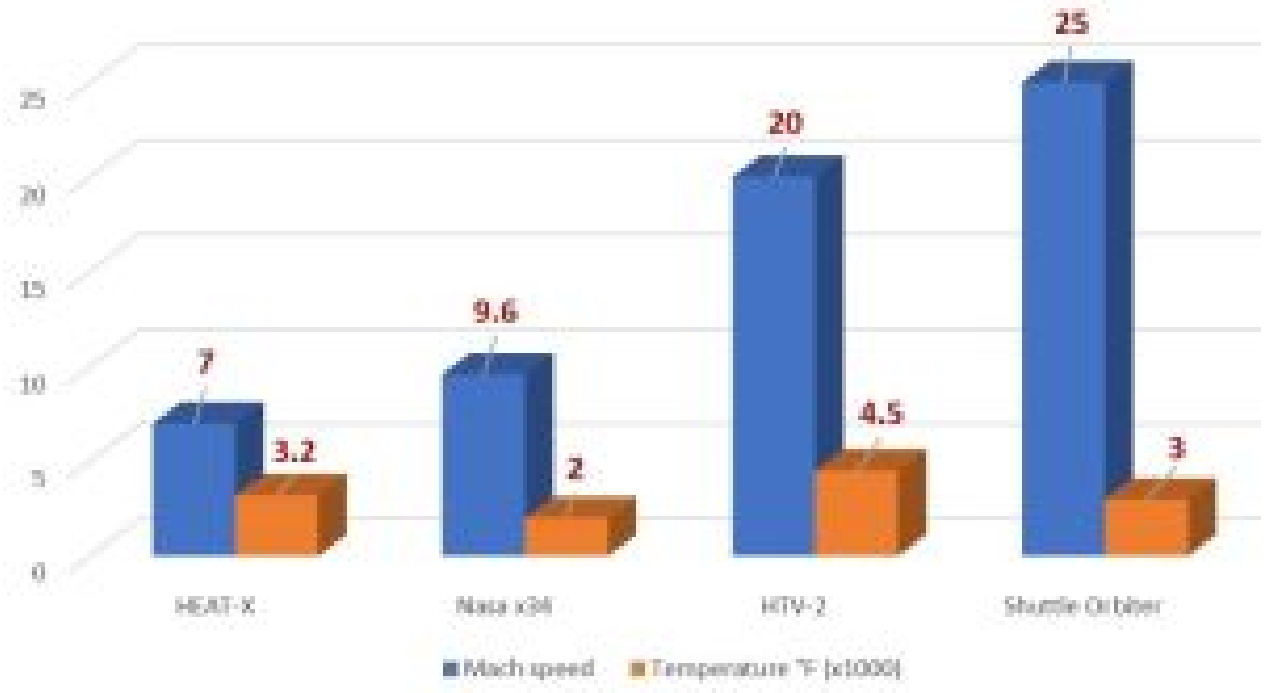
Source: (Glass, 2015)

This chapter only covers a few areas currently developing materials for hypersonic applications. This is an arena of active research with new materials and composites constantly being explored.

In addition to improving heat tolerance, it is critical to dissipate heat through Thermal Protection Systems (TPS) improvements via more advanced protective materials and techniques. Heat dissipation is usually addressed via aerodynamic/structural design and the implementation of effective Heat Management Systems (HMS) that quickly redistribute heat to protect airframes and electronic instruments. This becomes a critical engineering challenge due to the rapid changes in pressure and temperature that can pose significant risks to electronic components. For example, almost all electronic components are joined with a form of solder. One such solder is Eutectic Gold Tin "(Gold-tin (AuSn) solder is a eutectic alloy composed of 80% gold and 20% tin by weight, with a melting point of 280°C (536°F)." (Electricity – Magnetism, 2023). Other specialized alloys are reported to have melting points of 1000 degrees Celsius (1,832°F) in brazing applications. In the situation with Eutectic Gold Tin "(Gold-tin (AuSn) solder, if the internal temperature exceeded the melting point of 280°C (536°F), the solder would begin to melt and loosen the connections between components. This is just one example, but other components are also directly affected by heat. Fortunately, decades of information collected for satellite research, development, and actual launches, have derived many operational limits for

instrumentation. However, regardless of the structure's heat resistance to melting, "The maximum structure temperature is still far higher than the temperatures that would cause degradation and failure to electronic components...Components can be subjected to temperatures as low as −55°C (−67°F) and as high as 125°C (257°F)... These thermal conditions induce several failure modes, including package and die cracking, bond-wire breakage, moisture ingress, die delamination, tin whisker growth, and solder-joint failure." (Electronic Products, 2019).

Figure 13-7 Comparative Speeds and Temperatures



Note: The temperature will vary based on the material and aerodynamic design of the vehicles.

As illustrated in the above chart, thermal management must be applied and maintained to ensure the instrumentation needed for computation, navigation, directional control, communications, and other management functions are not compromised.

Heat Management Systems (HMS) research has expanded in many areas to address challenges discovered due to heat generated from hypersonic velocities. These systems are designed to dissipate or absorb excessive heat, prevent damage to critical components and ensure the missile's performance. The following are a few examples:

Heat Sinks and Radiators: Heat sinks and radiators dissipate excess heat from critical components. These systems typically use high-conductivity materials and structures, such as heat pipes or cooling fins, to absorb

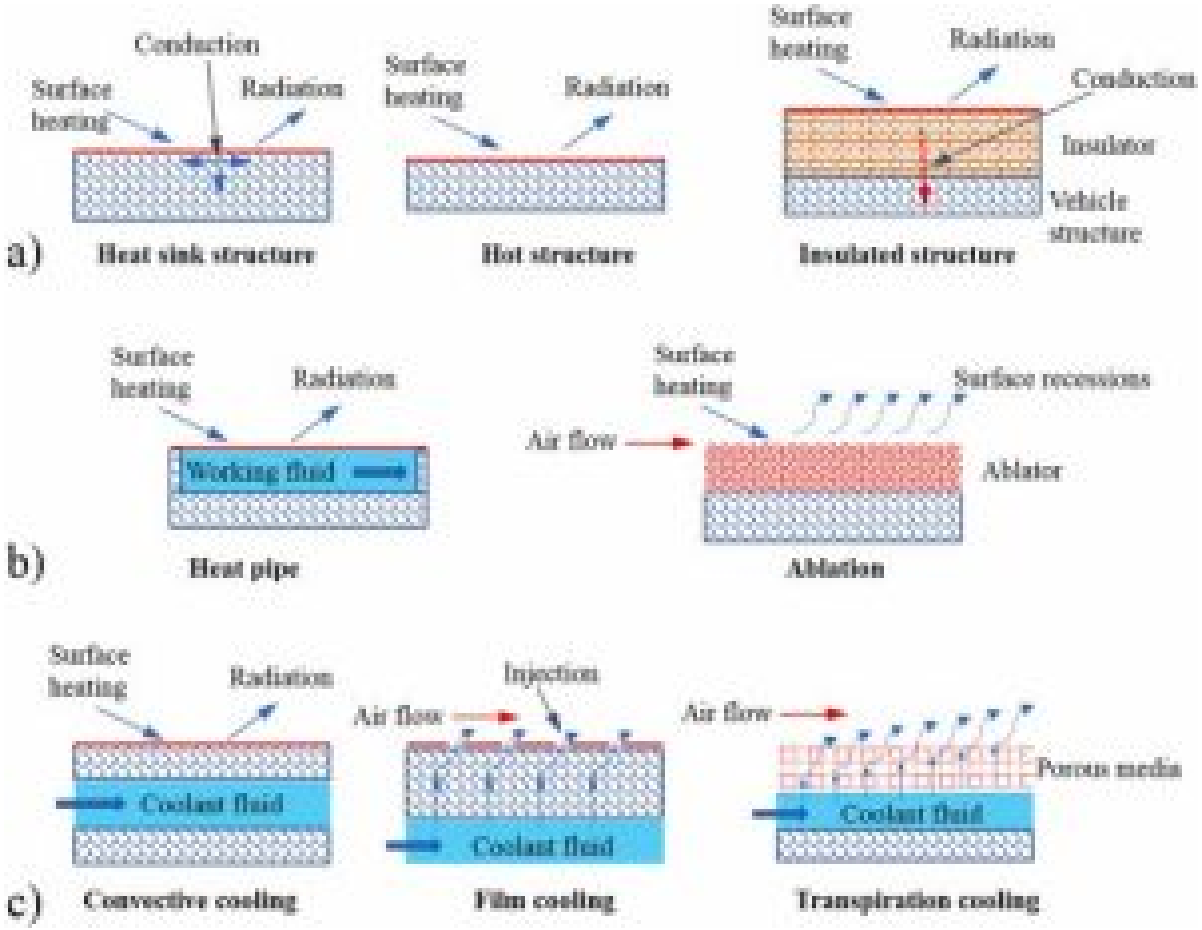
and transfer heat from sensitive areas. Radiators provide a surface for heat to radiate into the surrounding environment, helping to cool down the missile.

Active Cooling: In some cases, hypersonic missiles utilize active cooling techniques to manage heat. This can involve circulating a coolant, such as a liquid or gas, through channels within the missile's structure to absorb and carry away heat from critical components. Active cooling systems, though more complex, can provide efficient heat transfer and enable sustained operation under high-temperature conditions.

Insulation: Insulation materials are used to minimize heat transfer between the hot exterior environment and the internal components of the missile. Multi-layered insulation (MLI) blankets or other low-thermal-conductivity materials create a thermal barrier and protect sensitive components from excessive heat exposure.

Thermal Management Design: The overall design of the missile, including its shape and configuration, is optimized to manage heat. By carefully shaping the missile's body and incorporating aerodynamic features, it can help control the intensity of heat generated during flight and minimize its impact on critical components.

Figure 13-8
Examples Of Various Cooling Techniques



Source: (Le, Ha, & Goo, 2021)

Of particular interest for sustained hypersonic flight are the various types of active cooling systems; some hypersonic missiles may employ active thermal control systems that use advanced techniques to manage heat. These systems can include various methods, such as regenerative cooling, film cooling, and other cooling technologies, to effectively control the temperature and protect critical components:

Regenerative Cooling: Regenerative cooling is a common active cooling technique in hypersonic missiles. In this method, a coolant, such as liquid hydrogen or fuel, is circulated through channels or tubes in the missile's structure, typically around the combustion chamber or nozzle. The coolant absorbs heat from the hot surfaces and then passes through a heat exchanger to cool down before being recirculated. This continuous circulation of the coolant helps maintain the temperature within acceptable limits.

Film Cooling: Film cooling is another active technique employed in hypersonic missiles. It involves the release of a thin film of coolant, usually a liquid or gas, over hot surfaces. The coolant forms a protective layer that helps reduce the heat transfer to the structure. The coolant film can be sprayed from small orifices or delivered through porous materials on the missile's surface.

Transpiration Cooling: Transpiration cooling involves using porous materials or coatings on the missile's surfaces. Coolant is supplied to the porous material, which then permeates through the material and evaporates on the outer surface. This evaporation absorbs heat from the surface, effectively cooling it.

The specific cooling system used in a hypersonic missile depends on various factors, including the missile's design, materials, operating conditions, and mission requirements. Each cooling system has advantages and limitations, and the choice of the cooling technique is determined by weight, complexity, and reliability and will require performance trade-offs.

Progress in airframe design and maneuverability

Recent advancements have focused on increasing maneuverability by making vehicles more agile. This agility will aid in avoiding enemy defenses and better enable them to hit their targets more accurately. Some notable improvements in this area have been:

Aerodynamic Shape Optimization: Advanced computational fluid dynamics (CFD) techniques, combined with powerful computing resources, allow for detailed analysis and optimization of the airframe's shape. This involves refining the vehicle's external contours to minimize drag and enhance aerodynamic efficiency at hypersonic speeds. Improving the vehicle's aerodynamic shape helps reduce heat generation and enables more efficient propulsion.

Maneuvering and Control Systems: Hypersonic vehicles require advanced maneuvering and control systems to navigate the challenging flight demands. Developing advanced flight control algorithms, reaction

control systems, and aerodynamic control surfaces enables better maneuverability, stability, and control authority during hypersonic flight. These systems allow for precise trajectory control, maneuver execution, and vehicle stability.

Variable Geometry: Some hypersonic airframe designs incorporate variable geometry features, such as adjustable wings or control surfaces. Variable geometry allows the vehicle to optimize its configuration based on different flight conditions, including changing aerodynamic forces, center of gravity, and stability requirements. This flexibility enhances performance and control across various flight conditions or requirements.

Active Flow Control: Active flow control techniques involve manipulating the airflow around the airframe using sensors, actuators, and intelligent control systems. These systems can enhance aerodynamic efficiency, reduce drag, and improve stability and control by manipulating boundary layer flow or employing adaptive control surfaces. Active flow control enables better vehicle response, improved maneuverability, and increased overall performance.

Integrated Vehicle Design: Advancements in hypersonic vehicle design involve considering the vehicle as a whole system rather than individual components. To achieve overall performance improvements, integrated vehicle design approaches optimize the interactions between various subsystems, such as aerodynamics, propulsion, structures, and controls. This holistic design approach ensures efficient use of resources, minimizes weight, maximizes performance, and enhances maneuverability.

The concept of Variable Geometry, also known as Morphing airframes, is a product of the holistic design approach. It refers to the design and technology that allows for changes in the shape or configuration of an aircraft's structure during flight. This capability offers several potential benefits, including improved aerodynamic performance, increased maneuverability, reduced drag, enhanced fuel efficiency, and adaptability to varying flight conditions. Here are some key aspects and examples of morphing airframe technologies:

Shape-Changing Structures: Morphing airframes incorporate structures that can change shape or configuration to optimize performance. This can involve using flexible and intelligent materials or mechanisms for controlled deformation. For example, variable camber wings can change the curvature of the wing surface to improve lift characteristics and control.

Adaptive Wing Morphing: Adaptive wing morphing focuses on changing the wing shape to adjust to different flight conditions. This can include altering wing sweep, span, chord length, or twist. By adjusting the wing's geometry, aircraft can optimize their performance across various flight conditions, from subsonic to supersonic or hypersonic speeds.

Active Flow Control: Morphing airframes can incorporate active flow control technologies, such as synthetic jet actuators or fluidic devices, to manipulate the airflow over the aircraft's surfaces. These devices can create localized changes in airflow patterns, reduce drag, enhance stability, and improve control authority.

Shape Memory Alloys (SMAs): SMAs can undergo deformation and return to their original shape when subjected to specific stimuli, such as electrical or temperature changes or mechanical stress. By integrating

SMAs into the airframe structure, components can change shape or position in response to different flight conditions.

Distributed Control Systems: Morphing airframes require sophisticated control systems to monitor flight conditions and adjust the shape or configuration of the aircraft accordingly. These systems often use sensor arrays, computational algorithms, and actuators to enable real-time adjustments to provide safeguards and ensure optimal performance.

Biomimicry: Morphing airframe designs can draw inspiration from nature, imitating the adaptive features of birds, insects, or marine animals. For instance, the ability of birds to change wing shape during flight has inspired the development of biomimetic morphing wing designs.

Figure 13-9
Morphing Wings And Airframes

Note: Different morphing configurations can provide the ultimate configuration relative to the action performed. The above image has standard flight, Lottering, and dash configurations.

Adapted from: https://trimis.ec.europa.eu/sites/default/files/project/documents/40418/final1-maws-overview.pdf (Yang, Nangia, & Cooper, 2014)

Morphing airframes are a promising research area in the early stages. However, as previously stated, these require continued study and advancements in materials science, control systems, and manufacturing techniques to enable a morphing airframe that could meet military demands.

ADVANCEMENTS IN COMPUTER DEVELOPMENT AND ARTIFICIAL INTELLIGENCE (AI)

Developing computers for hypersonic missiles is crucial in achieving the desired performance, accuracy, and responsiveness intended for such weapons. Achieving such will require sophisticated onboard computers to handle real-time complex tasks. The following are some critical aspects of computer development that will be impacting to the advancement of hypersonic missiles:

Radiation-Hardened Processors: Hypersonic missiles often operate in environments with high radiation levels, such as during space travel or atmospheric re-entry. To ensure the reliability of onboard electronics, radiation-hardened processors are used. These processors are designed to withstand the effects of radiation and prevent malfunctions caused by radiation-induced errors.

High-Performance Processors: The need for powerful processors capable of executing complex algorithms quickly and accurately are required for hypersonic activity. These processors must handle navigation, guidance, control, and sensor data processing tasks at extremely high speeds. Specialized high-performance computing architectures such as Multi-Core Processing are often employed to meet these requirements.

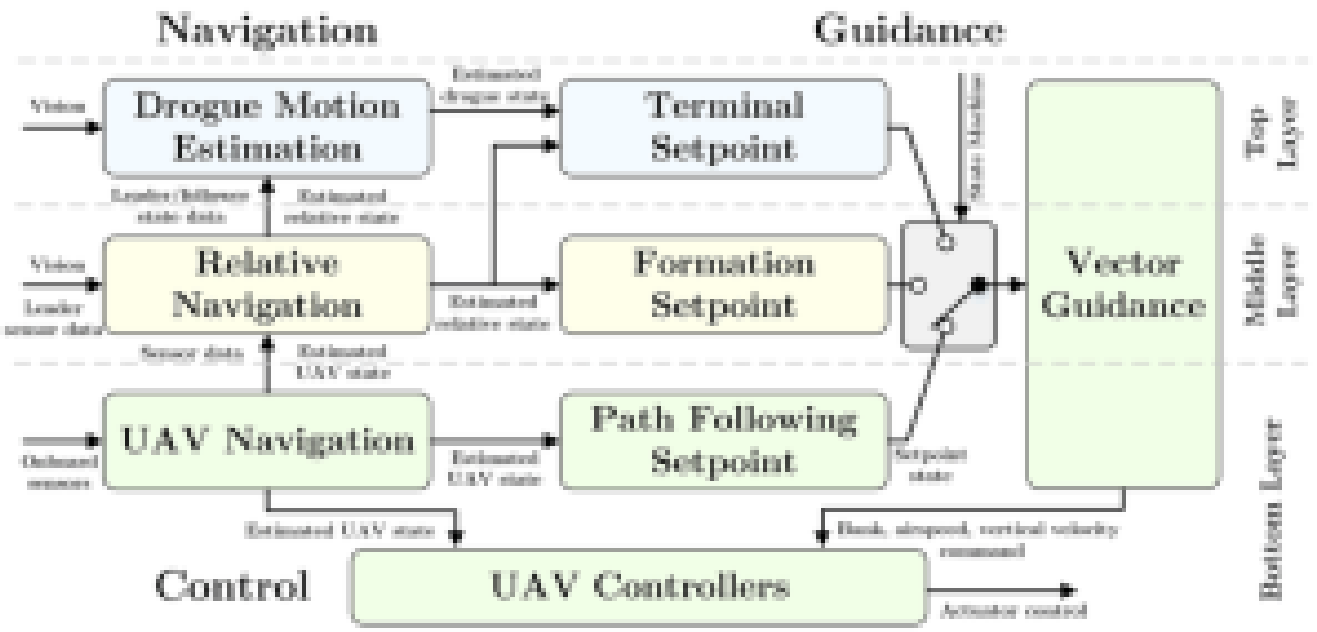
Real-Time Operating Systems: To ensure timely execution of critical functions, hypersonic missiles typically use real-time operating systems (RTOS). RTOS prioritizes tasks based on their urgency, minimizing the possibility of delays, and ensuring precise control and responsiveness during flight. Some RTOSs allow for separating critical and non-critical software components, enabling the coexistence of multiple operating systems or applications on the same hardware platform.

Navigation and Guidance Algorithms: Sophisticated navigation and guidance algorithms are essential for hypersonic missiles to maintain their intended trajectory and accurately hit their targets. These algorithms continuously analyze sensor data, such as GPS signals and inertial measurements, to compute optimal flight paths and adjust course corrections in real time.

Sensor Fusion: Hypersonic missiles rely on various sensors, such as inertial measurement units (IMUs), GPS receivers, and advanced imaging or target-tracking sensors, to gather data about their surroundings and targets. Sensor fusion algorithms integrate information from these diverse sources to enhance situational awareness and improve the missile's ability to identify and engage targets.

Autonomous Decision-Making: Hypersonic missiles often operate in contested and rapidly changing environments. As a result, they may need to make autonomous decisions to adapt to unexpected scenarios or countermeasures. Advanced artificial intelligence (AI) and machine learning algorithms are integrated into missile computers to provide intelligent decision-making capabilities.

Figure 13-10 Sample Of High-Level Architecture For U Coupling With A Refueling Drogue Coupling



Note: This does not represent the far more complex architecture and sub-systems that would provide services for a hypersonic vehicle but gives a general idea of activities that must be accounted for.

Adapted from: (Wilson, 2015)

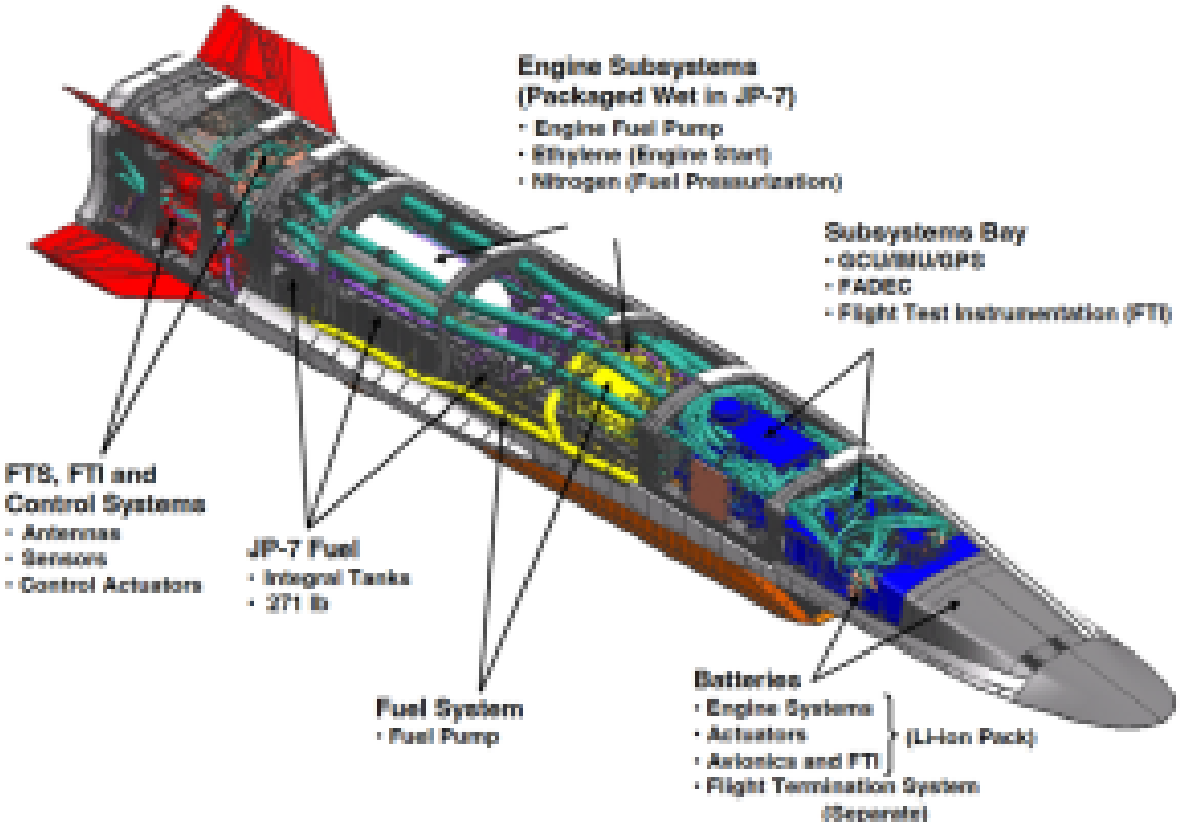
Secure Communication: Hypersonic missiles may communicate with command centers or other platforms during flight, requiring secure and robust communication systems to relay data and receive updated instructions. Encryption and secure communication protocols are essential to protect the missile's integrity and maintain operational security. In addition, the encryption/decryption process must be performed quickly to avoid introducing delays in the Communication, Command, and Control(C3) flow. The systems must also account for the ionization surrounding the vehicle at such speeds.

Fault Tolerance and Redundancy: Exposure to extreme conditions and challenging environments makes it necessary for onboard computers to incorporate fault-tolerant design principles and redundant surface

control systems to improve the reliability of mission success. This redundancy enables the missile to continue functioning even if specific components fail during flight.

Although much of the information related to the types of processors used is classified, they must have high-performance computing capabilities to perform real-time processing from the many sensors needed for vehicle operation and make real-time calculations for precision maneuver execution. For example, at Mach 5, a missile will travel approximately 1 mile a second. There is no time for delayed calculations or signal delivery to critical maneuvering components. Such development is a multidisciplinary endeavor involving aerospace engineering, computer science, electronics, system integration, and manufacturing expertise.

Figure 13-11
Cutaway Diagram of the X-51A HCM with Subsystems



Source: J. Hank, J. M., Murphy, J. S. and Mutzman, R. C., 'The X-51A Scramjet Engine Flight

Demonstration Program', 15th AIAA International Space Planes and Hypersonic Systems and Technologies Conference, May 2008, p. 7., (J. Hank, 2008)

In addition, to improve computing hardware. It is crucial that the software be equally as efficient and can perform exceptional analytics. Artificial intelligence (AI) plays a role in various aspects, including guidance, navigation, control (GNC), target acquisition, and autonomous decision-making. Here are some specific AI uses in hypersonic missiles:

Data Processing and Fusion: Vast quantities of data are generated from onboard sensors and external sources. AI can assist in processing and fusing this data to provide a comprehensive situational awareness for the missile's guidance and decision-making systems. Machine learning algorithms can integrate and analyze information from multiple sources to generate accurate and real-time assessments for flight duration.

GNC Optimization: AI can optimize hypersonic missiles' guidance, navigation, and control algorithms to enhance flight performance and accuracy. Machine learning techniques can analyze vast data to improve trajectory planning, control surface adjustment, and overall flight stability.

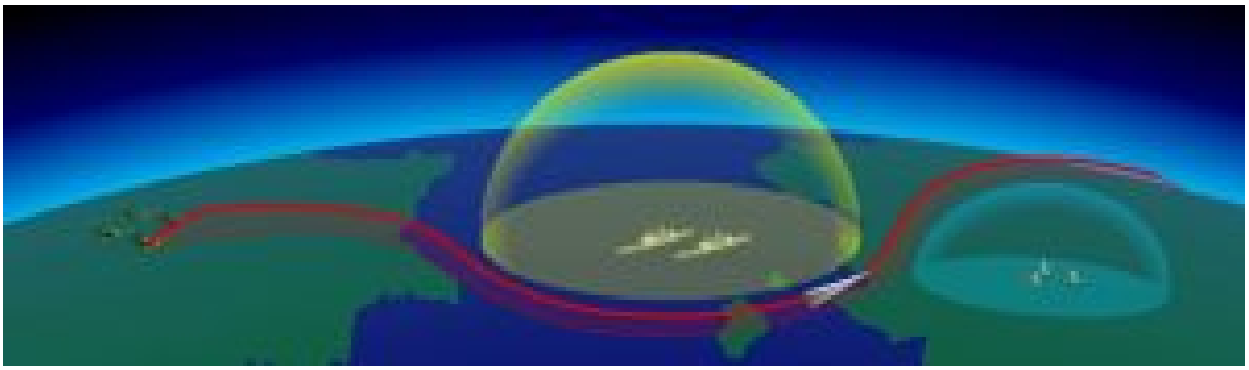
Target Recognition and Tracking: AI can analyze sensor data, such as radar and infrared imaging, to detect, identify, and track targets. Machine learning algorithms can recognize patterns and signatures associated with various types of targets, improving the missile's ability to acquire and engage them. This same technology is beneficial in countermeasures used to detect hypersonic missiles during various stages of flight.

Autonomous Targeting: AI can autonomously select and prioritize targets based on predefined criteria. Integrating AI algorithms into the missile's system allows it to analyze real-time data, assess threats, and make decisions on target engagement without human intervention.

Countermeasures and Adaptability: Hypersonic missiles must evade potential enemy defenses and react to changing scenarios. AI algorithms can assess and respond to incoming threats, identify countermeasures, and adapt the missile's trajectory or tactics accordingly. This adaptability can enhance the missile's survivability and increase the likelihood of mission success.

Figure 13-12

Detection avoidance



Source: (Brimelow, 2018)

AI applications augmented with machine learning have the potential to evade enemy countermeasures and reconfigure themselves based on current circumstances and situational awareness. This capability will allow the device to react to unplanned encounters and revise operational requirements based on current environmental and available operational information or decide without such data.

ENHANCEMENTS TO DELIVERY SYSTEMS

To appropriately frame the concept of hypersonic missiles, it is essential to understand that there are two major categories, each of which can be deployed from multiple platforms, such as air, ship, land, or space. As discussed in Book 7, chapter 2 on Satellite Killers and Hypersonic Drones (2022), there is the **Hypersonic Cruise Missile** (HCM) has a self-contained propulsion system, typically driven by SCRAM jet technology and **Hypersonic Glide Vehicle** (HGV), relies on gravity and atmospheric conditions to produce speed and maneuverability. These vehicles are difficult to track if released from an aerial or space platform.

Figure 13-13
Categories of Hypersonic Missiles

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

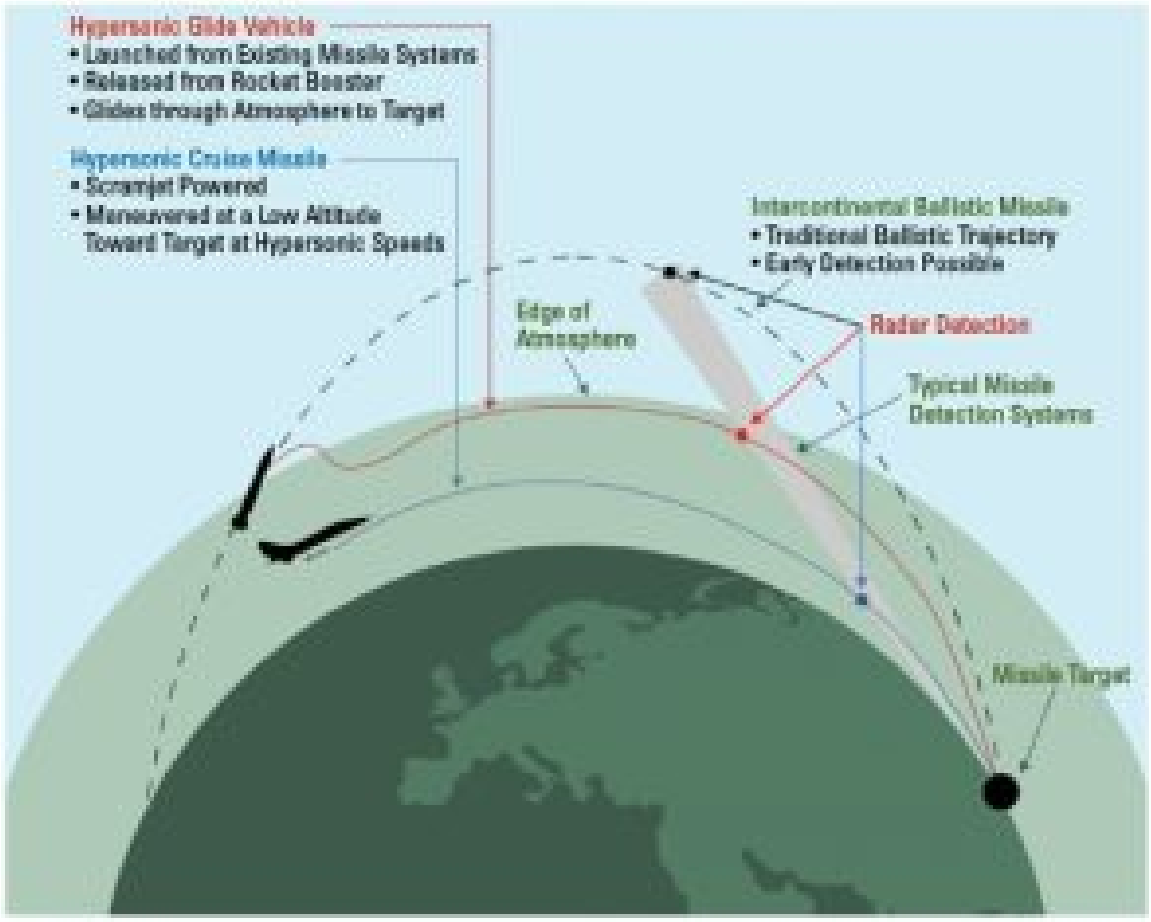
Unlike their predecessor, the ballistic missile, which follows a parabola-shaped arch and has a predictable flight path from launch to target.

Figure 13-14
Sample Ballistic Missile Trajectories

Source: (Salia, 2018)

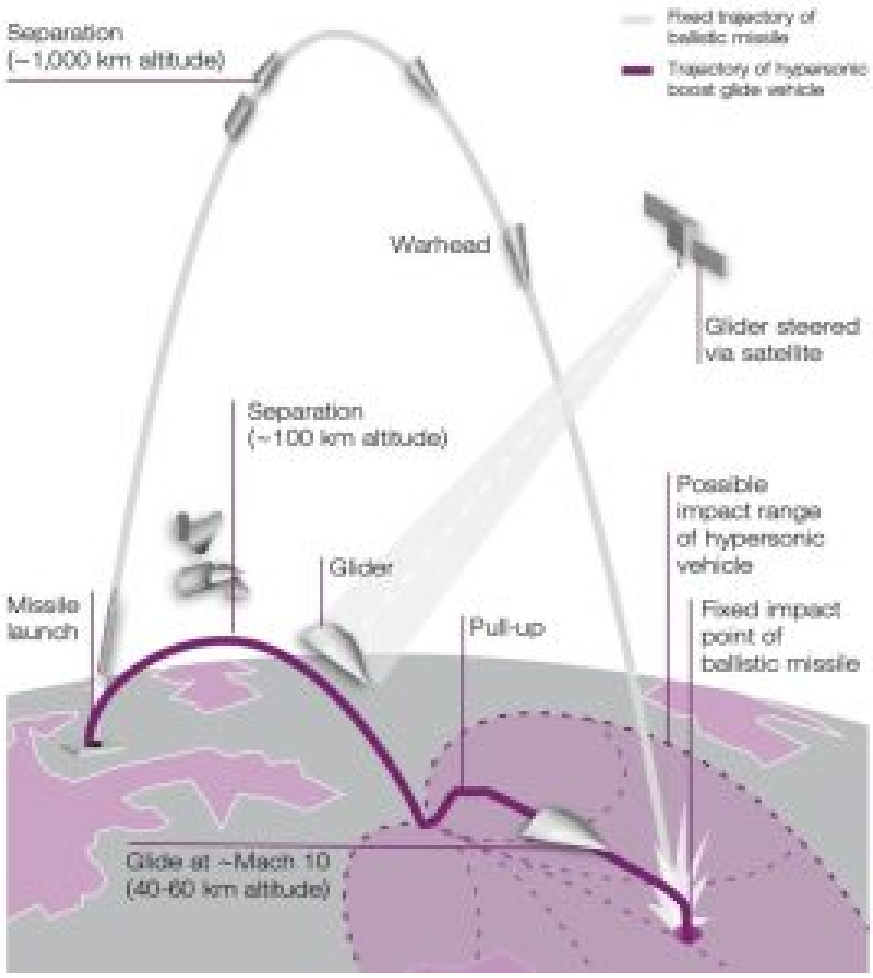
The hypersonic HCM and HGVs operate on a flatter trajectory and are more maneuverable. Their agility provides a more capability to avoid detection by terrestrial-based radar and a higher probability of evading opposition countermeasures if deployed. Improvements in navigation, guidance, and control technology make it possible to seek alternate targets within its strike range and even calculate flight paths that would introduce confusion into opposition tracking used to detect and calculate the probability of which locations may be potential targets. This type of deception would help impede the opposition's ability to deploy countermeasures to protect the actual target.

Figure 13-15
Points Of Terrestrial Detection of HCM, HGV, and Ballistic Missiles



Source: (Higham & Strategy_Analytics, 2022)

Figure 13-16
Possible Alternate Target Options of an HCM or HGV



Source: (Delcker, 2019)

As with any weapon system that takes flight, weight and flight characteristics become a consideration in the design, operational range, and speed. For example, both designs require some initial level of flight assistance. HGVs frequently require assistance from a booster to achieve low orbit and utilize gravity. In the case of HCMs, a booster or air launch is necessary to obtain the speed required to engage the onboard SCRAM jet engine. Also, the HCM must carry its fuel and other needed control systems and payload it would deliver. Advancements in rocket boosters, electronics, lightweight, heat-resistant material, and aerodynamic designs have made it possible to carry larger payloads, either nuclear or conventional.

The advent of aeronautical advancements such as the Space Shuttle and Space-X have removed obstacles that once rendered consideration of some previous concepts cost prohibitive or just unfeasible. These more contemporary advancements and technical improvements have opened the door for reconsidering old concepts based on applying advancements in other areas. For example, there is renewed interest in space platforms such as "Project Thor" or "Rods from God," which refers to creating a space-based weapon system involving kinetic bombardment. The concept is to use the gravitational force to accelerate a large rod or projectile, typically

made of dense materials like tungsten, that would generate significant destructive power upon impact with a target on Earth. Once launched from an Orbital Kinetic Energy Bombardment Platform, tungsten rods of 20-foot lengths by 1-foot diameters and traveling at approximately Mach 10 would have sufficient Kinetic Energy to cause mass destruction (Stilwell, 20211).

To provide context, given that the rod has a diameter of 1 foot (0.3048 meters) and a length of 20 feet (6.096 meters) and is constructed of tungsten, we can calculate the weight as follows:

Radius = diameter / 2 = 0.3048 / 2 = 0.1524 meters

Volume = π * (0.1524^2) * 6.096 = 0.554 cubic meters

Weight = Volume * Density = 0.554 * 19,250 = 10,676.75 kilograms

The tungsten rod would weigh approximately 10,676.75 kilograms (or approximately 10.68 metric tons).

The Kinetic Energy produced at this weight coupled with a speed of Mach 10 would produce:

Velocity = 10 * 343 (Mach 1) = 3,430 meters per second

Converting the mass of the tungsten rod to kilograms (~10.7 metric tons = 10,700 kilograms)

Kinetic Energy = (1/2) * 10,700 kg * (3,430 m/s)^2

Kinetic Energy ≈ 248,594,050,000 joules or 248.6 gigajoules

To add perspective, one ton of TNT is equivalent to 4.184 gigajoules. Therefore, the energy from the 20-foot rod would be equivalent to 59.4 metric tons of TNT. This would be slightly more than the 6.4 magnitude earthquake that hit off the coast of Puerto Rico on January 6, 2020, causing widespread devastation to the southern region. This concentrated amount of kinetic energy converted to potential energy in milliseconds would have a devastating impact. Estimations would have the rod at said weight and speed with a 50–60-degree angle of impact, could displace approximately 23,700 cubic meters of earth, generate intense heat, and leave an impact creator approximately 49-meters (161.75 ft) wide and 12.3 meters (40.35 ft) deep. This would not account for the damage created by shockwaves, flying debris, or EMP generation and would leave virtually no radioactive fallout.

Figure 13-17 THOR

Image from: Kebal Space Program Forums / LADBible (SOFREP, 2022)

Figure 13-18 Chinese Reported a test drop of KE HGV

Source: (China Arms, 2020)

REVISIONS IN DEFENSIVE STRATEGIES

The continued multi-discipline improvements refining hypersonic technology have made it difficult, at best, to detect and neutralize weapons employing these technologies. This provides for offensive superiority even if the defending side has offensive parity unless the defending side has developed appropriate countermeasures; even then, because of the speeds involved, target acquisition capabilities, and maneuverability of these weapons, it may nullify any reaction time of the defender. Therefore, defensive detection methods must be enhanced to provide quicker and more reliable notifications/alerts to increase the probability of neutralizing such a threat. As discussed earlier in the chapter, the Observe, Orient, Decide, Act (OODA) loop is a primary methodology for evaluating subsequent actions and acting on them. The sooner the steps of observation and orientation are accomplished, the more time is available to decide and act.

As with the innovations in computer technology, Real-Time-Operating-Systems (RTOS) and AI are assisting with hypersonic-based delivery systems; the same or similar technology can aid in its detection and implementation of countermeasures. We discussed how technological advances such as the Space Shuttle and Space-X can enable the delivery of platforms like the "Thor Project." These have also enabled innovations in early observation/detection. Such innovation will help improve the "Observe" phase of the OODA loop.

Since 2019 The Pentagon's Space Development Agency (SDA) has been actively partnering with Northrop Grumman, York Space Systems, L3Harris, and Space-X to architect and deploy a U.S. military mega-constellation consisting of hundreds of small satellites to improve the detection of hypersonic missiles. Before advancements in booster technologies, capabilities to reuse a booster, and the ability to return to the launch pad, deployments of such scall were not achievable. Such technological advancements have made it technically and financially feasible to field a network of space-based monitoring and communication satellites to provide a virtual canvasing of the entire globe.

Figure 13-19 Plans For A U.S. Military Mega-Constellation

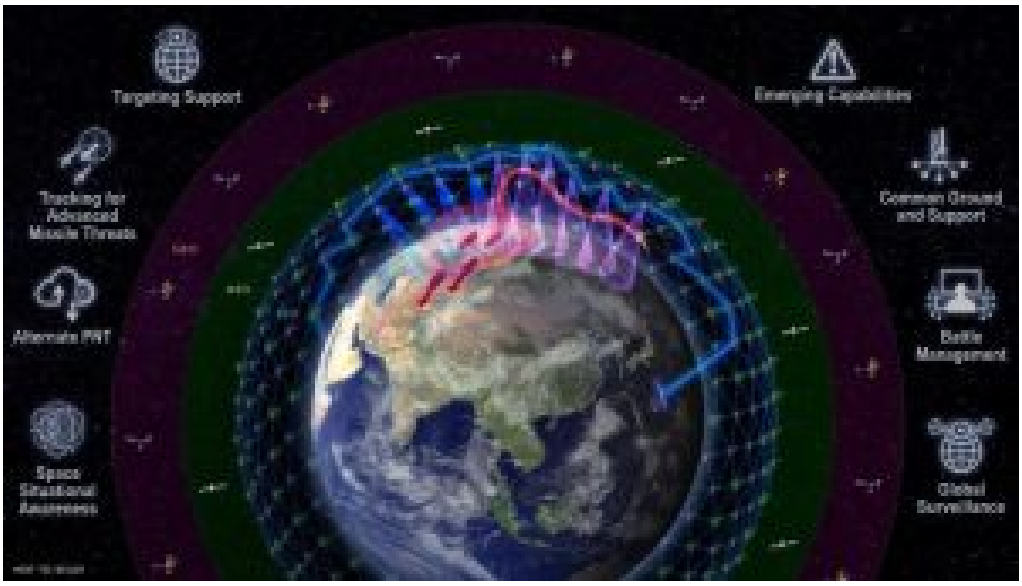


Photo: US Department Of Defense,
Source: https://www.defense.gov/Multimedia/Photos/igphoto/2002511880/

These new networks of satellites equipped with new sensor technology can detect new Infrared signatures and pierce the armor of plasma stealth. In many cases, as the missile reaches such high velocities, it experiences extreme aerodynamic heating due to air compression, leading to a plasma cloud around the missile. Plasma stealth, also known as active plasma-based stealth, is a proposed technique for reducing the radar detectability of an aircraft or missile by creating a plasma cloud around it.

The idea behind plasma stealth is to use the high temperatures generated by the hypersonic flight to create a layer of ionized gas, or plasma, around the missile. This plasma cloud could interfere with radar signals and reduce the missile's detectability. The ionized gas would reflect, absorb, or scatter the incoming radar waves, making it more difficult for radar systems to detect and track the missile accurately.

The exact speed at which a plasma cloud forms can vary, but it generally occurs from Mach 7 to Mach 10 (approximately 2,390 to 3,430 meters per second at sea level). At these speeds, the air surrounding the missile

becomes so highly energized that the electrons and ions dissociate from their atoms, forming a conductive plasma.

Although Plasma Stealth can provide a viable stealth value from radar to such missiles, the ionization of air that provides this stealth can itself be detected because it will leave a Plasma footprint which, although is shortly lived (milliseconds), can be detected from satellites property equipped (Harshitha & Baskaradas, 2023). As discussed, the legacy technology was optimized for launching and tracking ICBMs with satellites that would detect the large plums and exhaust from silos and ground-based radar sensitive to the distinct heat signatures and radar reflections of

Figure 13-20

Mesh Network Of Satellites in a Constellation

Source: (Tingley, 2021)*, Photo: US Department Of Defense's SDA*

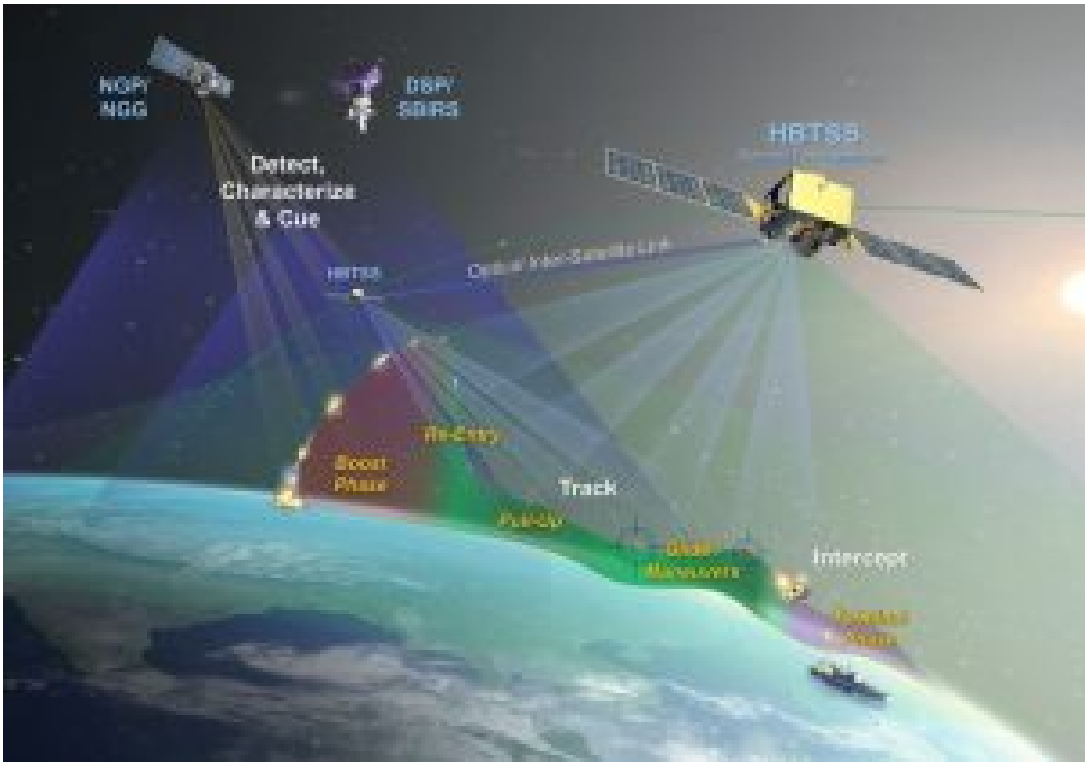
Such missile launches.

LAYERED DEFENSE

Due to new technology in the area of Electro-optical Infrared (EO/IR), it is possible to detect hypersonic missiles transitioning from glide to terminal phases of their flight profiles. In addition, the development of a Space-Based Infrared System (SBIRS) and Hypersonic and Ballistic Tracking Space Sensor (HBTSS),

in a constellation configuration, can perform detections from the moment of launch and track the missile to completion. Advancements in AI are aiding in friend-or-foe identification, Battle Management, Communication, Command, and Control. The combination of these technologies will be part of a multi-layer defense strategy. This would include surveillance and early warning systems that are radar and space-based and would include ground-based units equipped with inceptors and various types of Direct Energy Weapons (DEW). Such a defense strategy would incorporate advanced battle management systems to coordinate and integrate various data collection platforms, including air and sea-based reconnaissance. This integrated information collection would provide a comprehensive real-time situational picture providing the essential information necessary for critical decision-making. Because of the speed associated with hypersonic weapons, it may be necessary to have AI incorporated into the intercept decision-making process. Such a need will be dictated based on when the missile was detected and its distance from any assets within the range of potential attack vectors.

Figure 13-21
Layered Detection, Tracking, And Intercept

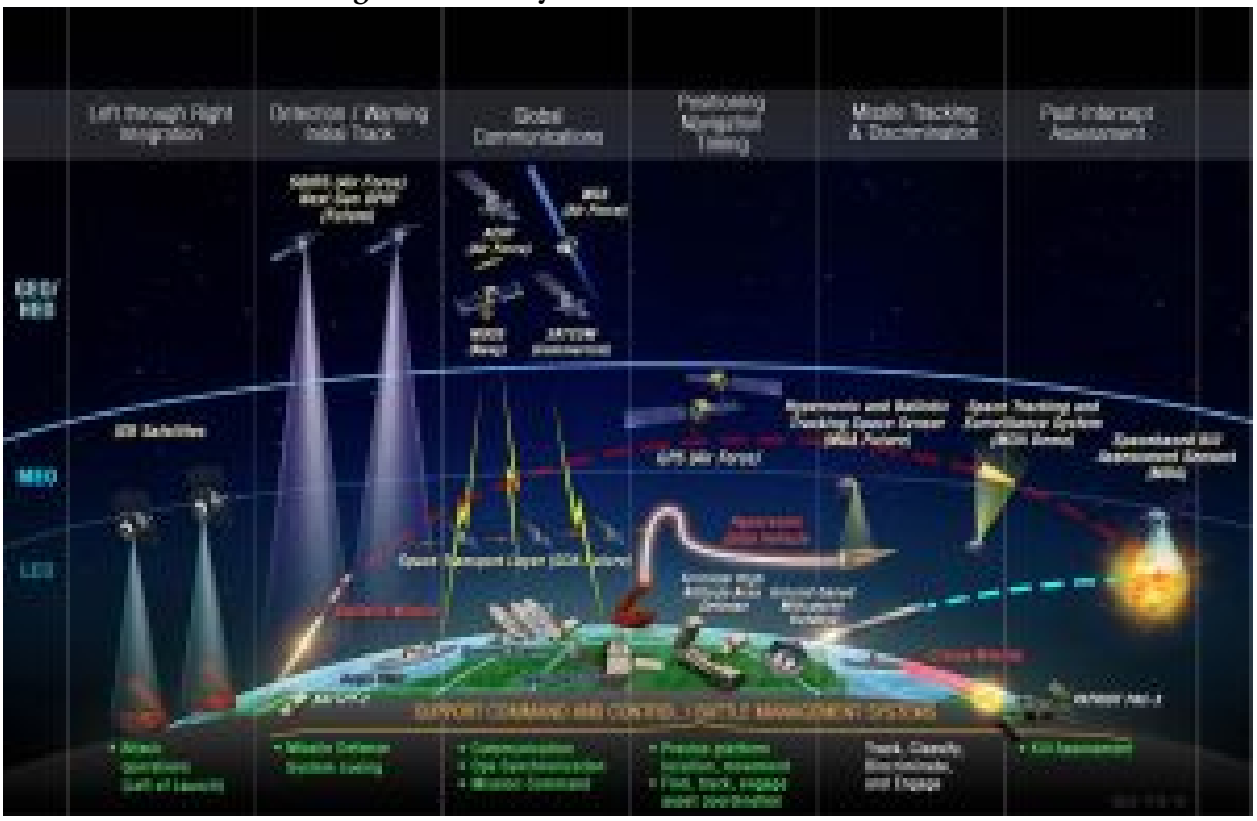


*Source: (*Burgess, 2022) *Photo: Northrop Grumman*

The end-to-end time to iterate through the OODA loop decreases as technology advances. The recently discussed topics help improve the ability to "Observe" a launch. With the aid of advanced computer algorithms and inputs from other sources and space-based systems, it, and proper integration of battle management

systems, it is possible to "Orient." much quicker. However, it is critical to have sufficient information to "Decide" and "Act." This may require another set of technologies that will perform predictive analytics based on collected information from the previously discussed data collection points to make informed decisions in predicting the probability of where a hypersonic vehicle may be targeting. This becomes complicated since the devices are so fast and agile that there may not be sufficient time to decide to intercept, evacuate, or accept the collateral damage. This may be further impacted by onboard intelligence of the oncoming weapon. It is feasible that the attacking device may have similar built-in intelligence to thaw or counter any attempts by the defender to analyze or compute an intercept and therefore consume additional time. All such tactics can incur additional delays in the "Decision" making process, not to mention political implications, both national and international, which may be a further hindrance. However, in a pure combat theater, such as shore-to-ship attacks, or ground support operations, such a decision may be made quicker with AI, and in combat scenarios, attacks are usually focused on military or war-supporting assets. However, it should be noted that there are significant moral and ethical concerns surrounding using AI systems to make autonomous launch decisions. Most militaries worldwide require human intervention and oversight to authorize a missile launch.

Figure 13-22 Layered Detection And Defense



Source: (CSIS, 2019), Photo: Missile Defense Agency

Note: With Overhead Persistent Infrared (OPIR) satellites, improved communications, and AI, it is possible to perform integrated battle management and intercept activities more expediently.

INTERCEPT AND DEFENSE CAPABILITIES

The final step in the OODA loop is to act once a decision is made. At this point, a critical portion of the time to act has been consumed in the previous three steps of the process. The final step also takes considerable time because physical activities include target acquisition, development of a firing solution, launch, and travel time to a plotted intercept location of the agile target, traveling at Mach 5 or greater. As previously mentioned, this type of interception calls for a multi-layered and integrated defense strategy. The strategies include current and future intercept capabilities

- Surface-To-Air missiles, which include ship-based missile systems.
- Direct Energy Weapons (DEW), which fall into the general groupings of

Particle Beam Weapons: Consist of a beam of high-energy particles.

Microwave-Based: Designed to produce electromagnetic interference

LASER-based: Designed to heat or pulse a target and destroy critical parts

LIPC weapons: Laser-Induced Plasma Channel makes a channel to allow clear passage of an electromagnetic stream to the target.

Currently, the arsenal of fielded aerial defensive weapons is limited to such systems as RIM-161 or SM-3 class missiles. Such limits make the ability to detect, track and communicate timely extremely important.

Figure 13-23 Hypersonic Surface-To-Air Inceptor Missile

Source: (CSIS, 2023)

Development of additional land and sea-based systems, such as electromagnetic railguns (EMRG) that

would catapult a gun-lunched guided projectile (GLGP) or hypervelocity projectile (HVP), are actively being explored and tested.

As outlined in the April 21, 2023, report to Congress, which discussed concerns regarding navel vulnerabilities with existing shipboard defense systems, it was suggested that investments be made in ship-based Solid-State Laser(SSL) technology. This has led to the development of the Navy Laser Family of Systems, which include such projects as Advanced Test High Energy Asset (ATHENA), High Energy Laser Counter-ASCM Program (HELCAP), and the development of the High-Energy Laser with Integrated Optical Dazzler and Surveillance (HELIOS) weapon systems (CRS, 2023).

In addition to laser-type technologies, there are many advancements in using High-Power Microwave systems to perform Counter-Electronic activity. Such systems would damage the electronics of an adversary's weapons and Electronic Warfare and Countermeasure systems, including navigation, in which the microwaves would jam or disrupt communications and other functionality essential to operate the attacking weapon adequately. This is currently being pursued in an effort known as CHAMPS (Counter-Electronics High Power Microwave Advanced Missile Project) and has been stated as deployed on one or more naval vessels for testing and evaluation.

Figure 13-24 Stated ODIN System aboard USS Stockdale

Source from: (Tingley, 2021) https://www.thedrive.com/the-war-zone/41525/heres-our-best-look-yet-at-the-navys-new-laser-dazzler-system

This technology has also been demonstrated in the Tactical High-power Operational Responder (THOR), in which swarms of UAS were neutralized with microwave transmissions.

Figure 13-25 THOR Microwave DEW system

Sourced from: https://www.airandspaceforces.com/air-forces-thor-drone-swarm-demo/

It should be noted that more highly powered systems are under development to neutralize the threats imposed by hypersonic missiles. However, in the interim, there are fielded systems that can eliminate more minor threats and attacks from UAS. In many situations, an adversary would implement strategies that deplete a ship's aerial interceptor inventory or munitions supporting the Close-in Weapon Systems (CIWS). Once inventory is depleted, known as "limited depth of magazine," a ship would be virtually unprotected. This scenario has been realized with the use of swarms. Although not at the scale necessary to eliminate significant threats such as missiles, the use of Direct Energy (DE) weapons would assist with the elimination of more minor threats, such as drones, and maintain the consumable assets for the more significant threats, such as a hypersonic missile attack.

SUMMARY

Hypersonic weapons are real and have been in existence since the 1960s. As technology has advanced, so has the ability to develop and field more advanced weapons. However, the types of hypersonic weapons the current world powers boasted about continue to partially defy the physics and currently available materials and technology to support the brags, boast, and hype. However, research into heat-resistant compounds, streamlined aerial designs, computer components, sensor development, satellite constellations, combat management systems, and Artificial Intelligence continue to bring these aspirations into the realm of feasibility and continue to improve the first-strike dominance of whom every achieves such. Likewise, the same multi-discipline technological advancements are being undertaken to develop countermeasures to neutralize such attacks to maintain a balance of power.

Overall, the advancements in hypersonic missile technology are making these weapons even faster and more effective. The continued development also raises concerns about the risks of accidental or intentional use and the potential to destabilize the concept of offensive parity and mutually assured destruction as deterrents. Due to the sheer speed and agility of hypersonic weapons, which will only become faster and more maneuverable, will be required nations to adopt new strategies that may require launch decisions to be made by AI as opposed to humans intervention and the adoption of revised launch-on-detection (LOD) policies where the defender must launch any countermeasure and retaliatory actions on detection of what is perceived to be an enemy's launch as a last-ditch effort to provide the highest probability of survival. Such strategies will continue to heighten tensions and fuel the inevitable cycle of competitive superiority.

REFERENCES

AE Toolbox. (2022, Mar 31). *Melting Points for 10 Common Metals.* Retrieved from www.americanelements.com: https://www.americanelements.com/meltingpoint.html

Aero Corner . (2021, June 15). *13 fastest fighter Jets in the world (+ 4 fastest jet aircraft).* Retrieved from https://aerocorner.com/blog/fastest-fighter-jets/: https://aerocorner.com/blog/fastest-fighter-jets/

American Element. (2022, March 31). *Melting Point of Common Metals, Alloys, & Other Materials*. Retrieved from americanelements.com: https://www.americanelements.com/meltingpoint.html

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

Blair, B. G. (2019, Oct). *The U.S. Nuclear Launch Decision Process (on warning of incoming Russian missile).* Retrieved from www.globalzero.org/: https://www.globalzero.org/wp-content/uploads/2020/11/Full-LOWTimeline.pdf

Brimelow, B. (2018, April 30). *Russia, China, and the US are in a hypersonic weapons arms race — and officials warn the US could be falling behind* . Retrieved from www.businessinsider.com: https://www.businessinsider.com/hypersonic-weapons-us-china-russia-arms-race-2018-4

Burgess, R. R. (2022, February 2). *ice Adm. Hill: MDA Pushes Space-Based Sensor for Tracking Hypersonic Missiles for Fleet Defense* . Retrieved from SeaPower: https://seapowermagazine.org/vice-adm-hill-mda-pushes-space-based-sensor-for-tracking-hypersonic-missiles-for-fleet-defense/

China Arms. (2020, November 24). *China unveils 3 'wide-area aircraft' suspected to be Rods of God weapons*. Retrieved from China-Arms: https://www.china-arms.com/2020/11/china-aircraft-rod-from-god/

Cronk, T. M. (2021, May 3). *Defense official says hypersonics are vital to modernization strategy, battlefield Dominance.* Retrieved from www.defense.gov/: https://www.defense.gov/News/News-Stories/Article/Article/2593029/defense-official-says-hypersonics-are-v

CRS. (2023, April 21). *Navy Shipboard Lasers: Background and*. Retrieved from crsreports.congress.gov: https://crsreports.congress.gov/product/pdf/R/R44175

CSIS . (2021, July 31). *CSIS Missile Defense Project.* Retrieved from missilethreat.csis.org: https://missilethreat.csis.org/missile/avangard/

CSIS. (2019, October 7). *A Vision for the Future of Missile Defense*. Retrieved from CSIS.org: https://www.csis.org/events/vision-future-missile-defense

CSIS. (2021, Aug 2). *CSIS Missile Defense Project.* Retrieved from missilethreat.csis.org/missile/: https://missilethreat.csis.org/missile/df-17/#:~:text=Specifications%20The%20DF-17%20is%20solid-fueled%2C%20measures%20around%2011,as%20that%20used%20for%20China%E2%80%9

CSIS. (2023, March 91). *Standard Missile-3 (SM-3).* Retrieved from missilethreat.cus.org: https://missilethreat.csis.org/defsys/sm-3/

Delcker, J. (2019, Feb 8). *China leads research into hypersonic technology: Report.* Retrieved from defence.pk/: https://defence.pk/pdf/threads/china-leads-research-into-hypersonic-technology-report.600978/

Drag Coefficient. (n.d.). Retrieved from The Engineering ToolBox: https://www.engineeringtoolbox.com/drag-coefficient-d_627.html

Electricity – Magnetism. (2023, June 11). *Gold-Tin Solder*. Retrieved from Electricity – Magnetism.com: https://www.electricity-magnetism.org/gold-tin-solder/

Electronic Products. (2019, April 11). *A brief history of electronic reliability in space — including today's risks and how to mitigate them.* Retrieved from www.electronicproducts.com: Electronic Products. (2019, April 11). A brief history of electronic reliability in space — including today's risks and how to mitigate them. Retrieved from https://www.electronicproducts.com/a-brief-history-of-electronic-reliability-in-space-including-to

Forca Aerea Brasileira. (2021, Dec 16). *FAB realiza primeiro teste de voo do motor aeronáutico hipersônico 14-X.* . Retrieved from fab-mil-br.translate.goog/noticias/mostra/38395/: https://fab-mil-br.translate.goog/noticias/mostra/38395/
OPERA%C3%A7%C3%A3O%20CRUZEIRO%20-%20FAB%20realiza%20primeiro%20tes

Glass, D. E. (2015, May 18). *Hypersonic Materials and Structures*. Retrieved from ntrs.nasa.gov: https://ntrs.nasa.gov/api/citations/20160007098/downloads/20160007098.pdf

Harshitha, V. L., & Baskaradas, J. A. (2023, May 12). *Detection of Hypersonic Missiles in presence of Plasma Stealth*. doi:10.23919/URSI-RCRS56822.2022.10118527

Higham, E., & Strategy_Analytics. (2022, June 13). *The Age of Hypersonic Weapons is Upon U*. Retrieved from Microwave Journal: https://www.microwavejournal.com/articles/38245-the-age-of-hypersonic-weapons-is-upon-us

Hank, J. M. (2008). The X-51A Scramjet Engine Flight Demonstration Program. *15th AIAA International Space Planes and Hypersonic Systems and Technologies Conference* (p. 7). AIAA.

Le, V. T., Ha, N. S., & Goo, N. S. (2021, December 1). *Advanced sandwich structures for thermal protection systems in hypersonic vehicles: A review*, Volume 226. (Elsevier) Retrieved from Science Direct: https://www.sciencedirect.com/science/article/abs/pii/S1359836821006752

Lumen Learning. (2018, August 3). *17.8 shock waves | University physics volume 1*. Retrieved from Lumen Learning: https://courses.lumenlearning.com/suny-osuniversityphysics/chapter/17-8-shock-waves/

Military-Today. (n.d.). *Hwasong 8 ballistic missile with a hypersonic glide vehicle* . Retrieved from www.military-today.com/missiles/hwasong_8.htm: https://www.military-today.com/missiles/hwasong_8.htm

Military-Today. (n.d.). *Shaurya short- and medium-range ballistic missile* . Retrieved from www.military-today.com/missiles/shaurya.htm: https://www.military-today.com/missiles/shaurya.htm

Military-Today. (n.d.). *Tsyrkon anti-ship cruise missile.* Retrieved from www.military-today.com/missiles/tsyrkon.htm: https://www.military-today.com/missiles/tsyrkon.htm

N.O.A.A. ((n.d.)). *Speed of sound. .* Retrieved from www.weather.gov/: https://www.weather.gov/media/epz/wxcalc/speedOfSound.pdf

NASA. (2019). *Hypersonic tunnel facility.* Retrieved from www1.grc.nasa.gov/: https://www1.grc.nasa.gov/facilities/htf/

Nichols, R. K., Carter, C. M., Hood, J.-P., Jackson, M. J., Joseph, S. M., Larson, H., . . . S. (2022). *Space Systems: Emerging Technologies and Operations (2022).* Manhattan, KS: https://newprairiepress.org/ebooks/47/.

Nichols, R. K., Sincavage, S., Mumm, H. C., Lonstein, W., Carter, C., Hood, J. P., . . . Slofer, W. (2022). *Drone Delivery of CBNRECy – DEW Weapons of Emerging Threats of Mini-Weapons of Mass Destruction and Disruption (WMDD).* Manhattan, KS, USA: New Prairie Press #38. Retrieved from https://newprairiepress.org/ebooks/38/

Nilsen, T. (2021, July 19). *Northern fleet frigate test fires Tsirkon hypersonic missile.* Retrieved from thebarentsobserver.com/: https://thebarentsobserver.com/en/security/2021/07/northern-fleet-frigate-test-fires-tsirkon-hypersonic-missile

Northrop Grumman. (2019, October 14). *STSS satellites demonstration program paves the way for future missile defense*. Retrieved from news.northropgrumman.com: https://news.northropgrumman.com/news/releases/northrop-grumman-built-missile-tracking-satellites-reach-tenth-year-on-orbit

Northrop Grumman. (2023, June 7). *Counter hypersonics*. Retrieved from Northropgrumman.com: https://www.northropgrumman.com/space/counter-hypersonics/

Salia, D. M. (2018, February 6). *Was a space based weapons platform used against Hawaii bound ballistic missile?* Retrieved from Exopolitics.org: https://exopolitics.org/was-a-space-based-weapons-platform-used-against-hawaii-bound-ballistic-missile/

Science Daily. (2021, September 19). *Speed of sound.* Retrieved from www.sciencedaily.com/: https://www.sciencedaily.com/terms/speed_of_sound.htm

Slofer, W. (2022). SATELLITE KILLERS AND HYPERSONIC DRONES. In R. K. Nichols, & C. M. Carter, *Space Systems: Emerging Technologies & Operations.* Manhattan, KS: NPP #47. Retrieved from https://kstatelibraries.pressbooks.pub/spacesystems/chapter/satellite-killers-and-hypersonic-drones-slofer/

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

SOFREP. (2022, January 18). *Strange and Interesting Weapons During The Cold War* . Retrieved from SOFREP.com: https://sofrep.com/news/strange-and-interesting-weapons-during-the-cold-war/

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

Standard Missile-3 (SM-3). (2023, March 9). Retrieved from missilethreat.cis.org: https://missilethreat.csis.org/defsys/sm-3/

Stilwell, B. (20211, September 20). *These Air Force 'Rods from god' could hit with the force of a nuclear weapon*. Retrieved from Military.com: https://www.military.com/off-duty/2020/12/22/these-air-force-rods-god-could-hit-force-of-nuclear-weapon.html

Tingley, B. (2012, July 13). *Navy's New Laser Dazzler System*. Retrieved from thedrive.com: https://www.thedrive.com/the-war-zone/41525/heres-our-best-look-yet-at-the-navys-new-laser-dazzler-system

Tingley, B. (2021, July 12). *Here's Our Best Look Yet At The Navy's New Laser Dazzler System*. Retrieved from Thedrive.com: https://www.thedrive.com/the-war-zone/41525/heres-our-best-look-yet-at-the-navys-new-laser-dazzler-system

Tingley, B. (2021, July 12). *heres-our-best-look-yet-at-the-navys-new-laser-dazzler-system*. Retrieved from thedrive.com: https://www.thedrive.com/the-war-zone/41525/heres-our-best-look-yet-at-the-navys-new-laser-dazzler-system

Tingley, B. (2021, July 1). *Space Force Plans To Place New Early Warning Satellites Into Non-Traditional Orbits Closer To Earth*. Retrieved from The Drive: https://www.thedrive.com/the-war-zone/41383/space-force-plans-to-place-new-early-warning-satellites-into-non-traditional-orbits-closer-to-earth

U.S. Naval Institute. (2020, December 29). *Hypersonic Missiles Coming in Hot*. Retrieved from www.usni.org: https://www.usni.org/magazines/proceedings/2020/december/hypersonic-missiles-coming-hot

USAF. (n.d.). *X-51A Waverider*. Retrieved from www.af.mil: https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104467/x-51a-waverider/

USAF Office of Scientific Research. (2011, April). *Hypersonic Flighgt: Challenging Science & Integration*. Retrieved from Slideshare.net: https://www.slideshare.net/afosr/progress-and-challenges-in-foundational-hypersonics-research

Venose, A. (2016, January 16). *Breaking Point: What's The Strongest G-Force Humans Can Tolerate?* Retrieved from Medical Daily: https://www.medicaldaily.com/breaking-point-whats-strongest-g-force-humans-can-tolerate-369246

Wikipedia. (2003, Nov 28). *OODA loop*. Retrieved from en.wikipedia.org/wiki/OODA_loop: https://en.wikipedia.org/wiki/OODA_loop

Wilson, D. B. (2015, May). *Guidance, Navigation and Control for UAV Close Formation Flight and Airborne Docking*. doi:0.13140/RG.2.1.3167.9209

Yang, J., Nangia, R., & Cooper, J. (2014, July 16). *Optimization Framework for Design of Morphing Wings*. Retrieved from trimis.ec.europa.eu: https://trimis.ec.europa.eu/sites/default/files/project/documents/40418/final1-maws-overview.pdf

14.

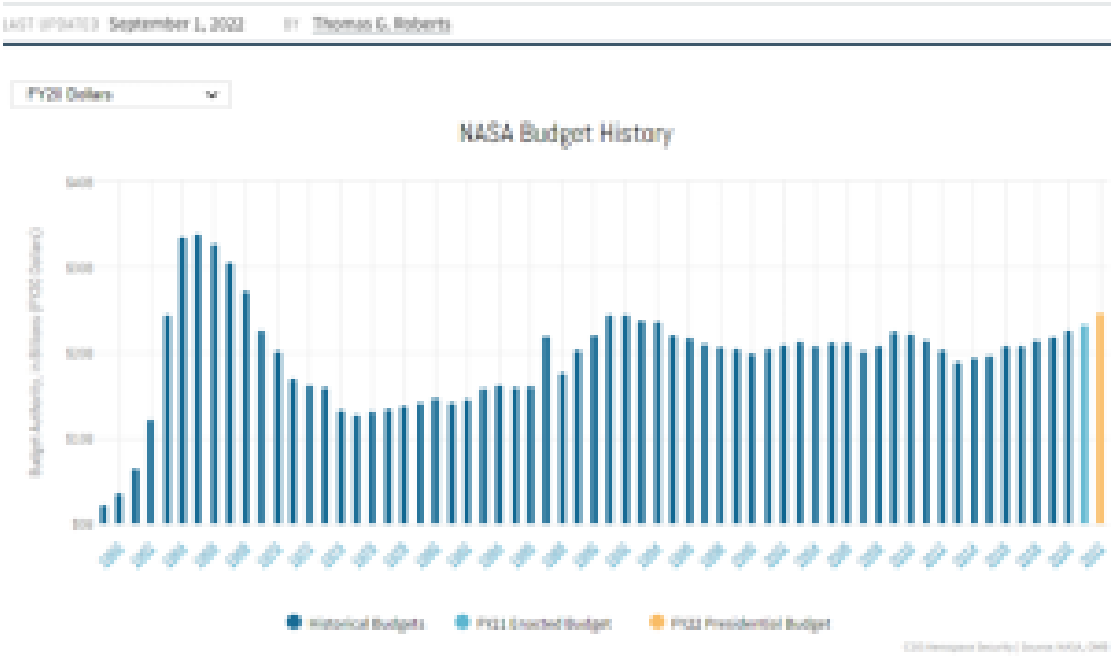
THE RISE OF CYBER THREATS IN SPACE - FUTURE OF CYBERWAR [FARCOT]

HISTORICAL OVERVIEW:

COLD WAR

At the end of the second world war, the rapid advancement of both jet and rocket technologies was overshadowed by the introduction of nuclear weaponry. The bombings of Hiroshima and Nagasaki demonstrated the raw destructive power of atomic bombs to the rest of the world. Shortly after, the Soviet Union conducted its own first successful nuclear tests. This, if anything, was the primary driver for the competition between the US and USSR that would soon become the Cold War. The race for military superiority eventually spilled beyond Earth's atmosphere. Beginning with the Sputnik launch of 1957, a great fear of nuclear weapons being launched from orbit was now taking shape amongst both the public and governments alike. Although these types of weapons were never actually launched into space, surveillance soon became the real threat. Thus, both the United States and the Soviet Union began developing the first satellite killers. These anti-satellite weapons, often referred to as ASATs, were developed as early as May of 1958 during the Bold Orion program (Lethbridge, 1996). This saw the testing of the ALBM-199B, a ballistic missile launched from a B-47. In the decade that followed, other forms of ASAT weapons soon took shape. The USSR even went so far as to develop nuclear-tipped interceptors several years later (Grego, 2012). Eventually, international agreements were reached such as the Partial Test Ban Treaty of 1963. While these types of bans altered both the US and USSR's approach to ASAT weapon development, they never fully put a stop to them. Within the first year of the so-called Space Race, threats against man-made satellites were already taking shape in the form of early ASAT systems. Many of these systems were designed by the Roscosmos group. Today, Roscosmos acts as the de facto continuation of the legacy soviet program and acts as the country's federal space agency, functionally the same as NASA's role in the US.

Figure 14-1: NASA's Budget Since 1960



Source: (Roberts & Harrison, 2022)

CHINESE ENTRY

Despite the end of the first Cold War between the US and USSR, the situation in space has only become more complicated. This is largely due to the entry of new factions in space. The most significant example, at least on the international level, is China, which began its own space program shortly after the US and USSR. However, the program remained small due to limited funding for the majority of the Cold War. In 1970, the first Chinese satellite was successfully launched into orbit, making it the fifth nation to do so (Futron Corporation, 2003). Towards the end of the 20th century, there was a major upscale in Chinese space activity due to a rapid increase in funding. This activity has only intensified into the 21st century and, while the US still dominates in overall yearly spending on its space programs, China has been steadily closing the gap ever since the ~2000 spending boom. Additionally, the country has followed a similar path to the US and Russia with ASAT development. On January 11th, 2007, China's first successful ASAT test using a ballistic missile was conducted, making it the third country to do so since the US and USSR in the 1980s (Kan, 2007). It is clear now that China has matured as the next national player of a newly revived space race.

Figure 14-2: Satellite Capabilities by Country – 1966 to 2020

Source: (Union of Concerned Scientists, 2022)

Figure 14-3: Satellite Capabilities by Country – 1966 to 2020

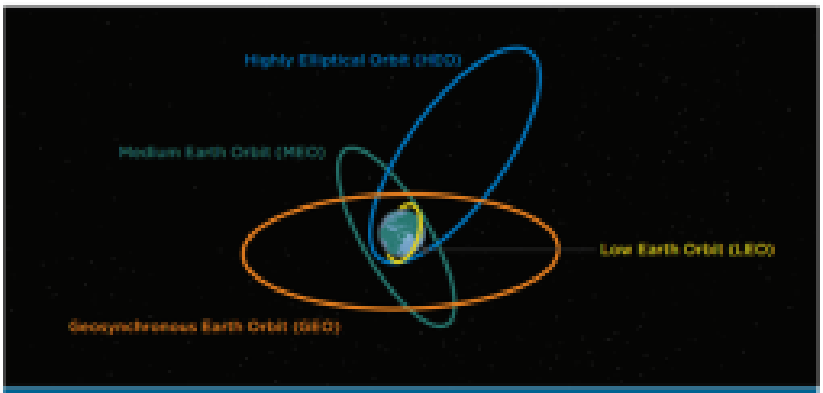
Source: (Union of Concerned Scientists, 2022)

CORPORATIZATION

Despite the entry of new international competitors, the US government has responded with little increases in spending on its own space programs. NASA was eventually forced to end the Space Shuttle program in 2011. While the US still maintained a presence on the International Space Station, it did so with the needed help of the Russian Soyuz rocket, which served to fill the void left by the Space Shuttle. However, NASA is no longer the only US-based organization specializing in space-bound missions. Private corporations that specialize in these types of missions are now often referred to as Launch Service Providers (LSP) (McCall, 2020), have emerged as a major game changer and have kicked off a new Space Race. This time, it is a race more specifically focused on satellite deployment. As of 2023, the largest corporate player so far, in terms of both overall rocket launches as well as satellite deployment, is SpaceX, which began operations in the early 2000s (SpaceX, 2023). Although new to the business of satellite deployment, SpaceX alone has made significant strides through an economically sustainable business model and the development of innovative rocket technology. In many ways, SpaceX, along with Blue Origin and United Launch Alliance, a cooperative between Boeing and Lockheed Martin, have effectively replaced NASA as the sole launch provider for satellites, especially in Low Earth Orbit (LEO). So far, these companies have yet to openly experiment with ASAT technologies, but they nonetheless pose a potential threat to foreign competition both on the national and corporate level.

Figure 14-4: Satellite Orbital Types

Orbit Types and Uses



Orbit	Altitude*	Uses
Low Earth Orbit	Up to 2,000 kilometers	- Communications - ISR - Human Spaceflight†
Medium Earth Orbit	Approx. 2,000 to 20,000 kilometers	- Communications - Positioning, Navigation, and Timing
Highly Elliptical Orbit	LEO altitudes at perigee (nearest to Earth) Approx. 40,000 kilometers at apogee (farthest from Earth)	- Communications - ISR - Missile Warning
Geosynchronous Earth Orbit	Approx. 36,000 kilometers	- Communications - ISR - Missile Warning

* The advantages of higher orbits for communications and ISR are near-persistent coverage of most of the Earth in view of the satellite, with the exception of Earth's polar regions where it is limited. LEO satellites cover all parts of the world, including the poles, but for shorter periods based on the speed of the satellite.

† With the exception of nine U.S. Apollo missions to the Moon, all human spaceflight has been completed in LEO.

Source: (Defense Intelligence Agency, 2022)

In summary, while threats in space originated from two major powers (i.e., the US and USSR), those threats have since diversified to other, more independent groups. Although the US and Russia still maintain their dominance, they now largely do so with the help of their semi-affiliated corporate entities. In many ways, this has made the situation in orbit unprecedentedly complicated. The following sections will attempt to provide a breakdown of the most serious threats posed against satellites today.

THE CURRENT SITUATION:

PLAYERS INVOLVED, INTERESTS

The faction associated with the US and its post-Cold War allies is the most complicated so this will be assessed first, starting with the US government. While NASA still plays an active role in the deployment and maintenance of satellite systems, it no longer receives the same support as it once did before the end

of the Cold War and subsequent collapse of the USSR. Over the course of the three decades since, federal funding for NASA has fluctuated, but overall alteration has been limited. Since 1991, the yearly budget has averaged at just over 20 billion USD (Roberts & Harrison, 2022). However, when adjusted for inflation and considering its shrinking proportion of the US government's total budget, these figures do not seem as optimistic. While the NASA budget Inflation, in particular, can hinder an organization's spending power with major consequences. As such, NASA has been faced with a diminishing capacity to procure necessary assets to maintain its operations. This has led to the termination of many programs, such as the Space Shuttle in 2011. NASA then turned to the Russian-made Soyuz to ferry astronauts to and from the international space station with no primary alternative. But this is just the tip of the iceberg. NASA became so desperate for affordable components that it turned to Russian and Ukrainian manufacturers to make its own rockets, as was the case with the Antares rocket system (Guinnessy, 2014). This partnership only came to an end with the Russian invasion of Ukraine in early 2022. In short, a lack of funding drives NASA to make trade deals with its former rivals, only for those agreements to deteriorate. It may seem like an uncertain situation for the US space program as a whole, but there is another side to this equation.

The newest factor to consider in the case of the US and the western powers is the emergence of corporate launch service providers (LSPs). As of this writing, the most notable of these in terms of development and contribution to satellite deployment is SpaceX. Founded in 2002, the company has blossomed into one of the biggest privately held companies in the world. It is important to note that, even without foreign resources, NASA relies on tech firms like Boeing, Northrop Grumman, and Pratt & Whitney to provide necessary components for every major space mission it plans to embark on. However, these companies have then so relied on Russian-made components due to their affordability. This was, of course, before SpaceX took over the market. Through heavy investments into research and development, improved supply chain management, and years of trial and error, the company has finally been making a name for itself by becoming a primary vendor for NASA and many other satellite operating organizations worldwide. In fiscal year 2022, SpaceX officially became the second largest seller to NASA after receiving just over $2 billion from the space agency (Berger, 2022). Only the California Institute of Technology receives more funding. Before turning the page to foreign adversaries and international competition, it is important to point out that as of May 2022, the US technically owns and operates at least 4529, more than 60% of the global total of 6718 (Union of Concerned Scientists, 2022). When critical of the risk of attacks against or disruptions of US satellite networks, these figures could be considered a vulnerability, as US satellites would be the target of attack or sabotage judging by quantity alone. It also makes these satellites difficult to manage and coordinate, while requiring excessive amounts of funding and resources to maintain. When looking at the total number of US-owned satellites, approximately 4000 are designated as commercial, meaning their operationality is primarily overseen by corporations. A recent spike in orbital objects, most notably payloads, has been attributed to various commercial actors such as ULA and BlueOrigin. However, SpaceX has been responsible for the majority of this growth through the Starlink program, by launching hundreds of satellites into Low Earth Orbit (LEO) since 2019. The company now owns

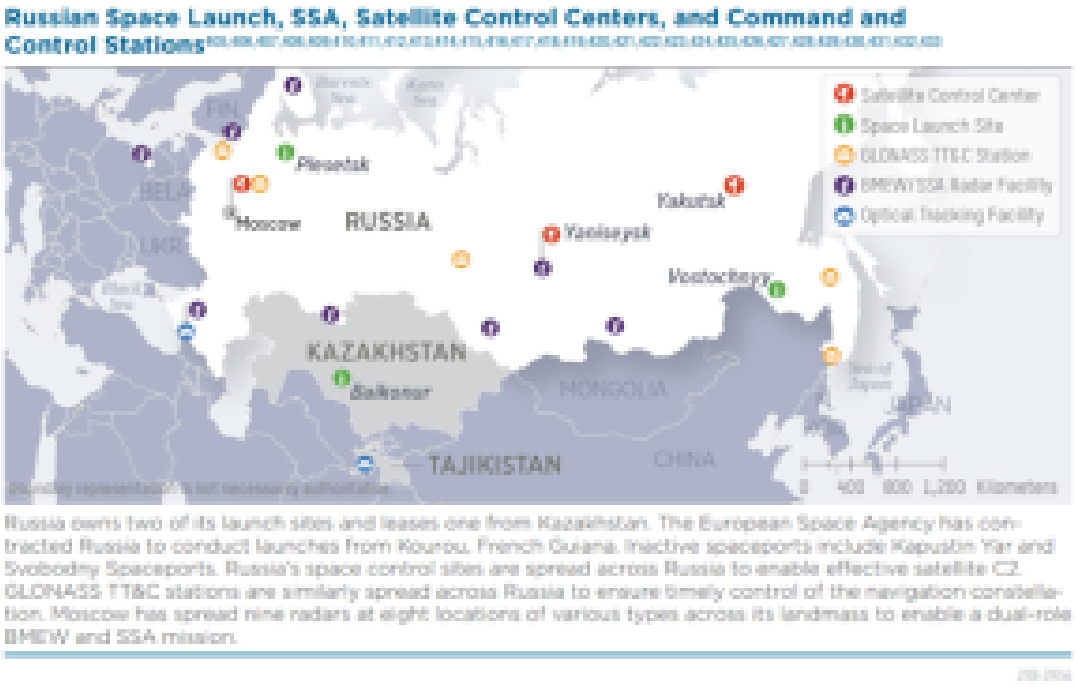
approximately one third of the total number in orbit, making it the largest single satellite owner and provider by far. This new development has been regarded by analytical groups as NewSpace (Boley, 2021). This new era of satellite deployment brings unprecedented challenges, particularly having no one center of authority over private corporations and NASA alike, and the vast majority of satellites being deployed by corporations with no direct government ties. Analysts have also predicted that as many as 25,000 could be launched by 2031, the vast majority will be commercially (Garino, 2018).

Turning the page to foreign competition, the most obvious faction is the oldest known adversary to the US in the Space Race, and that is Russia. Despite being diplomatically and economically shunned by the international community since its invasion of greater Ukraine in February of 2022, Vladimir Putin has made repeated claims that the Russian space program would push on with its concurrent projects. These include the Soyuz and Luna-Glob programs, the latter of which focuses on the establishment of a lunar base and is a continuation of the soviet Luna program. Since the end of the Cold War, the country has ironically become one the USs' largest foreign vendors in rocket and orbital technologies. The other side to this coin is China, which became significantly involved in satellite deployment recently. Through its worldwide initiative to invest in developing nations' economies, often referred to as Belt & Road, China has been able to establish bases and staging areas overseas and in some instances on the polar opposite side of its default location on the globe. For example, the El Sombrero Station in Venezuela has been used as a satellite launching facility since as early as 2005, when the Venezuelan government signed an agreement with the Chinese state-owned Great Wall Industry Corporation to assist in Venezuela's own satellite program (Krebs, 2023). It should also be noted that the Chinese have overseen the construction of as many as a dozen ground control stations across the South American continent in the time since. Chinese expansion in countries on the opposite side of the globe are indicators of a rapidly developing space program. The country recently established its fourth national launch facility on one of its southern islands. While Russia's attention remains focused primarily on Ukraine and the military assets involved there, China's ambitions for global hegemony are heavily affecting control over space. Between 2019 and 2021, the number of operational Chinese satellites doubled to 500, while major global investments have been drawn for Chinese startups intending to compete with the US and SpaceX (Garino, 2018). Both China and Russia believe superiority in space to be essential to their national security policy. Recent pacts between the two countries enforced by common geopolitical interests have created a common threat-actor for US and allied-owned LEO satellites.

Figure 14-5: Chinese Ground Stations

Source: (Defense Intelligence Agency, 2022)

Figure 14-6: Chinese Ground Stations



Source: (Defense Intelligence Agency 2022)

TECHNOLOGICAL ADVANCEMENTS AND CURRENT CAPABILITIES

As we move into a new chapter of space commercialization the global geopolitical landscape has shifted dramatically in large part due to the changing power dynamic in space. In contrast to the straightforward Red vs Blue, NASA vs Soviet matchup of the Cold War, the modern environment of high-tier outer-atmospheric actors has diversified significantly. Since the dissolution of the USSR, financial and technological resources along with the ingenuity to use such resources have expanded to corporate entities, specifically those based in North America, Europe, and Asia, with China entering as a new major player. While the US government still maintains overall authority in space, it must now channel that authority through a vast multitude of organizations, both federal and corporate. This has overcomplicated the way operations are coordinated in space. The voices of authority are no longer just emerging from the White House and the Pentagon. Executives of companies based around the country and with differing interests now control the means to deploy satellites. The capacity to do so and the capabilities of such satellites have dramatically increased throughout the 21st century. As a result, more reliable satellite networks like the GPS and NOAA as well as high speed internet have been introduced and/or maintained by government contracts, major tech companies, and private service providers alike. The introduction of satellite-based internet service has become highly

disruptive both commercially and militarily. Improvements in the reusability of modern rockets is allowing more of these satellite networks to be deployed at LEO and other orbital levels.

The greatest feat that SpaceX has ever accomplished in the grand scheme of the Space Race itself is its contributions to advancing **reusable rocket technology**. Currently we are seeing its attempts at advancing the Starship initiative which is, as of this writing, still in the testing phases of development. Unsurprisingly these attempts have thus far resulted in the spectacularly fashioned explosions that the company is now well known for. However, this is SpaceX's biggest virtue. Its willingness to push boundaries while also being able to financially whether the inevitable failures that initially arise are what have propelled it to become one of the most successful privately held tech companies thus far. Without trial, there may be no error, but there is also no success, and no entity in the United States has undergone such an intense amount of trial and error as SpaceX has since NASA during the 1960s. While the Space Shuttle program was the first to actively reuse rocket boosters at least once after the initial launch, a private company became the first to autonomously return them directly to the launch pad. The B1049 reusable rocket booster, unveiled by SpaceX in 2018 for the Falcon 9, set a record of six consecutive launches with minor refurbishments needed in between with another being used at least fifteen times in total (Reed, n.d.) This and many other B10 boosters have been partly responsible for the deployment of not only the Starlink satellite network, but those of various other companies including SkySat, Telstar, and Iridium (Thompson, 2020). The biggest seller of these rocket systems, and a major economic reason to develop reusable rockets in the first place, is their ability to make satellite launches excessively affordable to a growing pool of potential customers. The result was an unprecedented spike in satellite deployments over the past decade, attributed to the so-called NewSpace revolution (Union of Concerned Scientists, 2022).

Figure 14-7: SpaceX Starlink Satellite Deployment

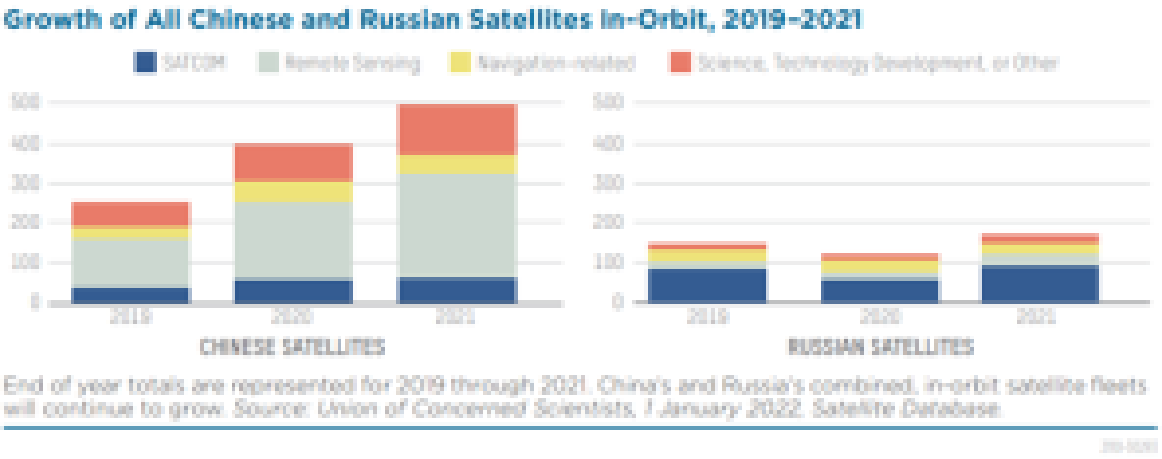
A fleet of SpaceX Starlink internet satellites is seen poised for deployment in orbit in this file image from a May 24, 2019 launch. (Image credit: SpaceX)

Source: (Malik, 2022) & (SpaceX, 2023)

This technological revolution was obviously highly disruptive, especially due to the rapid establishment of **satellite-based internet and communication networks** by private LSPs. This can be seen as an economic threat to potential competitors on the international level, within the private sector but also Chinese-controlled companies that serve similar functions. Geely, for example, now owns several major automotive groups under its umbrella, including Volvo, but has been rapidly expanding to satellite manufacturing, and has boasted plans of producing at a rate of 500 per year by 2025. Another Chinese startup known as GalaxySpace intends on competing directly with SpaceX's Starlink program by providing an integrated satellite/terrestrial 5G network via at least 1,000-satellites (Garino, 2018). The true concern isn't the absorption of foreign industries or even the rapid growth of startups, but rather the Chinese central government having far more control over its domestic companies than that of the US. The security risks that come with Chinese tech companies involve espionage, sabotage, and general data mining which have been demonstrated by ByteDance (Roth, 2021), through TikTok, and DJI (Upward, 2022), the world's top producer of small UAS. Both companies are accused of mishandling user data as well as for their roles in Chinese surveillance and censorship campaigns against the Uyghur minorities in Xinjiang. These incidents show how cooperative Chinese companies are with the CCP itself. The same comparison obviously cannot be made for the US government and US-based corporations.

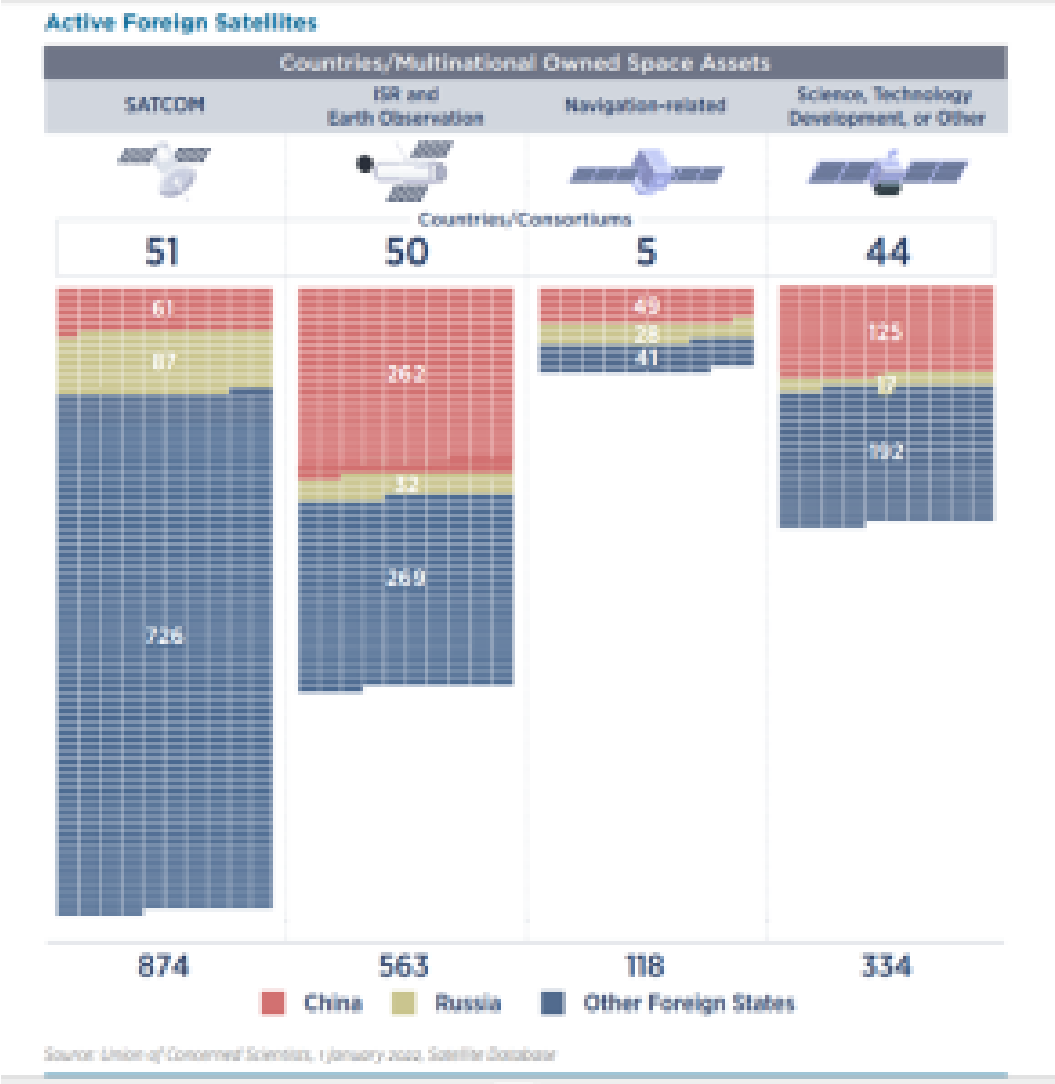
In a sense, the previous reliance on foreign government technologies in order to send US assets into orbit e.g., Russia's Soyuz rocket, would have been considered a major vulnerability. The potential threat of souring diplomatic relations, whether due to a war in Ukraine or otherwise, could result in a major disruption of an already questionable method of ISS astronaut ferrying. Thus, the transition to relying on US-based firms in times of reduced government funding is a necessary countermeasure to reduce the risk of losing a reliable transportation system to and from the ISS. However, the US government's newfound reliance on private corporations can be seen as a double-edged sword, at least from a diplomatic standpoint. According to the 1967 Outer Space Treaty, the US government technically holds responsibility for these firms' activities (Zedalis, 1978). Incidents such as the supposed near collision between Starlink satellites and a Chinese space station are just tastes of how easily this treaty can encourage excessive exchanges of blame and accusations between factions without any actual attack even happening (Hitchens, 2022). This is why the increasing congestion of space stations, vehicles, debris, and satellites in orbit can be seen as a major threat to both the unhindered operation of satellites in orbit and the US's international image as a competent world leader in space. Man-made debris is also an example of how human activity in space can contribute to environmental hazards. This problem will only continue to worsen, as the introduction to satellite-based Wi-Fi internet has triggered a race to establish the best satellite-based Wi-Fi network in the world. This opens the door for not only cyberattacks and satellite killers, but the environmental threat of mid-orbit collisions. Tens of thousands of additional satellites are expected to be launched by the end of the decade.

Figure 14-8: Current and Future Projection of Active Satellites in Orbit



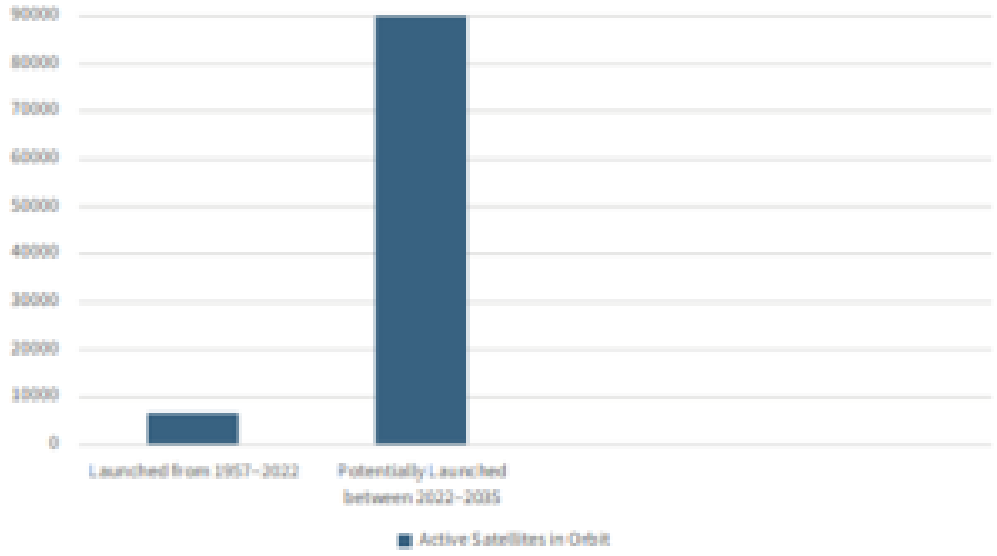
Source: (Defense Intelligence Agency, 2022)

Figure 14-9: Current and Future Projection of Active Satellites in Orbit



Source: (Defense Intelligence Agency, 2022)

Figure 14-10: Current and Future Projection of Active Satellites in Orbit



Source: (Garino, 2018)

In addition to improved payload deployment, ASATs have continued to evolve long after the end of the Cold War. As of today, there are four major nations that are actively researching anti-satellite weaponry. The US and Russia have been developing ASAT weapons since the 1960s, while China and India began around the end of the Cold War (Garino, 2018). The most surprising modern problem involving ASATs, however, did not involve their destructive potential of other satellites, but the creation of the majority of all man-made debris currently in LEO. Since 2007, about half of all the debris currently LEO was generated by man-made events, two of which were direct-ascent, kinetic kill ASAT tests (Defense Intelligence Agency, 2022). Despite Cold War-era international agreements discouraging the use of these types of weapons, it has not stopped these four powers from testing and further developing them for use in the near future. Today, the real hazard of using these types of ASATs is in the potential fallout of debris generated by the target's destruction. This, in turn, further increases the environmental threat of debris and potentially destructive space objects overall. Given today's worsening geopolitical climate over disputes such as Taiwan and Ukraine, the possibility of these weapons being used cannot be ignored

SATELLITE SYSTEM OVERVIEW ; RELATION BETWEEN GROUND, LINKS, & SPACE

A typical satellite system, such as the US Global Positioning System, consists of the following segments: User, Control, and Space. In the case of the American GPS satellite network, the User segment is considered the most secure, as it primarily receives signals from the satellites rather than transmits back. The Space and Control segments, on the other hand, are monitored and maintained by the US Space Force. In the case

of US government-maintained systems, the only control points of the *Control segment* are staffed by US personnel and tasked with tracking the network's satellites as well as updating and uploading navigational data (US Government, 2021). This leaves the *Space segment*, which primarily consists of the physical satellites themselves. Among the most common threats in this segment are obvious environmental hazards including small rocks of various origins and debris created from destroyed older satellites. These types of threats are always constant, yet they are oftentimes overlooked, at least more so than the ASAT and cyber/remote threats. While theoretically, these hazards will be slowly mitigated with the gradual improvement of monitoring and detecting equipment over time, increasing human activities, particularly those at LEO levels, are driving the threat far in the opposite direction, but this is a threat that will be elaborated in a later subsection. The more immediately mitigatable threats are those imposed by hostile foreign powers (i.e., China, Russia, Iran, & North Korea) including but not limited to: Cyber-weapons, Kinetic-Kill ASAT weapon systems, and Electronic Warfare. One of the most common manifestations of these threats is remote jamming. Such as GPS jammers employed by Russia.

Figure 14-11: Legacy GPS Jammer

Russian GPS jammer. (National Air and Space Intelligence Center photo)

Source: (Garino, 2018)

EFFECT OF SURFACE CONFLICTS ON SPACE SYSTEMS

Satellites have become essential to successfully conducting large-scale modern warfare. From navigation to surveillance to communication, satellites have become smaller and far more numerous in just the past several decades (Smith, 2011). This is because of the simple strategic advantage of relying on many cheaper, smaller units to fulfill a purpose rather than a few, more sophisticated and expensive ones. It is also in part the same reason so many mobile network providers, such as Verizon, continue to expand and develop their own infrastructure, which is to simply increase and improve overall coverage. With the rise of private LSP companies, overall satellite deployment expenses have significantly declined, opening the financial door to many big tech and government groups planning to launch their own networks. The "Starlink" internet network has been undergoing significant expansion, receiving a significant boost with the 2022 Russian Invasion of Ukraine. As of May 2023, there are more than 3500 operational SpaceX Starlink satellites in orbit (Dobrijevic, 2023). While the idea of mass-production and deployment may in many ways improve the overall reliability of a satellite network, it also simultaneously increases the vulnerability of that system being attacked from an external force, whether it be environmental (asteroid, debris) or man-made (anti-sat, cyberattack). The more operational satellites in a constellation, the more difficult it will be to manage each satellite as more resources and manpower will be needed to successfully maintain network operations.

In Wartime, satellite control has become essential, and not just merely for surveillance. Russia's targeting of SpaceX satellites to disrupt the Starlink network over Ukraine was just a taste of what could come in future conflicts elsewhere as satellite internet networks become globally established. These new satellite fleets have become critical communication arteries for militaries in situations like Ukraine's. In this case the strategic value was so high for Ukraine that Russian officials expressed concern over Starlink's military capabilities months before the February 2022 invasion of Ukraine and proceeded to launch cyber-attacks against the network once Musk announced its operationality over the country (Kolovos, 2022). Russia even flirted with the idea of using kinetic ASATs against Starlink satellites, even though doing so would be considered an act of war. This is still a threat worth considering though, as the invasion of Ukraine is one of the only ongoing military conflicts that directly involve at least one major space power. Losing an advantage on any front, including LEO satellite coverage, can be a major strategic disadvantage. Therefore, it can be assumed that Russia, or any other nation in a similar position, would resort to violating any agreements barring the use of ASATs against foreign-owned satellites if it felt pushed to do so.

KNOWN THREAT ASSESSMENT

RELATIONSHIP BETWEEN THREATS & RISK

There are four factors that should be considered when determining Risk: Threats, countermeasures, impacts,

and vulnerabilities. (Nichols R. K., 2022) (Nichols, et al., 2023) Threats increase overall risk while countermeasures reduce it, thereby acting against each other. Vulnerabilities and impacts also increased risk and compound to each other along with threats. Here is an example of these factors affecting Risk: Suppose a large cluster of SpaceX satellites is being deployed in LEO, but on the same day, an unannounced CCP anti-satellite weapons test is occurring at a similar altitude. This would increase the Risk of asset loss during the deployment stages of the already massive satellite fleet because of the *vulnerability* of a high target count and the possible *impact* of the company being set weeks behind schedule, not to mention the billions of dollars in assets lost. The *threat* in this scenario is the unpredictable debris fragmentation generated by the ASAT test. A potential countermeasure could be an early warning system that somehow detects the debris and delays further deployments. But given the poor timing and lack of coordination between the parties at play, Risk of asset loss would still be significant during this event. This chapter, and the research conducted for it, is dedicated to threat assessment, specifically any threat that significantly increases the Risk of losing US and allied satellites currently operating in orbit along with those that rely on them. Research was focused on anything that was meant to increase the likelihood of destruction, damage, or sabotage of friendly satellites. Vulnerabilities are also heavily acknowledged as they serve to provide a better understanding of the threats discussed in this chapter. A threat exploits a vulnerability, amplifying the effect on overall Risk. From early assessment all known threats against operational satellites in LEO come in three forms: Environmental, Remote, or Physical. A significant increase in overall human activity and general congestion in LEO have contributed to worsened environmental hazards, i.e., debris. Remote attacks with cyber and/or electronic weaponry can also be made directly on satellites in orbit or the ground segment of satellite systems through the respective control station(s). Other miscellaneous threats include the ever-present possibility of internal satellite system failures, which are less likely and more dependent on the reliability of the provider(s). (Way, 2022)

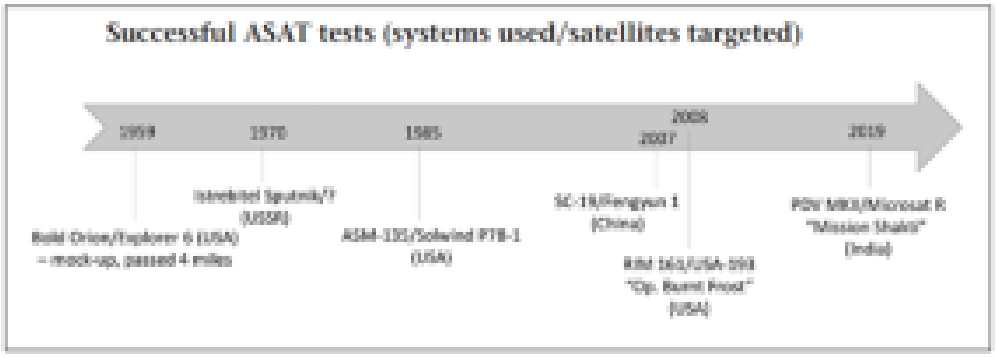
THREAT EVOLUTION

THREAT 1: KINETIC KILL ANTI-SATELLITE SYSTEMS

Commonly referred to as 'ASATs,' these weapon systems follow one of two principles: either direct-ascent or co-orbital, the former of which seems by far the more prevalent concept in reality. Direct-ascent weapons use some form of trajectory to intercept a target in orbit without putting itself into orbit as well. On the other hand, a co-orbital weapon system does just that by placing itself in an identical or similar orbital pattern as the target in order to eventually eliminate it through either direct collision or some form of sabotage (Defense Intelligence Agency, 2022). The vast majority of the weapons systems being developed for ASAT purposes are in the direct-ascent category. In the 21st century, new actors have been garnering more attention with these types of weapons. China's 2007 test of a ballistic missile destroying an old PLA weather satellite in LEO was the nation's first successful demonstration of a direct-ascent ASAT in action (Kan, 2007). This brings to light a new arms race that isn't limited to two superpower states and aims to reshape near-Earth

space. A lack in international law and defense agreements pertaining to anti-satellite weaponry has allowed the technology to boom unchecked. One of the biggest reasons the threat of anti-satellite weaponry is ever-increasing is due to escalating tensions between major powers, not just between the US, Europe, and Russia, but also specifically China, Pakistan, and India. While the concept of anti-satellite weapons is by no means unique to the 21st century, there has been renewed interest in the technology for two primary reasons: the first is that any treaties or agreements that do pertain to anti-sats, the rules are not specific or up to date on terminology (e.g., what constitutes as "Arms") (Sönnichsen, 2020). A more recent example of ASAT testing was India's 'Mission Shakti,' demonstrated when a ground-launched interceptor missile was used to destroy an Indian earth observation satellite in LEO on 27 March 2019. The 'Mission Shakti' test destroyed Microsat-R, which was deployed as an intentional target as it had itself only just been deployed two months prior. The usage of evident 'dummy' satellites and their relative ease of deployment combined with an ever-intensifying surface-to-air weapons arms race highlights the impending threat of a rapidly deployable ASAT system with surface-to-air capabilities. The vulnerability of highly dense satellite 'mega-constellations' presents a target-rich environment. The future of ASATs poses an even more concerning outlook for the safety and operation of satellite networks. China, for example, has begun development of laser-based direct energy weapons (DEW), which could potentially damage or destroy satellite sensors, both optical and non-optical (Defense Intelligence Agency, 2022). As the usage of ballistic ASAT weapons becomes less practical for all major powers, the transition to DEWs may come well within the next decade.

Figure 14-12: ASAT Testing Timeline



Source: (Sönnichsen, 2020)

THREAT 2: ELECTRONIC/CYBER ATTACK

One of the more overlooked threats against satellites is that of a cyberattack, in fact, it is the greatest general threat when determining risk. This is because every satellite, regardless of purpose, must have some type of

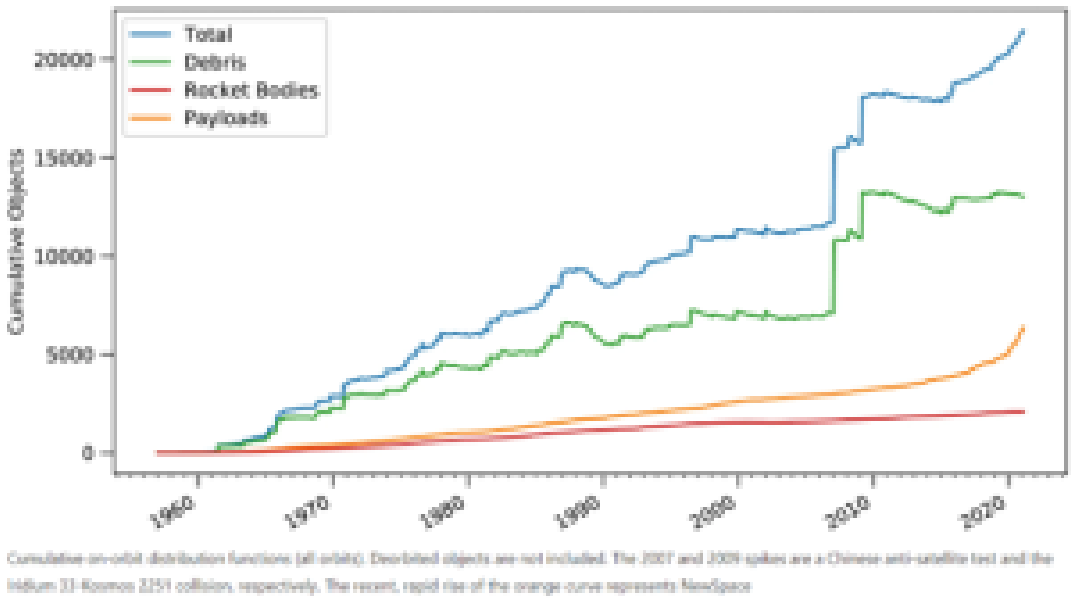
established radio-communication link with at least one control point or ground station on Earth in order to be useful in some form. This very link alone represents a serious vulnerability by default, and therefore allows for the specific threat of malicious actors broadcasting signals that could impede the proper functionality of a satellite network. The aforementioned ground stations are often considered less secure than the satellites themselves simply due to the ground station's need for network connectivity. This is why many previous cyberattacks, such as the ViaSat attack on the eve of the Russian invasion of Ukraine, have explicitly and successfully targeted the ground segment of these networks (Boschetti, 2022). In the rapidly expanding small-satellite industry, the combination of Commercial Off The Shelf (COTS) and open-source software brings additional security vulnerabilities to the satellites themselves. In large arrays of small satellites, the software and hardware rely on some form of redundancy for each satellite to be compatible and communicative with each other. These so-called "satellite constellations" are often considered larger targets than standalone satellites not just due to the size of the fleets but the high number of ground control points needed to communicate with them. Other cyber-security-related vulnerabilities include poor encryption, inconsistent software patching, and the usage of older, legacy equipment for operations (Holmes, n.d.). Prime targets for cyberweapons and cyberattacks in general are ground control stations and the personnel that work there. Generally speaking, the majority of cyberattacks can be attributed to breaches from, usually unwitting, insiders. When focusing on satellite systems, however, entire nation states are attempting to breach these networks. These obviously include Russia and China as they each follow policies adhering to the pursuit of data and information "superiority" (Defense Intelligence Agency, 2022). Russian jamming of Starlink satellites in light of the Invasion of Ukraine prompted SpaceX to ramp up its operations over the nation. This, of course, has since made the network a prime target for Russian jamming efforts throughout the ongoing invasion. The Starlink V1 network itself proved to be highly insecure, allowing Russian military units to single in on user positions in minutes, prompting the company to relay warnings on how to use the service as it became the only non-Russian provider operational in the whole of Ukraine shortly after the invasion began (Malik, 2022). SpaceX boasts that the Starlink V2 fleet being deployed was designed to provide additional security with increased traffic, but the reliability of jamming techniques has persisted as it will continue to do so in the foreseeable future. This remains the case for all communications-based satellite networks. In regard to more complex, direct cyberattacks aimed at stealing information or data, the target will far more likely be a ground control station and/or its staff.

THREAT 3: ORBITAL COLLISIONS

A new threat has emerged recently regarding the rapid influx of hazardous LEO objects in little over a quarter century. This was initially a minor threat early during the Cold War, but increased human activities in space and LEO in particular are gradually turning this issue into one of the primary threats against operational satellites. It is also a universal threat, unlike those previously assessed, meaning a threat posed to every stakeholder of operational satellites worldwide. The reason for this is the destructive potential of LEO

collisions, whether it be with another satellite or debris. This threat was brought to reality when, on 10 February 2009, a decommissioned Russian communications satellite, Cosmos 2251, collided with the operational Iridium 33 satellite, owned, and operated by a Virginia-based telecoms company of the same name. The collision generated over 1300 documented pieces of debris (Kelso, 2009). Objects generated from events such as these are tracked and recorded individually by groups including the US Space Surveillance Network (SSN) and the European Space Agency. However, potentially lethal objects that are not tracked by these groups are the most unpredictable and most concerning threat concerning orbital collisions. While groups like the SSN are not able to directly monitor the objects in LEO, they can at least make estimates based on previous events, such as orbital explosions and collisions that occurred and the fragmentation generated by them. The SSN designates these objects as lethal non-trackable debris (LNT). As of January 2022, it was estimated that between 600,000 and 900,000 LNTs exist in LEO (Defense Intelligence Agency, 2022). There are also 1300 objects, each with a mass exceeding that of an automobile, which are currently being tracked in LEO

Figure 14-13: Man-Made Space Objects



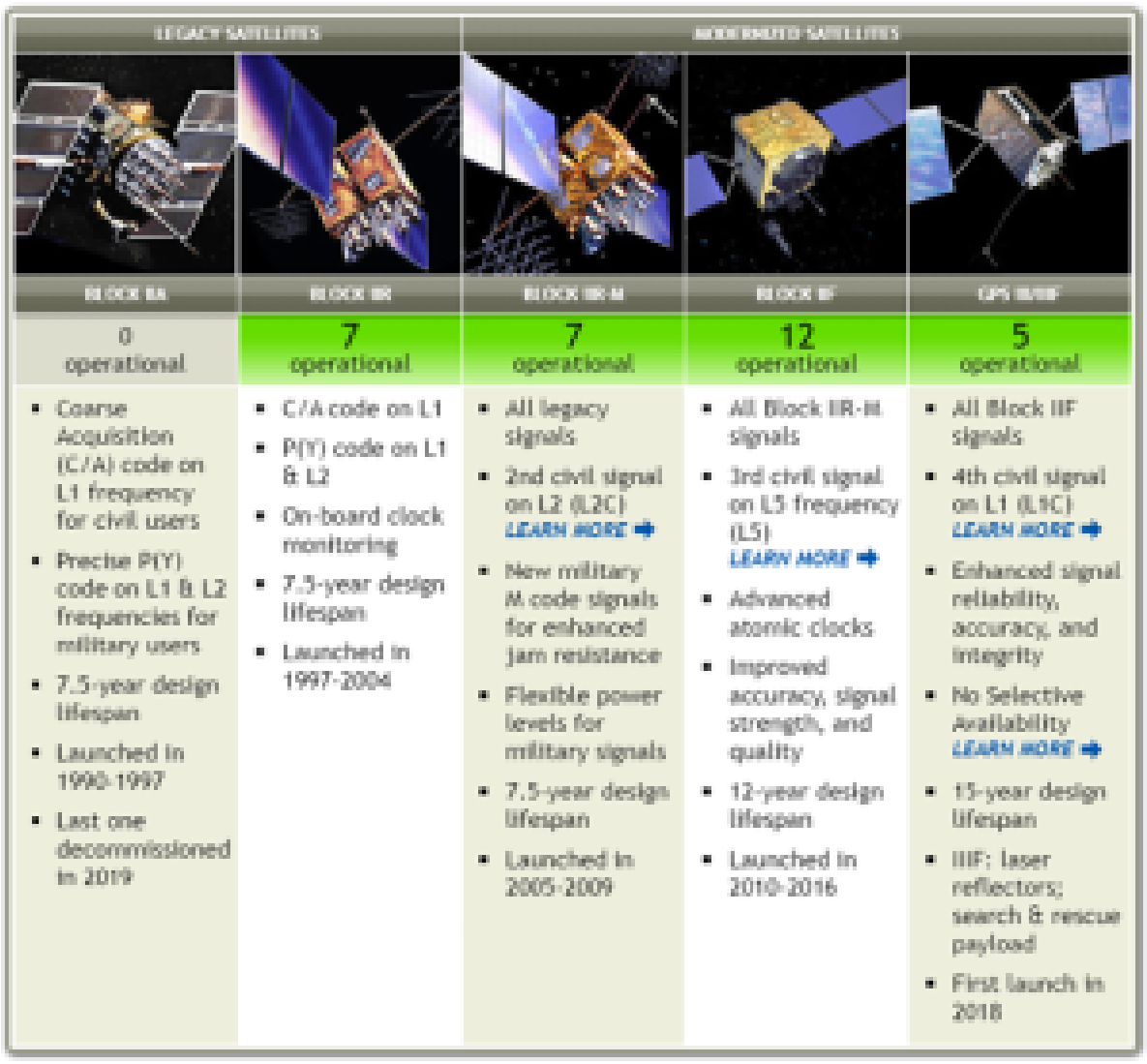
Source: (Boley, 2021)

VULNERABILITIES ACKNOWLEDGEMENT

When assessing variables in pertinence to Risk, it is essential to note that Vulnerabilities multiply the magnitude of Threats. Age, and the resultant decline of sophistication, is an often severely overlooked vulnerability when referring to satellites in orbit. A more unexpected threat may target decommissioned legacy

satellite systems. These satellites are by no means dead and are still in orbit to this day. The biggest issue with these systems is that, while they may no longer be used by the entities that were responsible for deploying and maintaining them, there could very well still be entities using them for their own gain. This is because satellites rely on ground stations to establish and maintain a stable communication link, otherwise the satellite would be useless. But ground-based links can easily be manipulated once the founding party has turned its attention away from so-called "retired" satellite systems. In 2022, researchers intentionally hacked the Anik F1R satellite launched in 2005 and successfully broadcasted malicious signals (Zarley, 2022). Generally speaking, the older the system, the more vulnerable it becomes to these types of attacks. Ground station security is also a major factor in determining the vulnerability of the respective satellite system. Any software glitch that can be exploited in a potential cyberattack is a vulnerability. When discussing satellites in LEO, first of all, an immediate vulnerability would be the proximity to most ASAT systems capable of reaching orbital levels. Since LEO is the lowest general orbital altitude attainable, it is cheaper to launch satellites at this level than at higher altitudes like GEO. There are also thousands of other satellites also operating in LEO, making it highly congestive and contested. In short, these are vulnerabilities of any satellite currently in LEO. The age and capabilities of the satellite systems in question would further determine the overall vulnerability of the system. For example, a twenty-year-old legacy GPS satellite would be far more susceptible to remote sabotage due to outdated systems and communications capabilities than a modern one. Furthermore, many of these satellites in orbit today are operating at up to four times their original life expectancy. The GPS network in particular is made up of thirty-one operational satellites, the network still operates with at least six designated "legacy satellites" launched prior to 2005 (US Government, 2022). Under the correct circumstances, the GPS network itself could be spoofed and an attacker would be able to inject false data into the communications systems. This could trick the system into calculating incorrect position, resulting in false data being presented to the user (King, 2020). While GPS operates at medium Earth orbit, other networks in LEO rely on hundreds of satellites to provide their services. SpaceX's Starlink network is considered the largest by far, reaching over 1200 units in just the initial two years of deployment (Garino, 2018). In doing this, SpaceX has presented an interesting strategy to address Russian cyber-attacks. By mass-producing and deploying hundreds and eventually thousands of satellites in order to achieve maximum coverage, the overall vulnerability of losing service in targeted attacks is reduced, at least for SpaceX and its Starlink users. This is due to the idea that the producers can develop and deploy units faster than they can be decommissioned. Nonetheless, this does not escape the ever-present reality that as a system ages, it becomes gradually more vulnerable to attack. This is a reality faced by every satellite network. In short, when considering the vulnerability of a satellite system, age, altitude, satellite and control station quantity, and strategic importance are all factors that should be immediately considered, whether for networks like Starlink or GPS.

Figure 14-14: GPS Satellite Fleet



Source: (US Government, 2022)

THREAT SUMMARIES & CONCLUSIONS

ANTI-SATELLITE WEAPONRY

An ASAT in this context serves the purpose of disabling a satellite by any physical means. These disabling techniques can involve either dismantling or destroying the device, or simply knocking it off of its orbital path and into a decaying one that eventually results in its destruction. Examples of Direct-Ascent ASAT weapons include Surface/Air-to-Space missiles, Kinetic Kill vehicles, Direct Energy Weaponry, and potentially any lethal projectile capable of reaching LEO altitudes. One of the most well-known demonstrations of these weapons was the destruction of the Chinese PLA weather satellite Fengyun-1C, which occurred in January 2007 at an

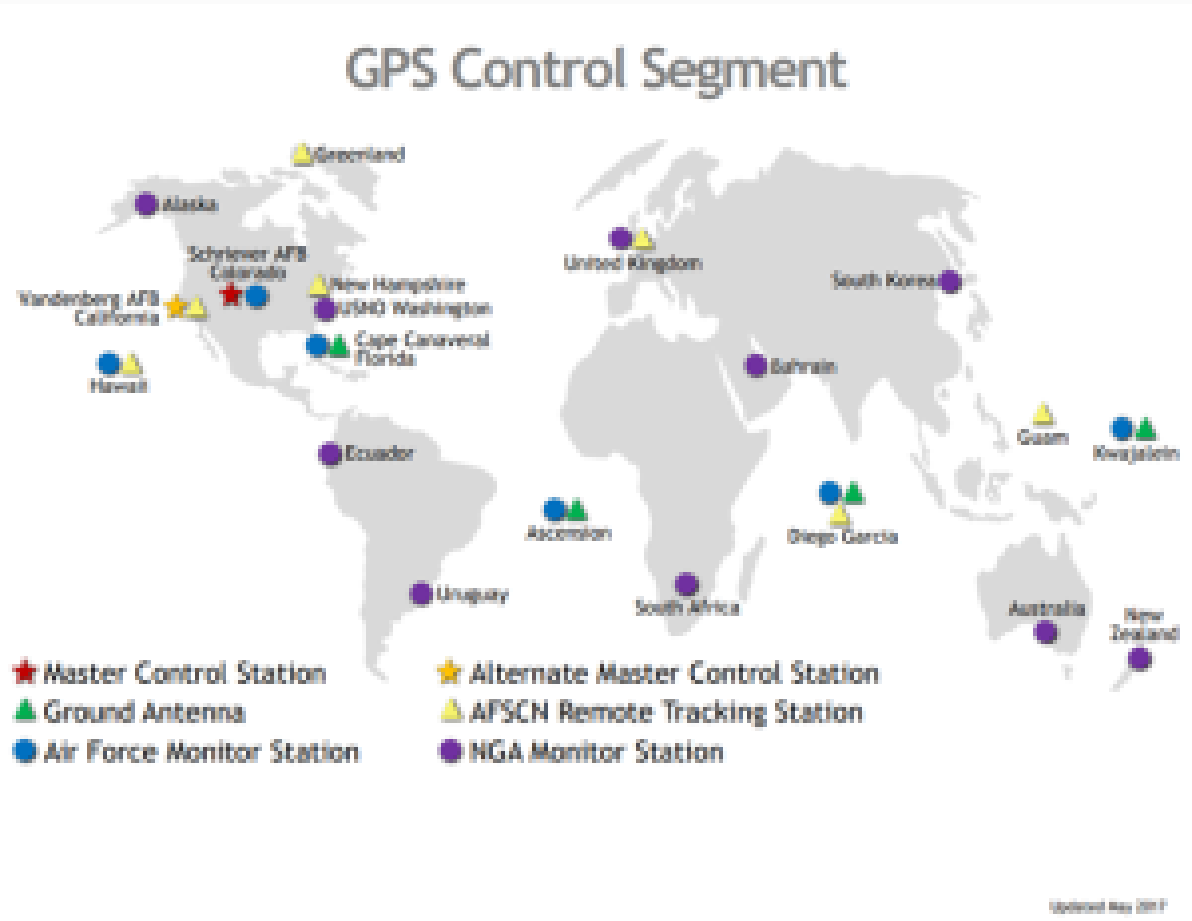
altitude of over 800 kilometers (Defense Intelligence Agency, 2022). Co-orbital weapons are not as prevalent but can include space mines, robotic arms (used to either dismantle or push), as well as other satellites. The vast majority of ASAT tests is surface-based projectiles, similar to those used in the 2007 and 2021 incidents. So far, ASATs have been used solely on one faction's own assets either to evaluate their capabilities or to physically destroy decommissioned satellites still in orbit, the numbers of which still rival currently active satellites (Slofer, 2022). The use of ASATs against another nation's satellite would increase tensions beyond a reasonable level, so much so that even Russia will not even risk it. In a way, an ASAT can be analyzed in a similar sense to a hypersonic missile, EMP, or even a tactical nuke; it is likely that they will only be used as a last resort and any use of such weapons will be limited. When accounting for debris fragmentation in LEO, however, the incentive to avoid using these weapons to attack enemy satellites in space heavily outweighs those for not doing so. This is because of the vast amount of orbital debris that has accumulated due to ASAT tests in the past quarter century. For this reason, the threat of ASAT usage is surprisingly lower than initially expected, but the ability for this type of weaponry to create other threats in space, i.e., debris, boosts their final threat level and this time for all parties involved.

REMOTE THREATS

One could, in a sense, consider cyberweapons and electronic warfare components to be remote ASATs. Their end purpose is more complicated, however. Rather than decommission a given satellite system by physically destroying its assets, these threats seek to gain access to the system and hijack it for another purpose. These methods include hacking and spoofing, which can be committed in a variety of ways including targeting the ground control stations established to maintain the satellite system through the 'ground' segment. In most cases these facilities are the key to gaining access to the rest of the satellite system. These stations could vary in quantity and defense capabilities depending on the satellite network in question, but these stations remain more vulnerable and prone to attack than the satellites they manage in orbit (Garino, 2018). Furthermore, as satellite-deploying companies expand on the services they provide, i.e., internet, they have made themselves far more prone to cyberattack and attempts to sabotage through remote means. We've seen a perfect example of this happening to SpaceX's Starlink network during the first year of Russia's invasion of greater Ukraine. These types of attacks, which mostly involve jamming techniques, have been conducted by Russia in other nations long before the 2022 invasion, but it is a method Moscow has settled into during times of war. On the other hand, no ASAT attack of kinetic or any other direct or co-orbital approach has been conducted on another party's satellite, even over Ukraine. Meanwhile, EW and cyber-based threats have significantly influenced Chinese military reforms over the past decade, often employing cyberespionage against rival space powers, mostly European and North American satellite, and aerospace industries (Defense Intelligence Agency, 2022). As demonstrated by Russian jamming of SpaceX Starlink satellites over Ukraine, jamming technology remains the most probable threat based on experimental analysis. While it may pose a lower lethality when compared directly to ASATs, satellite communication disruption is a useful tactic often practiced heavily by Russia since

the beginning of the Space Race and is currently one of the biggest threats against satellites over Ukraine right now. As a final note, it is important to consider the unique role that the ground segment plays and its, therefore, increased likelihood to be targeted in an attack.

Figure 14-15: GPS Ground Control Stations



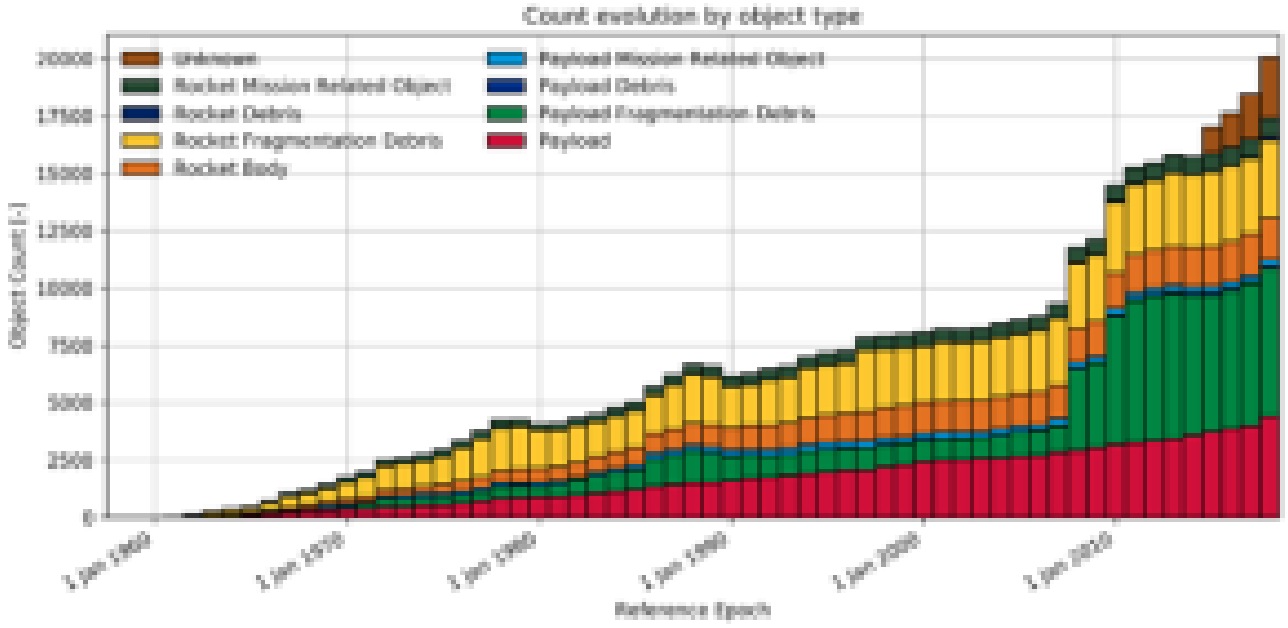
Source: (US Government, 2021)

ENVIRONMENTAL ELEMENTS

By far the most viable environmental threat in Earth's orbit is the debris that has accumulated due to human activity in the past half century or so. In fact, overall congestion, particularly in LEO, is a hazard that everyone now needs to deal with. Upon concluding this research, it was surprising to see just how congested the overall environment at LEO has become with debris and satellite fragments as well as just how much human activity has contributed to this congestion. Specifically, human-generated debris within just the past two

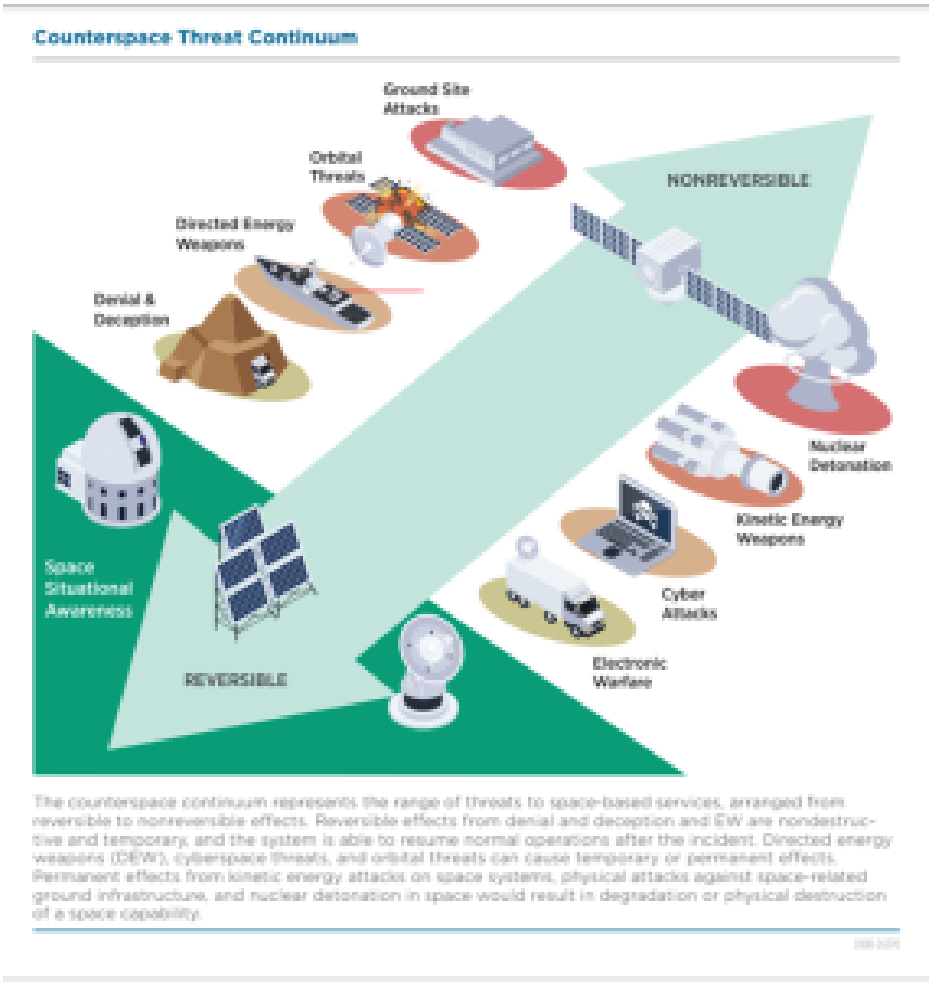
decades is deteriorating LEO conditions and has become one of the most prominent threats highlighted in this chapter. Man-made debris can worsen conditions in space by impairing abilities to monitor and track naturally occurring and potentially more hazardous objects, i.e., meteors. Debris can also significantly damage and/or destroy satellites and even create collisions if the fragments are large enough. Typically, the largest contributors to debris fragmentation have been segments of spent rocket stages and body parts. However, the continued reliance on reusable components is gradually changing these statistics. On the other hand, a more worrisome cause for debris fragmentation is the occurrence of orbital collisions, a threat expected to intensify due to concerns over worsening LEO congestion (European Space Agency, n.d.) Previous incidences of orbital collisions, such as the 2009 US-Russia satellite collision, and increased traffic in space due to increasing launch affordability enforces these concerns. Another recent source of overall LEO debris was the testing of direct-ascent ASATs. The now infamous ASAT demo on Fengyun-1C in 2007 is suspected of having contributed to increasing debris fragmentation and the overall number of trackable space objects by about 25%. The accidental collision between a US and a dead Russian satellite in 2009 as well as the Russian Nudol ASAT test in 2021 were also amongst the biggest contributors. In total, two ASAT tests and one accidental orbital collision between two satellites have nearly doubled the amount of all categorized debris in under fifteen years (Defense Intelligence Agency, 2022). Other environmental hazards include meteor showers and solar storms, but these are sporadic and rare. The more severe variants are also far easier to track and anticipate, providing time for preparations. Meanwhile, the threat of hazardous debris in LEO is only expected to worsen with overall object count expected to grow dramatically into the 2030s. From both a military and non-military perspective, the ongoing explosion of man-made debris has become a top threat concerning spacecraft and satellites in orbit.

Figure 14-16: Space Object Accumulation



Source: (European Space Agency, n.d.)

Figure 14-17: Man-Made Threats Overview



Source: (Defense Intelligence Agency, 2022)

CONCLUSIONS

The so-called NewSpace era has begun with commercial actors becoming the main providers for LEO launches. This resulted in the doubling of both active and defunct satellites in just two years (Boley, 2021). Based on the deals made between SpaceX and the FCC for increased Starlink network development, this trend is likely to continue to intensify at least for the short future. SpaceX's disruptive impact on the satellite industry as a whole has in turn helped generate threats against it. Many of these threats existed long before

NewSpace, but some are more unprecedented. The issues of debris and overall congestion in LEO is a new issue that have not exploded in severity until recently. These are environmental threats that were boosted in part by the general spike in LEO activity often attributed to NewSpace. The biggest contributor to this boost, however, were kinetic-based ASAT missile tests, making even ASAT assesses a threat in a completely new way (Defense Intelligence Agency, 2022). On the other hand, remote attacks are the only threat that has consistently demonstrated itself thus far. Jamming remains a common technique used by foreign actors such as Russia, while cyberattacks have often targeted the ground segment of satellite networks through ground control stations. Nationally, China's rapid rise as a space power can be seen as a major challenge to SpaceX and other western corporate LSPs who have surpassed NASA's capacity to establish and manage satellite networks. One recommendation, from a policy perspective, is to formally designate space systems as a critical infrastructure sector vital to both the economy and national security (Gillette, 2021). While relations with China and Russia are currently deteriorating, some level of cooperation must be maintained in order to ensure the space remains a stable playing ground. This has been previously achieved through international agreements effectively de-weaponizing space for at least a time. However, the unprecedented involvement of private LSPs has complicated the dynamic between opposing factions in space. A common system of communication will be essential for moving forward. While individual threats spanning from weaponry to debris will continue to worsen, countermeasures will inevitably need to be developed to further deal with them as corporations and governments alike come to terms with the developing situation in orbit.

REFERENCES

Berger, E. (2022, Oct 26). *SpaceX becomes NASA's second-largest vendor, surpassing Boeing.* . Retrieved from Ars Technica. arstechnica.com/science/: https://arstechnica.com/science/2022/10/spacex-becomes-nasas-second-largest-vendor-surpassing-boeing/

Boley, A. B. (2021, May 20). *Satellite mega-constellations create risks in Low Earth Orbit, the atmosphere and on Earth.* Retrieved from Sci Rep 11, 10642. https://www.nature.com/: https://www.nature.com/articles/s41598-021-89909-7#citeas

Boschetti, N. G. (2022). *Space Cybersecurity Lessons Learned from The ViaSat Cyberattack.* Retrieved from Johns Hopkins University. https://www.researchgate.net/: https://www.researchgate.net/profile/Gregory-Falco/publication/363558808_Space_Cybersecurity_Lessons_Learned_from_The-ViaSat-Cyberattack.pdf

Defense Intelligence Agency. (2022, March). *Challenges to Security in Space.* Retrieved from DIA.mil. www.dia.mil/: https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Challenges_Security_Space_2022.pdf

Dobrijevic, D. (2023, April 21). *Starlink satellite train: How to see and track it in the night sky.* . Retrieved from Space.com. https://www.space.com/: https://www.space.com/starlink-satellite-train-how-to-see-and-track-it

European Space Agency. (n.d.). *About space debris.* . Retrieved from European Space Agency. https://www.esa.int/: https://www.esa.int/Space_Safety/Space_Debris/About_space_debris

Futron Corporation. (2003, Oct 15). *China and the Second Space Age.* . Retrieved from www.futron.com/: https://web.archive.org/web/20120419165427/http://www.futron.com/upload/wysiwyg/Resources/Whitepapers/China_n_%20Second_Space_Age_1003.pdf

Garino, B. &. (2018, Sept). *Space system threats – aerospace security.* Retrieved from csis.org. https://aerospace.csis.org/: https://aerospace.csis.org/wp-content/uploads/2018/09/Space-System-Threats.pdf

Gillette, A. (2021, Sept 16). *From Supply Chains to Spacecraft: Taking an Integrated Approach to Cybersecurity in Space.* Retrieved from The Wilson Center.

Grego, L. (2012, Jan). *A History of Anti-Satellite Programs. Union of Concerned Scientists.* Retrieved from www.ucsusa.org/: https://www.ucsusa.org/sites/default/files/2019-09/a-history-of-ASAT-programs_lo-res.pdf

Guinnessy, P. (2014, May 8). *Ukraine crisis hits US space industry.* Retrieved from Physics Today. pubs.aip.org/physicstoday: https://pubs.aip.org/physicstoday/online/10200/physicstoday/search-results?f_Subjects=Politics+%26+Policy&fl_SiteID=1000045

Hitchens, T. (2022, Feb 3). *US rejects charge that Starlink satellites endangered China's space station.* Retrieved from Breaking Media, Inc. https://breakingdefense.com/: https://breakingdefense.com/2022/02/us-rejects-charge-that-starlink-satellites-endangered-chinas-space-station/

Holmes, M. (n.d.). *The Growing Risk of a Major Satellite Cyber Attack.* Retrieved from interactive.satellitetoday.com: https://interactive.satellitetoday.com/the-growing-risk-of-a-major-satellite-cyber-attack/

Kan, S. (2007, April 23). *China's Anti-Satellite Weapon Test.* . Retrieved from Congressional Research Service: https://apps.dtic.mil/sti/pdfs/ADA468025.pdf

Kelso, T. (2009). *ANALYSIS OF THE IRIDIUM 33-COSMOS 2251 COLLISION.* Retrieved from celestrak.org/publications/: https://celestrak.org/publications/AAS/09-368/AAS-09-368.pdf

King, M. &. (2020, Oct 8). *Cybersecurity Threats in Space: A Roadmap for Future Policy.* Retrieved from The Wilson Center https://www.wilsoncenter.org/: https://www.wilsoncenter.org/blog-post/cybersecurity-threats-space-roadmap-future-policy

Kolovos, A. (2022). *Commercial Satellites in Crisis and War: The Case of the Russian-Ukrainian Conflict.* Retrieved from Hellenic Air Force Academy. https://www.researchgate.net/: https://www.researchgate.net/profile/Alexandros-Kolovos/publication/368806976_Commercial_Satellites_in_Crisis_and_War_The-Case-of-the-Russian-Ukrainian-Conflict.pdf

Krebs, G. D. (2023, Jan 14). *VENESAT 1 (Simon Bolivar 1).* Retrieved from Gunter's Space Page. https://space.skyrocket.de/: https://space.skyrocket.de/doc_sdat/venesat-1.htm

Lethbridge, C. (1996). *BOLD ORION FACT SHEET. Spaceline, Inc.* . Retrieved from www.spaceline.org/: https://www.spaceline.org/cape-canaveral-rocket-missile-program/bold-orion/

Malik, T. (2022, Mar 5). *Elon Musk says SpaceX focusing on cyber defense after Starlink signals jammed near Ukraine conflict areas.* Retrieved from Space.com. https://www.space.com/: https://www.space.com/elon-musk-spacex-starlink-cyber-defense-ukraine-invasion

McCall, S. M. (2020, Feb 3). *National Security Space Launch.* Retrieved from Congressional Research Service: https://www.everycrsreport.com/files/20200203_R46211_746668d39ebc17bb2860c8271e3a907a138bfef6.pdf

Nichols, R. K. (2022). *SPACE SYSTEMS: EMERGING TECHNOLOGIES AND OPERATIONS.* Manhattan, KS: NPP #47.

Nichols, R., Carter, C., Diebold, C., Drew, J., Farcot, M., Jackson, M., . . . & Toebes, J. (2023). Space Electronic Warfare. In R. Nichols, *CYBER HUMAN SYSTEMS, SPACE TECHNOLOGIES AND THREATS* (p. Chapter 10). Manhattan: New Prairie Press. Accepted for Publication, 2023; NPP#TBN.

Reed, J. G. (n.d.). *Vulcan Reuse* . Retrieved from American Institute of Aeronautics and Astronautics. https://ntrs.nasa.gov/: https://ntrs.nasa.gov/api/citations/20205008263/downloads/ASCEND-Vulcan%20Reuse%20R2%20FMC_V2.docx.pdf

Roberts, T. G., & Harrison, T. (2022, September 1). *History of the NASA budget – aerospace security project – CSIS.* Retrieved from aerospace.csis.org/: https://aerospace.csis.org/data/history-nasa-budget-csis/

Roth, S. M. (2021). *DATA SNATCHERS: ANALYZING TIKTOK'S COLLECTION OF CHILDREN'S DATA AND ITS COMPLIANCE WITH MODERN DATA PRIVACY REGULATIONS.* Retrieved from Journal of High Technology Law and Samuel M. Roth. https://bpb-us-e1.wpmucdn.com/: https://bpb-us-e1.wpmucdn.com/sites.suffolk.edu/dist/5/1153/fi

Slofer, W. (2022). SATELLITE KILLERS AND HYPERSONIC DRONES. In R. K. Nichols, & C. M. Carter, *Space Systems: Emerging Technologies & Operations.* Manhattan, KS: NPP #47. Retrieved from https://kstatelibraries.pressbooks.pub/spacesystems/chapter/satellite-killers-and-hypersonic-drones-slofer/

Smith, M. V. (2011). *Spacepower and Warfare. U.S. Air Force.* Retrieved from apps.dtic.mil/sti/: https://apps.dtic.mil/sti/pdfs/ADA536586.pdf

Sönnichsen, A. &. (2020, Jan 1). *A Developing Arms Race in Outer Space? De-Constructing the Dynamics in the Field of Anti-Satellite Weapons*.* Retrieved from S&F Security and Peace. https://www.nomos-elibrary.de/: https://www.nomos-elibrary.de/10.5771/0175-274X-2020-1/s-f-sicherheit-und-f-sicherheit-und-frieden-jahrgang-38-2020-heft-1?page=1

SpaceX. (2023). *SpaceX Mission.* Retrieved from SpaceX.com: https://www.spacex.com/mission/

Thompson, A. (2020, Aug 24). *SpaceX's most-flown Falcon 9 rocket booster yet returns to Florida home port.* . Retrieved from Space.com. https://www.space.com/: https://www.space.com/spacex-falcon-9-rocket-booster-six-time-flier-returns-home.html

Union of Concerned Scientists. (2022, May 1). *UCS Satellite Database.* Retrieved from Union of Concerned Scientists www.ucsusa.org: https://www.ucsusa.org/resources/satellite-database

Upward, S. E. (2022). *The American Security Drone Act: America's Paper Tiger vs. China's Trojan Horse.*

Retrieved from American University National Security Law Brief. https://digitalcommons.wcl.american.edu/: https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1143&context=nslb

US Government. (2021, Aug 9). *Control segment.* Retrieved from GPS.gov. https://www.gps.gov: https://www.gps.gov/systems/gps/control/

US Government. (2021, Feb 22). *GPS Overview.* Retrieved from GPS.gov. https://www.gps.gov/systems/gps/: https://www.gps.gov/systems/gps/

US Government. (2022, June 28). *Space segment.* Retrieved from GPS.gov. https://www.gps.gov/systems/gps/space/: https://www.gps.gov/systems/gps/space/

Way, T. (2022). *Counterspace Weapons 101.* . Retrieved from Center for Strategic and International Studies. https://aerospace.csis.org/: https://aerospace.csis.org/aerospace101/counterspace-weapons-101/

Zarley, B. D. (2022, April 14). *An old satellite was hacked to broadcast signals across North America.* Retrieved from Freethink Media Inc. https://www.freethink.com/: https://www.freethink.com/space/decommissioned-satellite-hacking

Zedalis, R. J. (1978). *ANTI-SATELLITE WEAPONS AND THE OUTER SPACE TREATY OF 1967* . Retrieved from CWSL Scholarly Commons. https://scholarlycommons.law.cwsl.edu/: https://scholarlycommons.law.cwsl.edu/cgi/viewcontent.cgi?article=1947&context=cwilj

15.

STRATEGY AND ECONOMICS OF SPACE MISSIONS [JACKSON & JOSEPH]

STUDENT LEARNING OBJECTIVES

- To understand the principles of manufacturing in space
- To understand space systems for the manufacturing mission
- To understand the economics of space missions and strategies

INTRODUCTION

Manufacturing in space is a strategic endeavor that produces materials that cannot be manufactured on Earth and where processing is affected by Earth's environment. The advantages of manufacturing in space include operating in microgravity and vacuum, extracting high-value minerals from other planetary bodies or asteroids, and processing in low-Earth orbits before returning to Earth. Space missions established science-based manufacturing in space by studying microgravity environment effects that started with the Mercury, Gemini, Apollo, and Skylab programs. The Space Shuttle and Spacelab missions generated further manufacturing experiments aboard the International Space Station (ISS), such as processing materials without constraints, casting dynamics, and additive welding, the characteristics needed to invent printing processes with recycled/planetary feedstocks used in space. This chapter explains the advances of manufacturing in space and the strategies and economics of missions associated with this activity.

MANUFACTURING IN SPACE

The interest in manufacturing in space is due to a number of unique attributes because the environment controls convection motions in liquids and gases and eliminates sedimentation, which allows crystals to be grown in large formations that are very low in defects (the cleanliness of vacuum allows pure materials to be produced with processes such as vapor deposition creating very pure thin layers to be produced in an additive manner creating superlattice layer structures, or additive nanolayers). The extremes of heat provided by sunlight and shade create a dramatic temperature gradient that can be used to produce very strong materials.

The US government-led consortium known as 'America Makes' (www.nasa.gov) is creating initiatives

associated with 'in-space manufacturing' (Figure 15-1) with NASA leading on exploiting the fundamentals of manufacturing in the space environment (https://www.americamakes.us/).

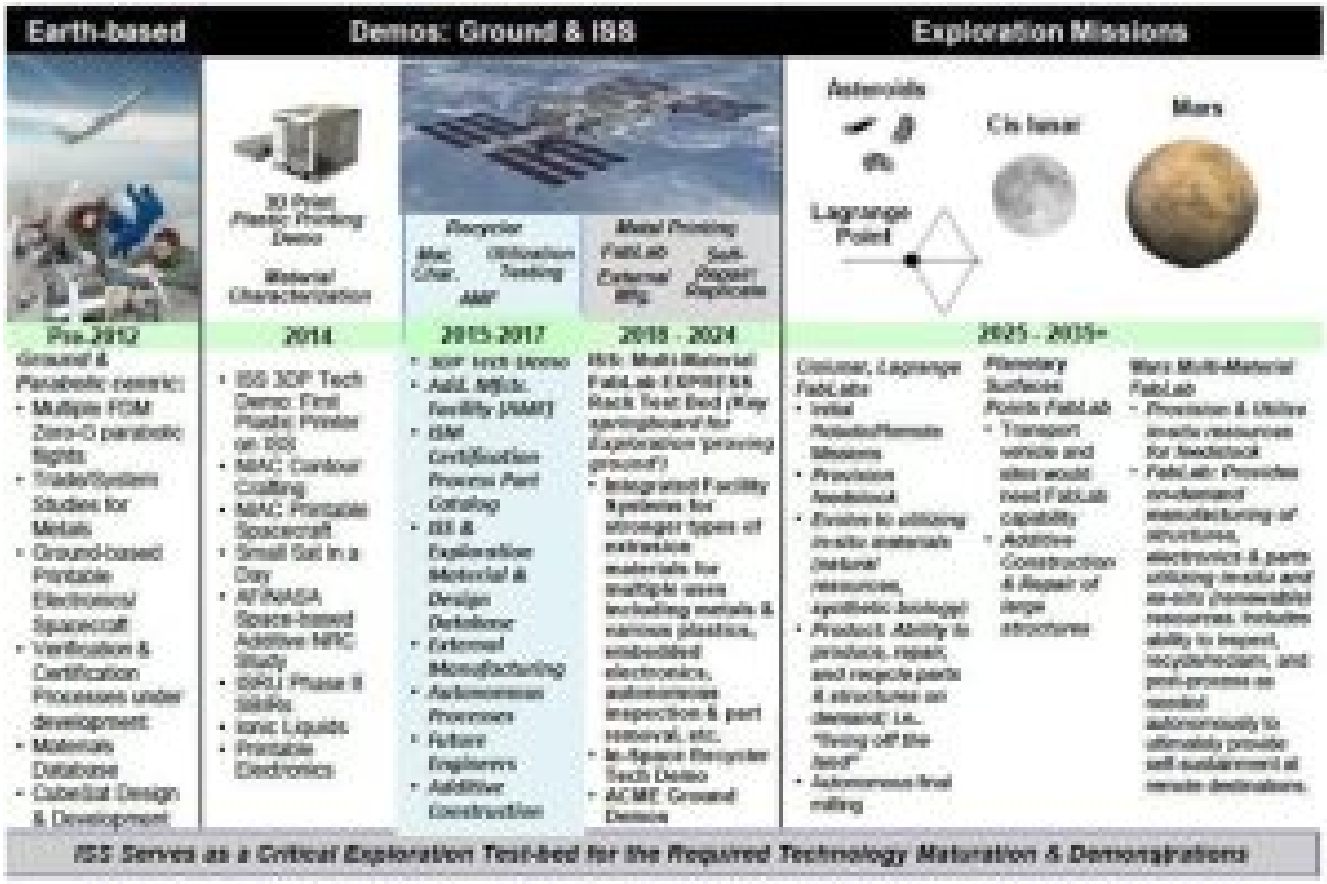
The European Union's focus is primarily on developing materials, technology associated with manufacturing, engineering, and the circular economy using the Fraunhofer Institutes to create the conditions of manufacturing in space (AM Sub-Platform 2013, EU Powder Metallurgy Association 2014, Volz 2014, Weinzierl and Sarang 2021, Nichols et alia 2022). The European Space Agency's (ESA) focus on additive manufacturing in space to develop replacement parts for use aboard ISS is notable and is centered around recycling, reuse, and remanufacturing. The EU's Additive Manufacturing Aiming Towards Zero Waste and Efficient Production of High-Tech Metal Products (AMAZE) project involves in-space applications as a core area of its impact on space manufacturing efforts (https://cordis.europa.eu/project/id/313781). ESA is funding additive manufacturing on planetary habitats such as the Moon and on asteroids using methods developed in the US. However, the development of manufacturing standards in space and the international cooperation between space agencies need further work to eliminate duplication of the costs of manufacturing in space (Volz 2014, Nichols et alia 2022).

The development of materials science aboard the ISS has led to the creation of 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 (Figure 15-2), which shows the differences between anisotropic dendrite formation in Pb-Sb alloys and segregation in Pb-Sn alloys grown on Earth and in space. Space-grown alloys show uniform microstructures because of reductions in thermal and solute convection flows (Volz 2014).

Microgravity environments minimize sedimentation and buoyancy of mixed materials, which promotes uniform particle distributions (Figure 15-3) (Volz 2014, Nichols et alia 2022). Systems used on the ISS uses a materials science glovebox, SUBSA vertical gradient furnace (transparent growth zone), PFMI low-temperature furnace for solidification and remelting of transparent materials and CSLM quench furnace for studying coarsening in metals (Figure 15-4).

In addition to the equipment on the ISS, 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 15-5). These pieces of equipment provide the laboratory equipment required to understand manufacturing in space (Volz 2014, Nichols et alia 2022).

Figure 15-1 NASA's In-Space Manufacturing Roadmap

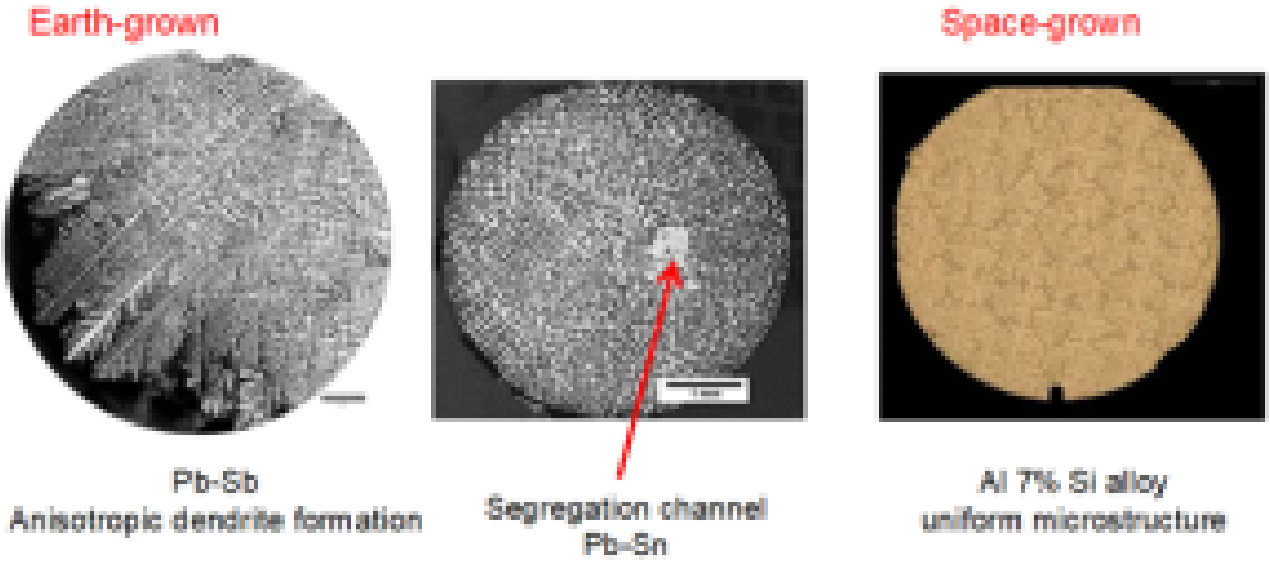


Source: Image courtesy of NASA/John Vickers

Cooper and Griffin of NASA MSFC published a report that referred to direct manufacturing and stated that in remote locations such as the Moon, Mars, or other planets; direct fabrication (manufacturing) could be used to produce items on location (NRC 2000). The report explained how additive manufacturing in microgravity demonstrated the benefits of fused deposition modeling (FDM) to rapidly produce replacement components or repair broken hardware on the Space Shuttle (SS) or the International Space Station (ISS).

Cooper and Griffin conducted low-gravity aircraft experiments to demonstrate the capability of FDM 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 volume, mass ~ 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 (Korkut and Yavuz 2022).

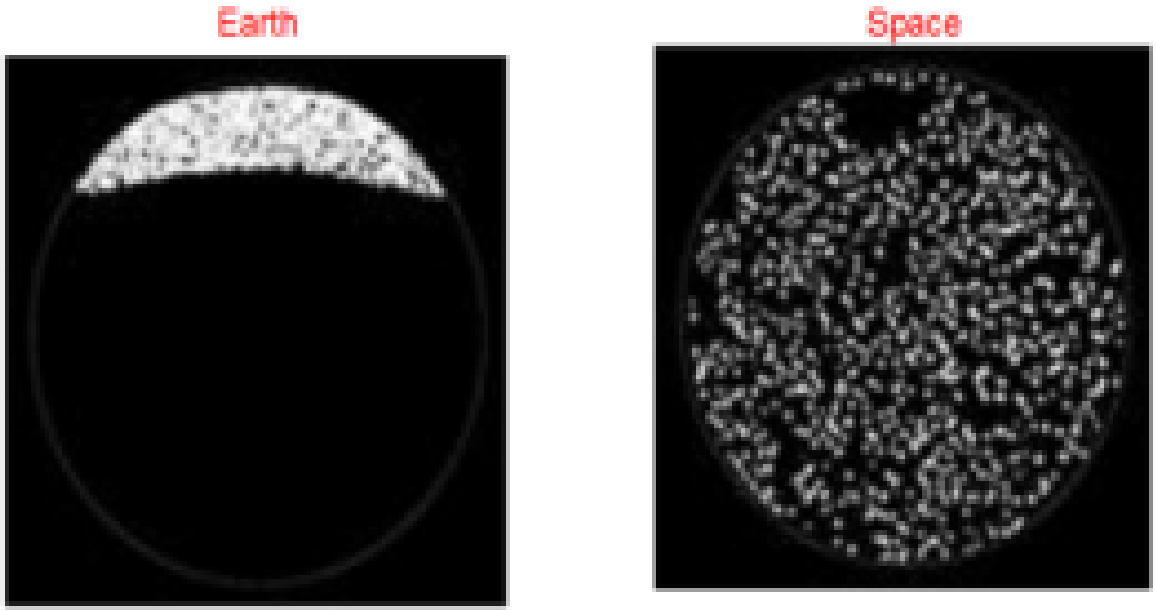
Figure 15-2 Microgravity Environments Reduces Thermal and Solute Convection Flows



Source: Image Courtesy of NASA (Volz 2014); (Volz 2014, Nichols et alia 2022).

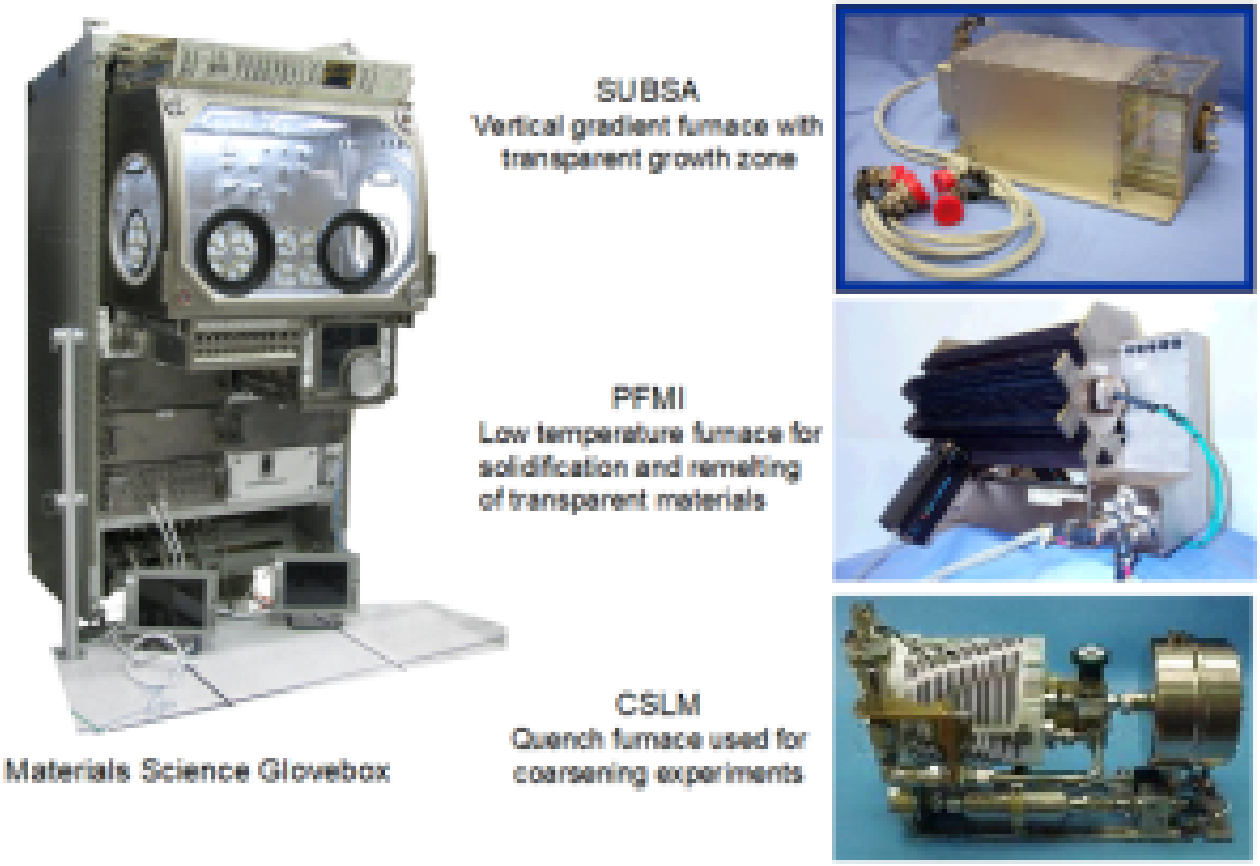
Manufacturing in space allows the construction of structures and subsystems fully optimized to operate in the zero-gravity environment with impressive volume-to-mass efficiencies (Prater et al., 2018, 2019).

Figure 15-3: Microgravity Environments Minimizes Sedimentation and Buoyancy of Phases



Source: (Volz 2014, Nichols et alia 2022). Image Courtesy of NASA (Volz 2014).

Figure 15-4 ISS Materials Science Facilities: Materials Science Glovebox (MSG) Facilities

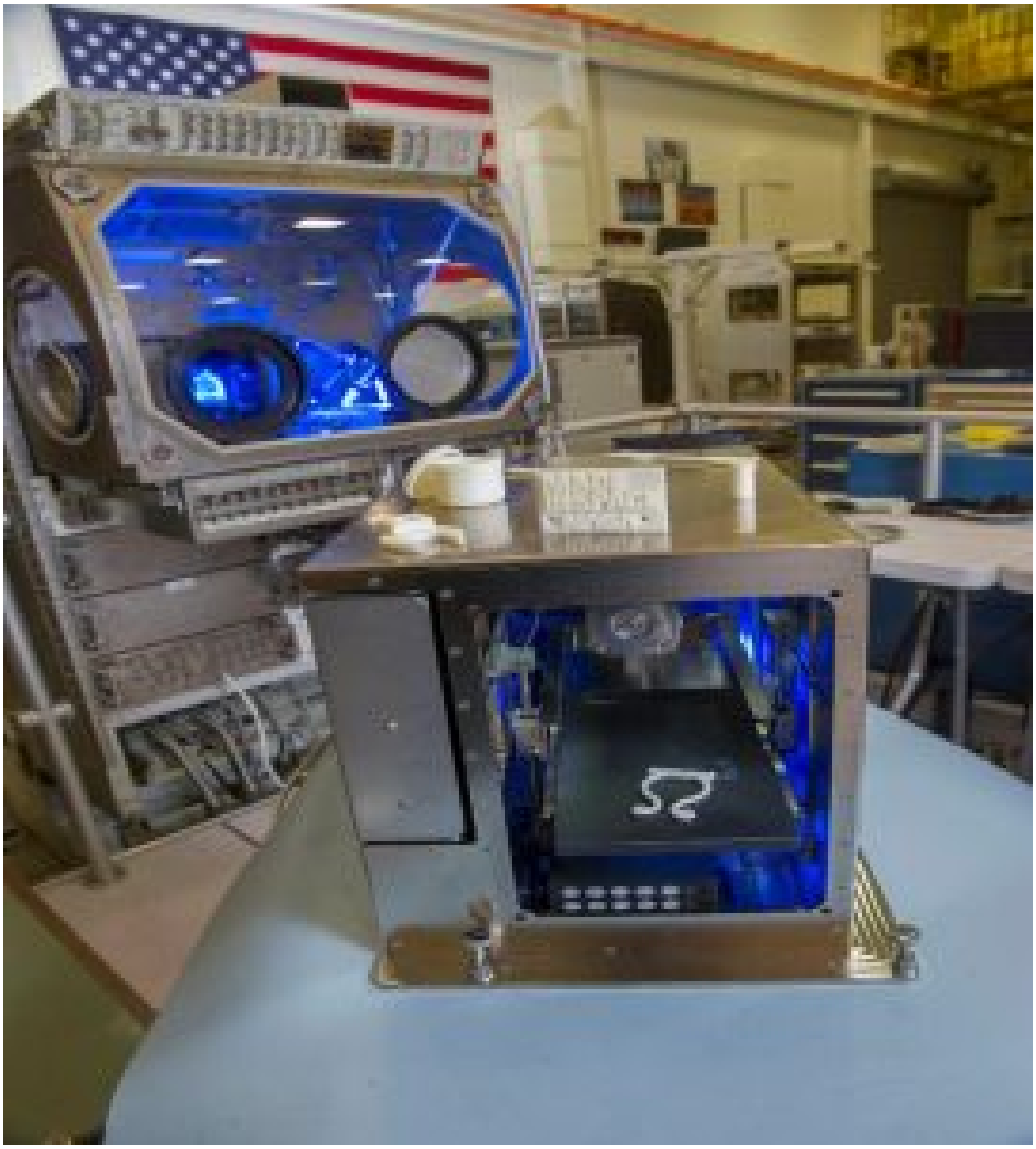


Source:(Volz 2014, Nichols et alia 2022). Image Courtesy of NASA (Volz 2014).

The percentage of hardware failures on the International Space Station (ISS) involves polymeric and composite materials (~ 35 %) and are using additive manufacturing techniques on board the ISS. NASA has developed several ways to achieve this including contracts with 'Made In Space, Inc.' (www.madeinspace.us) to provide extrusion-based additive manufacturing in microgravity environments on board the ISS (Weinzierl and Sarang 2021). 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 al., 2019).

The ISS 3-D printer made its first 3-D printed object in space in 2014. Figure 15-5 shows the printer during flight certification and acceptance at NASA's Marshall Space Flight Center, Huntsville, Alabama, prior to its launch to ISS aboard the SpaceX commercial resupply mission. The first objects built in space returned to Earth in 2015 for detailed analysis and comparison to the identical ground control samples made on the flight printer prior to launch. The goal of this analysis was to verify that the 3-D printing process works in the microgravity environment as it does on Earth (Prater et al., 2018, 2019). The printer works by extruding heated plastic, which then builds layer-upon-layer to create three-dimensional products. Long-term space missions would enable on-board manufacturing capabilities to supply needed parts.

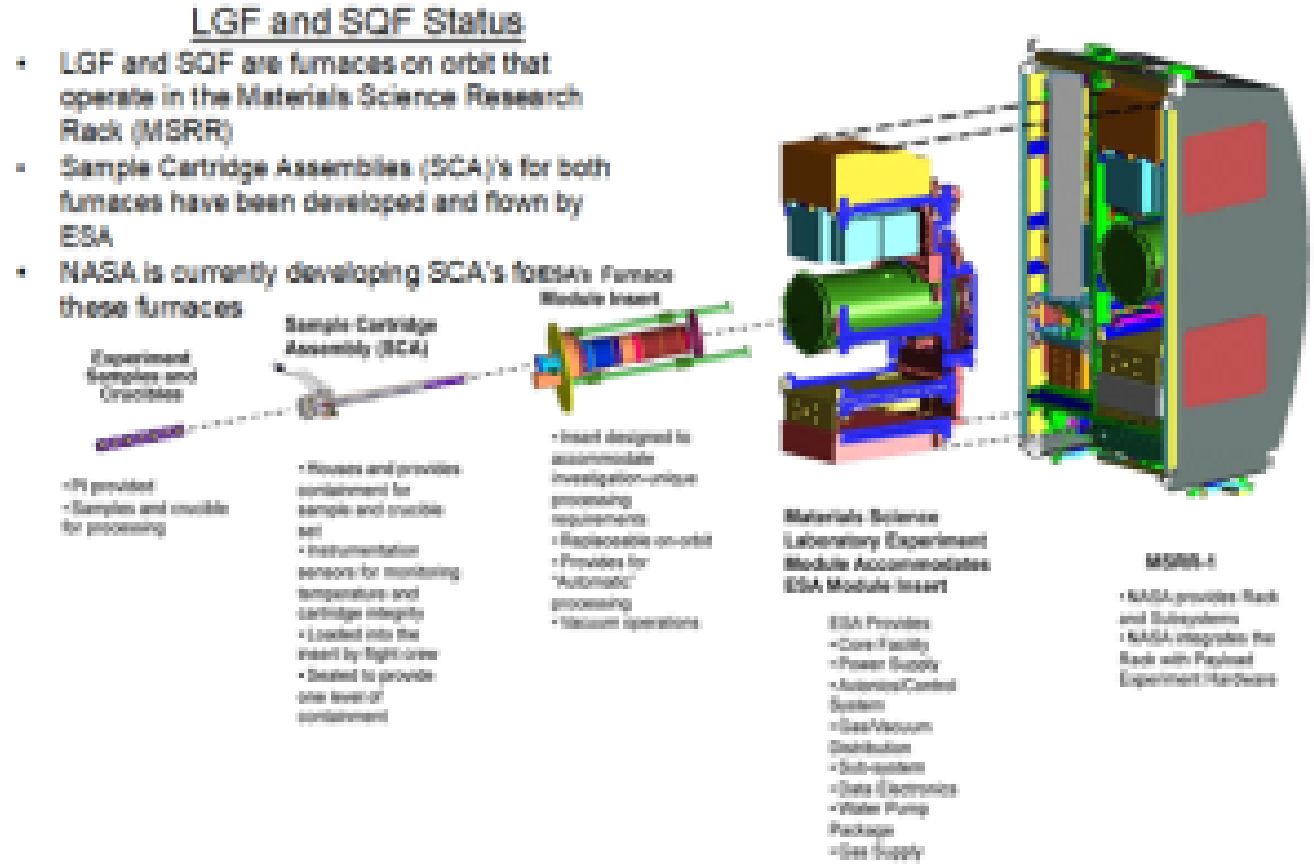
Figure 15-5: International Space Station's FDM Printer



Source: *Image Credit: NASA/Emmett Given.*

In addition to additive manufacturing, other forms of manufacturing such as free melting of metals (Figure 15-6), mixing of liquids for pharmaceuticals and processing of two-phase solutions are required. Additive manufacturing in space presents new opportunities for recycling. Recycled material has a significant impact on ISS operations. The disposal of waste on the ISS is achieved by detaching from the ISS and burning in the upper atmosphere of Earth. However, using recycled materials will eliminate waste and component/system creation of recycled materials allows feedstock to be produced (Prater et al., 2018).

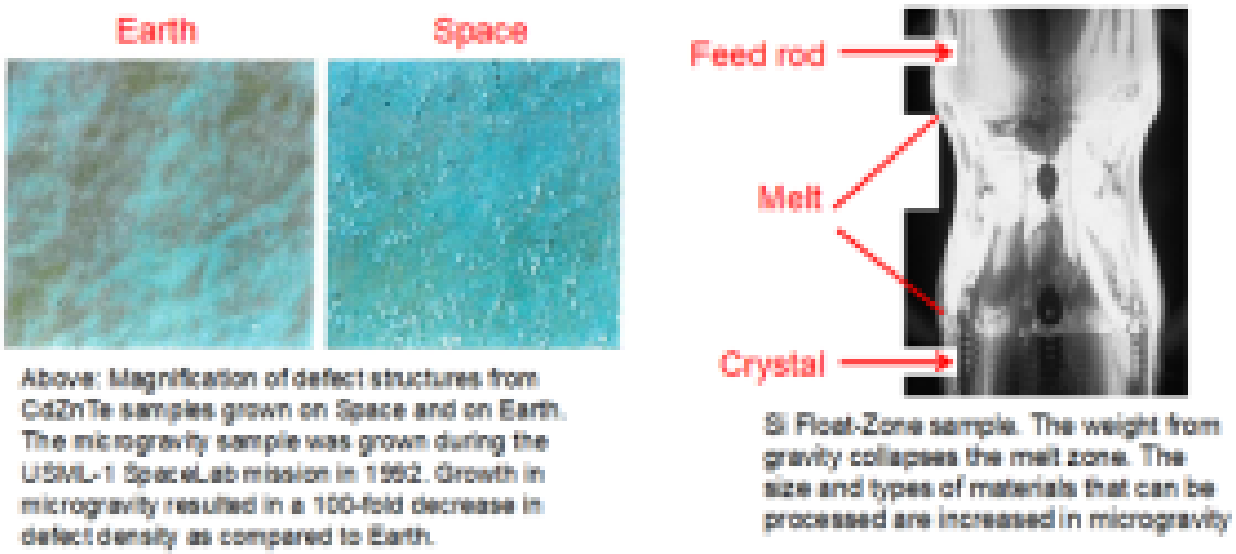
Figure 15-6: ISS Materials Science Facilities: Low Gradient Furnace (LGF) & Solidification Quench Furnace (SQF)



Source: (Volz 2014, Nichols et alia 2022). Image Courtesy of NASA (Volz 2014).

Microgravity environments enable accurate measurements of material properties such as viscosity and surface tension, facilitate nucleation studies, increase the size of crystals that can be grown, and reduces defect densities from contact with container walls (Figure 15-7). Manufacturing hardware enables the production of low-mass systems, thereby reducing launch and storage space. Antennas, booms, and panels are designed for launching and their size and shape are limited in addition to functionality and scale. Manufacturing in space enables the deployment of systems without constraints. Such systems include mirrors, gossamers, antennas, arrays, reflectors, and trusses (Kovalchuk et al. 2022).

Figure 15-7: Microgravity Allows Processing without Containment to Manufacture Items on the ISS



Source: (Volz 2014, Nichols et alia 2022). Images Courtesy of NASA (Volz 2014)

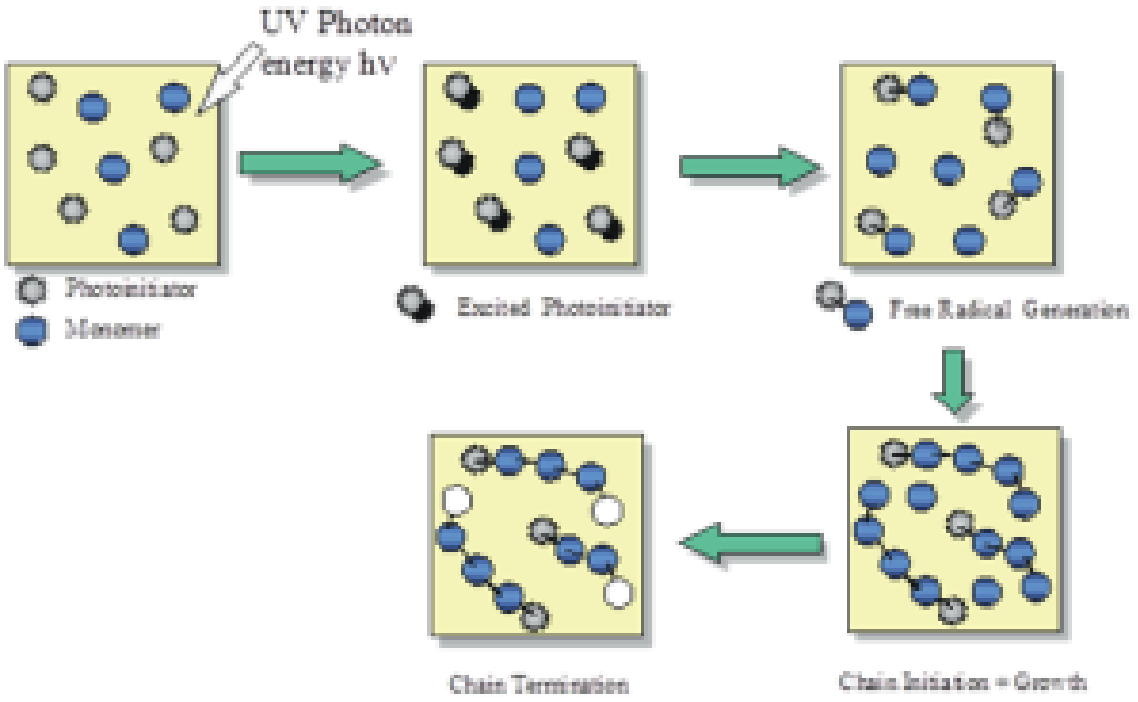
ADDITIVE MANUFACTURING FOR SPACE MISSIONS

There are wide ranges of process options for the user wishing to implement circular manufacturing technologies for space missions. Additive manufacturing (AM) technologies such as stereolithography (SLA), selective laser sintering, fused deposition modeling, ballistic particle manufacture, laser net shaping, etc., are available for use in the space environment. Most of these technologies have evolved from expensive systems producing basic models to relatively low-cost machines producing various components in metals, plastics, wax, and paper for applications such as design aids, rapid tools, and functional prototypes. For those involved in the study of AM, growth of this technology has far exceeded the adoption rate of other laser-based technologies such as welding. In terms of circular economic principles of recycling and reuse, this section examines the most common AM technologies and explores their limitations and advantages for use in space.

STEREOLITHOGRAPHY (SLA)

In the stereolithography process, photopolymers are composed of Photoinitiators and liquid monomers. The sequence of the photopolymerization process is shown in Figure 15-8. Photoinitiators are held in a solution composed of liquid monomers. On exposure to an ultra-violet photon, photoinitiators are excited and a small percentage of these molecules chemically transform to become reactive species. The reactive species stimulates photo polymerization through the formation of a free radical polymer initiation sequence. Additional monomers proceed to react with the chain until the process terminates.

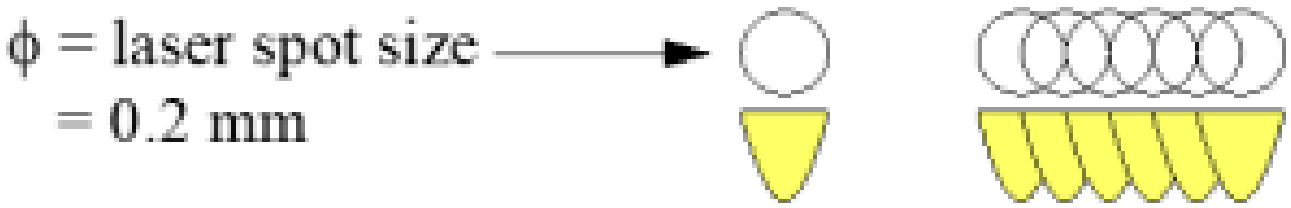
Figure 15-8: Photo-Polymer Reaction Sequence



Source:(Jackson 2023).

Commercial photopolymer AM machines work either by laser-based photocuring or masked-lamp curing. Stereolithography starts with a solid or surface CAD model of a three-dimensional object. A computer program slices the CAD model into many thin layers. The solid model is built in a vat of liquid resin that has the property of changing from liquid to solid when exposed to ultraviolet light. An ultraviolet HeCd laser, U.V. enhanced Ar+, or a frequency quadrupled Nd:YAG laser scans through a series of discrete vectors. At each point, the resin is cured to form a layer (Figure 15-9).

Figure 15-9: Sequential formation of solids through UV laser curing

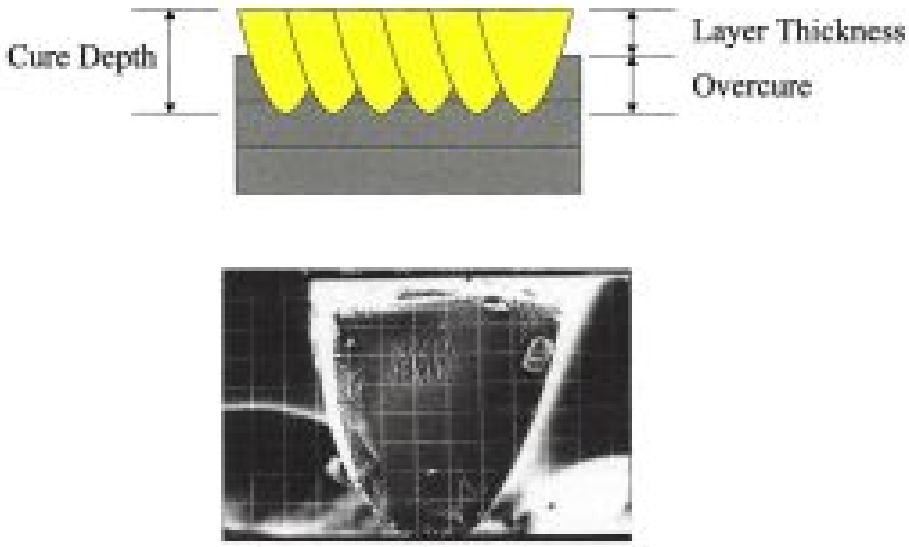


Source: Author

The overlapping of solids forms a line, and overlapping lines form a solid layer. The depth of cure is a function of laser power and dwell time; a substantial over-cure is produced to ensure layer-to-layer bonding. Figure 15-10 shows layer-by-layer bonding and a cross-section of a cured line.

Figure 15-10: Layer-to-layer Bonding and a Scanning Electron Micrograph Showing the Cross Section of a Cured Line

Figure 15-10: Layer-to-layer Bonding and a Scanning Electron Micrograph Showing the Cross Section of a Cured Line



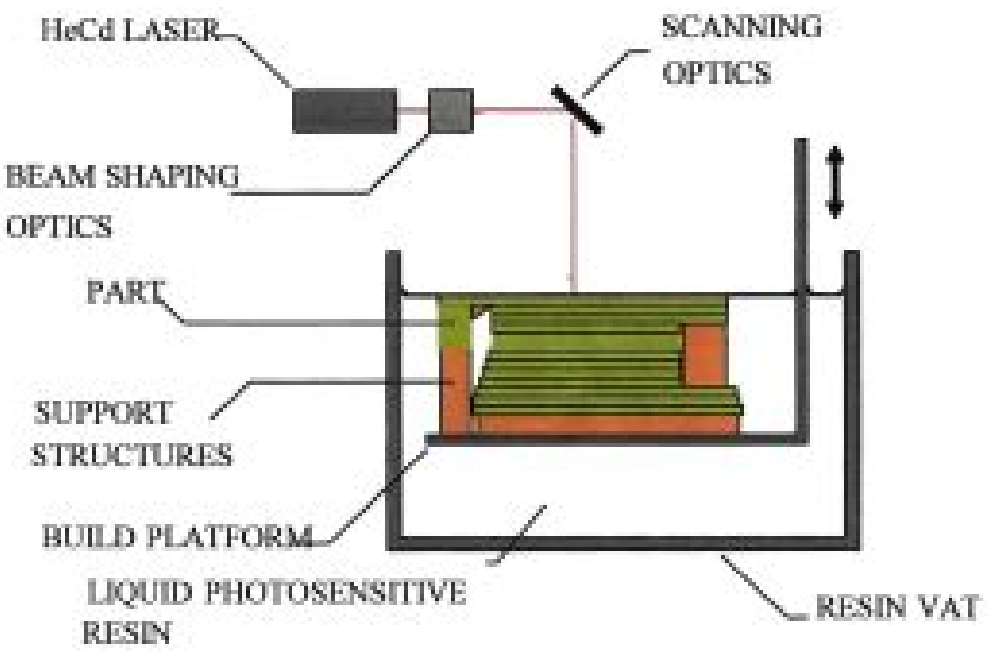
Source: Author

Source: Author

Building a solid object starts by drawing the bottom layer of the object on the surface of the liquid resin (Figure 15-11).

Figure 15-11: Schematic of the Stereolithography Process

Figure 15-11: Schematic of the Stereolithography Process



Source: Author

Source: Author

CAD data representing a layer moves the ultraviolet beam across the surface of the liquid resin by controlling the deflection of mirrors. After the entire bottom layer has been exposed and solidified, the layer of solid resin is lowered so that a thin layer of liquid covers the solid layer. Then the second layer of the solid object is drawn on top of the first. As the second layer is drawn, the liquid resin solidifies and adheres to the first layer. This process continues layer-by-layer, until the entire object is complete. The time taken for the process depends on the size and complexity of the object. After the object is completed, it is raised above the resin to allow excess liquid resin to drain. Finally, the object is exposed to a flood of ultraviolet light to complete solidification of the resin. After completion, various finishing processes may be used, depending on the use of the model. There are now many photo-polymer resins on offer ranging from epoxy, vinyl ether, or acrylate functional groups. Each photo-polymer resin will have offer specific build rates and produce models with a range of properties and accuracy.

The speed of a photopolymer is directly associated with the laser exposure necessary to achieve a prescribed cure depth, Cd. Most SLA users wish to know how long it will take to make a build with a particular resin. Information such as resin photo speed will allow the user to make accurate calculations about curing rates for

a particular laser power. The resin is exposed to a laser beam scanned at a series of known velocities. The cure depth Cd is then measured and plotted as a function of the incident energy density. The gradient provides the energy requirements of curing per unit volume, Dp, and Ec, is the critical exposure of the resin.

HeCd lasers produced radiant energy in both visible and ultra-violet wavelengths. The UV output provides sufficient energy for curing most photopolymers. Metastable states of neutral Helium atoms are excited. These collide with neutral cadmium atoms, the upper state of the cadmium ion is excited thereby emitting radiation with wavelengths 441.6 nm and 325 nm, which are visible light and ultra-violet light, respectively.

To calculate parameters that will illuminate the SLA AM process, the interaction of light with resin needs to be understood. Radiation that has been transmitted to the surface is absorbed according to Beer-Lambert's law, $I = Io.e^{-\lambda Z}$, where the absorption coefficient is determined by the intensity and wavelength of the radiation and the surface medium with which it is interacting. Let us assume that a laser beam is scanned in a straight line with constant velocity. Where the x-y plane relates to the surface of a liquid and the z-axis relates to the penetration through the liquid. Irradiance at any point within the resin can be calculated as a factor of the irradiance incident on the surface of the resin, H (x, y, 0). For an ideal Gaussian laser beam:

$$H(x,y,z) = H(r,0) = H_0 . exp^{-2\left(\frac{r^2}{w_0^2}\right)} \qquad 15\text{-}(1)$$

Wo relates to 1/e2 Gaussian half-width, which is ~ 13.5% of peak H. When considering that irradiance, H, is termed the 'radiant power per unit area,' it can be seen that exposure, E, is a function and as it is termed, 'energy per unit area,' which is the integral of irradiance with respect to time. Thus,

$$E(y,z) = \sqrt{\frac{2}{\pi}}\left[\frac{P_0}{w_0 v_s}\right] exp - \left(\frac{z}{D_p} + 2y^2 w_0^{-2}\right) \qquad 15\text{-}(2)$$

Where, E (y, z) = exposure (Jm-2), PL = laser power (W), Vs = laser velocity (ms-1), Dp = penetration depth (m), and Wo = 1/e2 Gaussian half-width (m).

In the case of laser interaction with photopolymers there is a critical value of exposure, Ec. Any value below this and the polymer will remain liquid, any value above this and the polymer will solidify. The transition point between the two states is termed as the gel point where the polymer changes viscosity. It follows that as the laser energy penetrates the resin at some point there will only be enough energy to raise the resin to the 'gel point,' i.e., energy absorption by the resin, and at this distance there will be a solidification boundary.

In order that the shape of a curing line is determined, Eq. 15-2 can be used with values set at the gel point. The result is a parabolic cylinder. This effectively produces a single cured line in the direction of travel. The maximum exposure will be at y = 0, so the maximum depth of the curing process can be determined. This is done by first determining what the maximum exposure is at the centre of the incident beam,

$$E(0,0) = E_{max} = \sqrt{\frac{2}{\pi}}\left[\frac{P_L}{w_o v_s}\right] \qquad 15\text{-}(3)$$

The maximum cure depth Cd can now be determined at Zmax:

$$C_d = D_p . ln\left(\frac{E_{max}}{E_c}\right) \qquad 15\text{-}(4)$$

Cd represents a fundamental side of SLA and provides essential information that can be used to control the laser and determine what effects occur within the resin. As the parabolic cure pattern was determined, the maximum cured line width can also be determined because it will occur on the surface, i.e., z=0. The cured line width, Lw:

$$L_w = 2w_0\sqrt{\frac{C_d}{2D_p}} \qquad 15\text{-}(5)$$

This is another important result, namely that the cured line width is directly proportional to the laser spot diameter. When cure depth is increased the cured line width increases by the square root of the cured depth:

$$E_{max} = E_c \cdot \exp\left[\frac{C_d}{D_p}\right] \qquad 15\text{-}(6)$$

Substituting for Emax and solving for Vs:

$$v_s = \sqrt{\frac{2}{\pi}\left(\frac{P_L}{w_0 E_c}\right)}\exp\left[\frac{-C_d}{D_p}\right] \qquad 15\text{-}(7)$$

Laser scan velocity is inversely proportional to laser spot size and decreases exponentially with an increase in the ratio of cure depth/penetration depth (Cd/Dp), i.e., increased cure depths draw more slowly than shallow cure depths. Accuracy is heavily dependent on the thickness of the layers that are used to construct the model. The layer thickness is a user definable parameter and as such can affect build quality. Layers will also affect the quality of the curved surfaces and leads to a phenomenon called stair stepping. Stair stepping affects build time, accuracy, and cost. Stair stepping phenomena affect all AM processes. Part orientation can reduce stair stepping effects and is essential to maximize part accuracy. Here are some common guidelines: define the most important surfaces, orientate part for best build, use adaptive slicing procedures for maximum resolution and position surface with respect to steps for ease of finishing. Support structures are necessary to maintain part integrity while it is being constructed: (1) supporting 'island' structures – it is extremely important that each

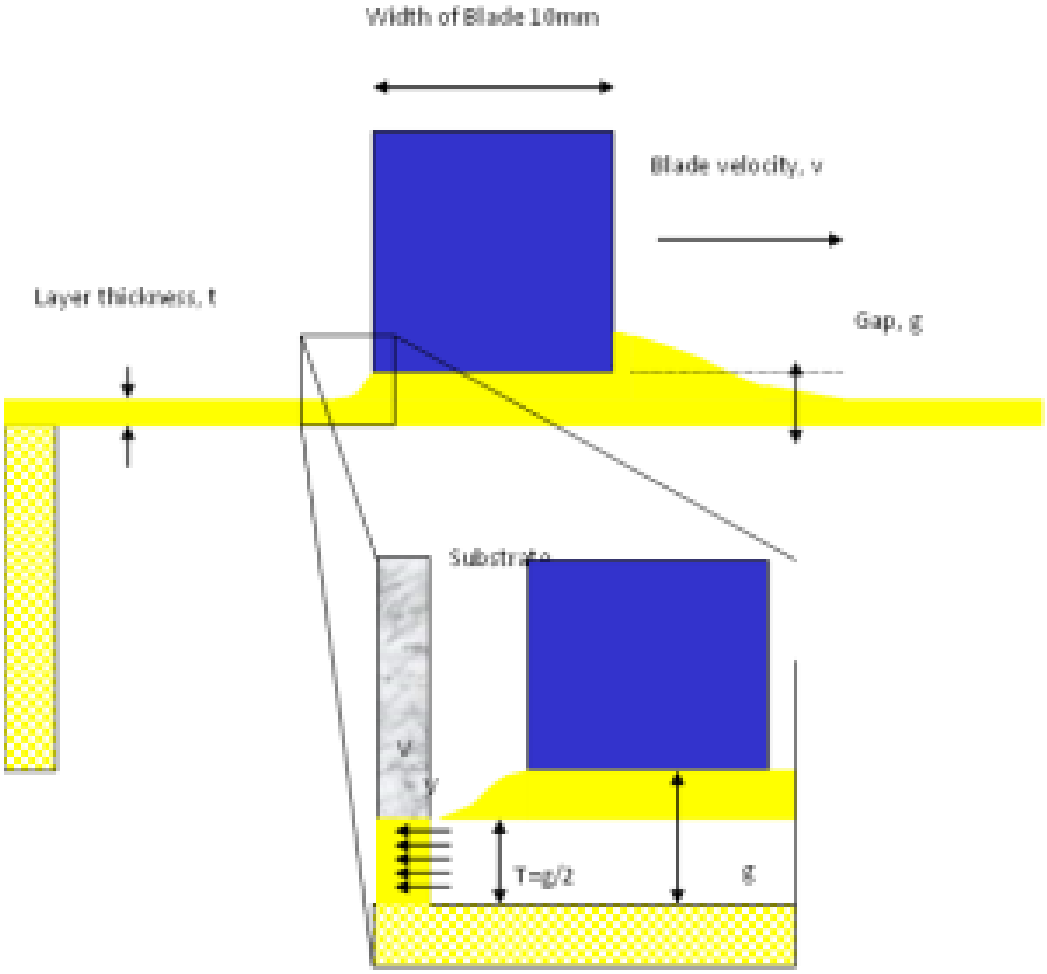
layer has a layer of some form underneath to attach itself to. With complex geometry this is often not the case and supports are therefore needed to ensure the cured resin does not float away; (2) support to reduce part distortion where solidification takes place there is likely to be an amount of distortion. This can be constrained by placing support structures that maintain tension during contraction. The result is stress concentrations, but the part will be geometrically superior**.**

In order that SLA parts to be built to the highest degree of accuracy there must be some form of calibration of the mechanisms within the machine. For example, over time the diameter of the beam will change as the cavity ages. Optical alignment may shift due to small temperature variations. Mode structure may alter due to internal misalignments from small vibrations and the laser power reading of the SLA may drift from the calibrated value. Practical studies into this problem have shown interesting results. Studies into accuracy show that the major sources of inaccuracy are shrinkage and laser linewidth, both of which can be compensated for by the equipment user and the hatch pattern.

The limiting factor that controls the speed of the SLA process is the re-coating time. Free liquid surfaces are very problematic, they must be given settling time after a disturbance such as dipping. Meniscus effects will distort the liquid level around surface features of the model. Hence, a doctor blade is used to level the resin after each layer and before each slice exposure is commenced. The problems are compounded by fluid dynamics of the sweeping motion. The blade is competing with surface tension forces acting on both the blade and part within the vat. There are additional affects which produce a build-up of resin ahead the of the blade which then provides a pressure gradient that drives resin underneath the blade as it sweeps across and affects the thickness of the resin coating behind the blade. The effects are a function of the resin temperature, viscosity, doctor blade geometry and velocity (Figure 15-12).

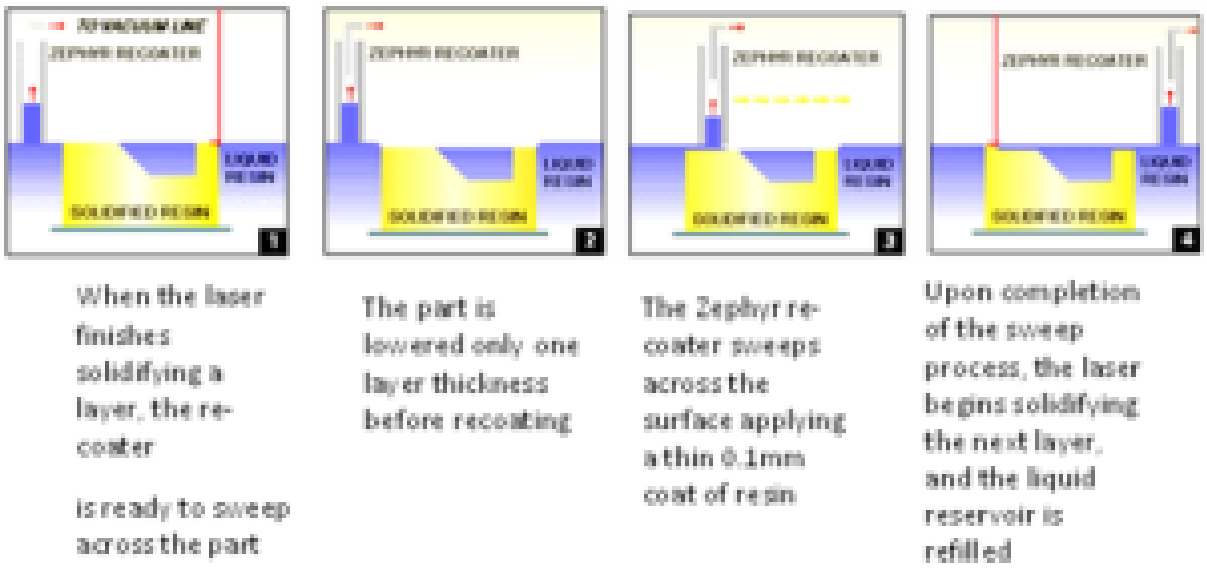
Figure 15-13 shows the workings of the Zephyr re-coating system that is now provided for most 3D SLA systems as an upgrade option. The blade deposits a curtain of resin directly onto the new surface thereby minimizing the time for re-coating and the effects of dragging and displacing the resin through sweeping.

Figure 15-12: Factors Affecting the Sweeping Process



Source: Author

Figure 15-13: The Zephyr Re-coating System

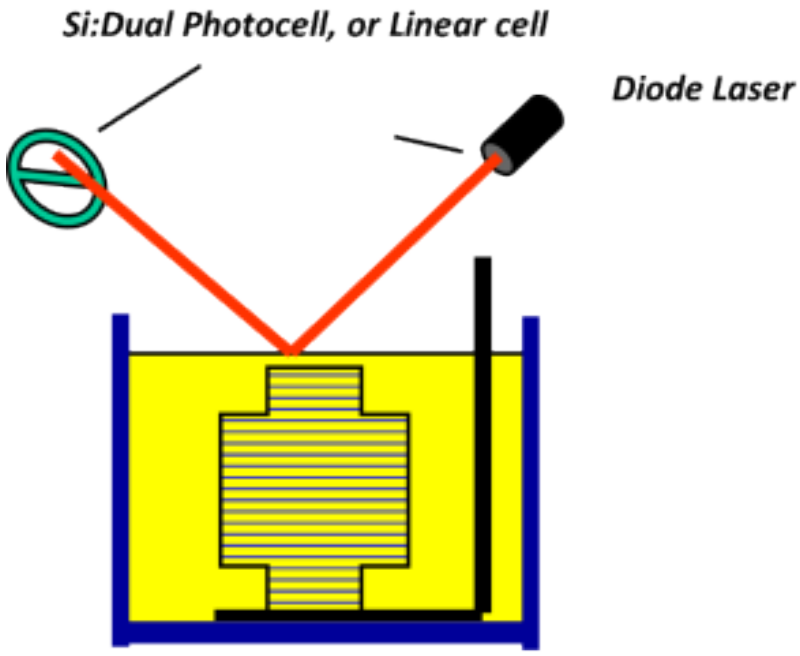


Source: Author

In order to prepare the new layer for curing, issues must be addressed: the resin surface must be maintained at the focal plane of the imaging system; the surface must be uniformly flat, level, and free of extraneous features; the surface must be a controlled distance above the previous layer; and control systems are essential!

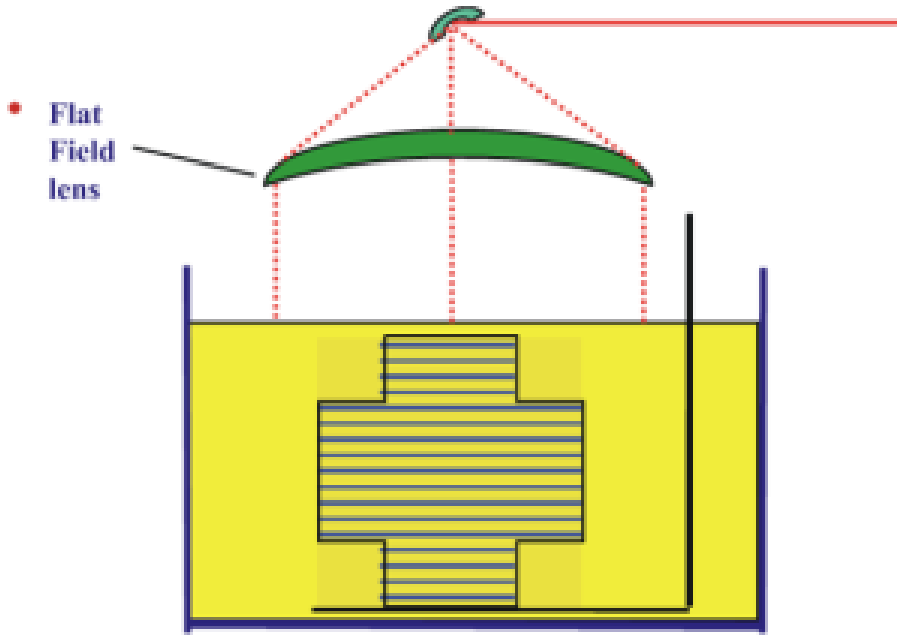
The resin surface position must be known. Light-bounce techniques are employed to locate surface, Diode Laser Levelling System (DLL). Layer thickness is usually around of 100-200 sq. m. Surface positioning typically requires positional control of 3-7% of the layer thickness, about 7.5mm. Location can be determined allowing feedback to the liquid control system and speeds are increased (Figure 15-14). Laser spot size influences the irradiance (energy distribution), which in turn will affect depth of cure, width of the cured line, and the extent of overcure. We must therefore keep the illumination conditions constant across the whole area of the vat. An alternative is a flat-field focusing lens that maintains the focal properties across the vat and forces the beam to interact with the resin at near normal incidence (Figure 15-15). This system is commonly used in laser marking systems. The way in which the object is cured within its layer boundary determines the level of internal stress and shrinkage factors. Part accuracy can be improved by careful choice of hatch pattern as there are many to choose from. Hatch patterns determine part accuracy, hatching is used to photo cure the liquid in the interior regions of the part. Hatch pattern determines the amount of curing within an object which therefore affects its physical properties and internal stresses and many patterns have been developed Tri-hatch uses a scanned line parallel to the x-axis combined with lines at 60 and 120 degrees to the x-axis.

Figure 15-14: Level Determination on the Resin Surface



Source: Author

Figure 15-15: Using a Flat-field Lens to Correct for Focal Displacement



Source: Author

There is approximately 50% uncured resin within the triangular matrix, which is cured in post processing generating high distortion. The Weave adopts two orthogonal vector sweeps per layer. The amount of uncured resin is reduced, part accuracy is increased along with build speed. Errors on the corners are often observed. STAR-Weave is a staggered hatch pattern, alternative sequencing, and retracted hatch offsets every other layer of the x- and y-hatch vectors. It prevents x-and y-hatch overlay and reduces stress build up. A retracted hatch keeps endpoints from bonding with the border.

The following advantages are associated with SLA:

- It can use several types of resin with varying properties apart from the resins from Ciba-Geigy.
- It has good surface finish and accuracy.
- It has a good speed depending on model types.
- The SLA does not require any attendant when it is in operation, it can be left to run on its own.
- Parts can have both internal and external contours and shapes.
- The SLA can build multiple parts at once.
- The SLA can be used to produce complex geometry. SLA produced parts can be used to create patterns for soft tooling, with part design duplicated in a polyurethane material that more closely approximated the acrylonitrile butadiene styrene (ABS) material from which the actual part would later be made. It can also be used for mold making for casting operation.
- Parts produced by SLA are used for flow test visualization; and
- Parts produced by SLA are used as investment casting patterns.

Despite all the accompanying advantages, the SLA has some disadvantages:

- Shrinkage and distortions are present in the material. This leads to layers separating from the structure.
- The surface finish depends on the slice thickness and material. Also, the accuracy greatly depends on the parts complexity.
- It needs a lot of finishing operations that can be tedious and messy. This will lead to the purchase of finishing apparatus that is an added cost. Post cure is required for all the resin-based processes either acrylic or epoxy resin.
- Large and thin flat structures are most difficult to produce and hold within tolerance. The Engineers compensate for these effects by altering the part's orientation or by adding the proper type of fixing to hold the features in position during the post-curing process, a lot of the stresses that cause the part to wrap are basically molded in, so when the supports are removed, there is a good chance that the wall is going to warp.
- Surface finish and tolerance are not complementary. Orienting a part one way may result in higher

accuracy and a less attractive surface finish. Conversely, orienting the part another way may lead to a smoother finish with less precise tolerances.

- The use of expendable patterns generated with the aid of SLA is not without problems. Because of the high thermal expansion characteristics of the polymers used in SLA, use of patterns created with the process can result in mold cracking or breaking during burn-out.
- For each part, a support structure must be modeled and designed in the CAD system; and
- Unlike other systems, Process does not produce very fine tolerances. Hence tolerance of ±0.0013 mm is not possible for now with SLA, which is ±0.2 mm in x-y plane.

A clear advantage of using SLA in space is its ability to convert liquids into solids and the solids to be used for feedstocks/fillers for other AM processes such as FDM. The use of lasers to fuse materials can be extended to metals making selective laser sintering (SLS) a technique that will be of great use in the space environment especially for the creation of very high strength alloys and alloys that cannot be manufactured on Earth.

FUSED DEPOSITION MODELING

Fused Deposition Modeling (FDM) processes uses thermoplastic wire-like filaments that are melted in the deposition head. The material is then extruded from the head and deposited on a layer-by-layer basis. The layering lamination technique is based upon the rapid solidification (~ 1/10 second) of the molten laminate material from the Modeling filament. The semi-liquid thermoplastic material is deposited onto thin layers, building the model upwards off a fixture base. The plastic or wax material solidifies in place positioned by the x-y controlled extrusion head. A precision volumetric pump is used to control the material passing through the extrusion orifice. The extrusion process shears the material, and it quickly solidifies while bonding to the previous layer by heating it and then fusing. The model is fabricated upon a piston, which is lowered between layers to make room for the next layer. This process is repeated until the part is fully built.

A series of cassettes or spools supplies the system with a polyester compound. Each cassette holds 50 rectangular wafers. A stapling mechanism feeds the wafers into a pressurized heated channel that supplies the material to a viscosity pump. To ensure accuracy, the material is extruded through a 150-300 mm diameter orifice at a controlled rate. Parts are built on a thermally controlled metallic substrate that rests on a table. As each layer is extruded, it bonds to the previous layer and solidifies. The pump head, table and gantry move in the x, y, and z axes, respectively.

Supports for the parts are built from the same polyester material, using a support-generation algorithm. The system creates perforations where supports adjoin the model, making it easy to snap off any required supports. Printed models often require fewer supports than other systems' models due to precise pump control. A technique called "bridging" allows the material to be extruded across a distance without supports. Thin perimeter walls are created, and the pump head fills in the area, creating a flat surface between the walls. This technique speeds build time and maintains a good surface finish. No special clean-up is required.

Modeling filaments include ABS, medical grade ABS, (ABS prototypes have 85% of the strength of an actual molded part), investment casting wax, thermoplastic elastomers, and many other materials. Models can be marked, sanded, painted, or drilled. Accuracy of the models can be produced within ±0.127 mm (±.005 in). Layer Width / Thickness: Operator may optionally select road widths between 0.254 to 2.54 mm (0.010 to 0.100 in) and thickness from 0.05 to 0.762 mm (0.002 to 0.030 in). The advantages of FDM include:

- All the materials that are used for this process are non-toxic, hence it is safe for office use.
- It is a high-speed process. Layers are laid at speeds up to 23 m/min.
- The parts do not require support structure while building. There is no material wastage or cleaning. However, 3D Modeler creates a support in mid-air rather than building the support up from the base as in other applications.
- It is excellent for making investment-casting pattern using wax. Parts produced by FDM processes emerge fully cured so that they can be used immediately or can be treated after grinding, painting, etc.
- It uses varieties of heat-fusible thermoplastic filament materials and wax filaments. For example, machinable wax, ABS like plastics, investment casting wax and nylon.
- The system is also capable of extruding plastic into free space depending on the part geometry; and
- It is a desktop system that can operate in an office environment without any special ancillary service.

The disadvantages include:

- The following disadvantages are peculiar to the FDM process.
- Part strength is limited to adhesion/fusion between filaments.
- It requires support structure for some parts.
- There is the problem of delaminating of parts due to poor bonding between layers; and
- The operating temperature of between 82 and 105 oC makes it suitable for office use and puts a natural limit on the useful in-service temperature range of parts.

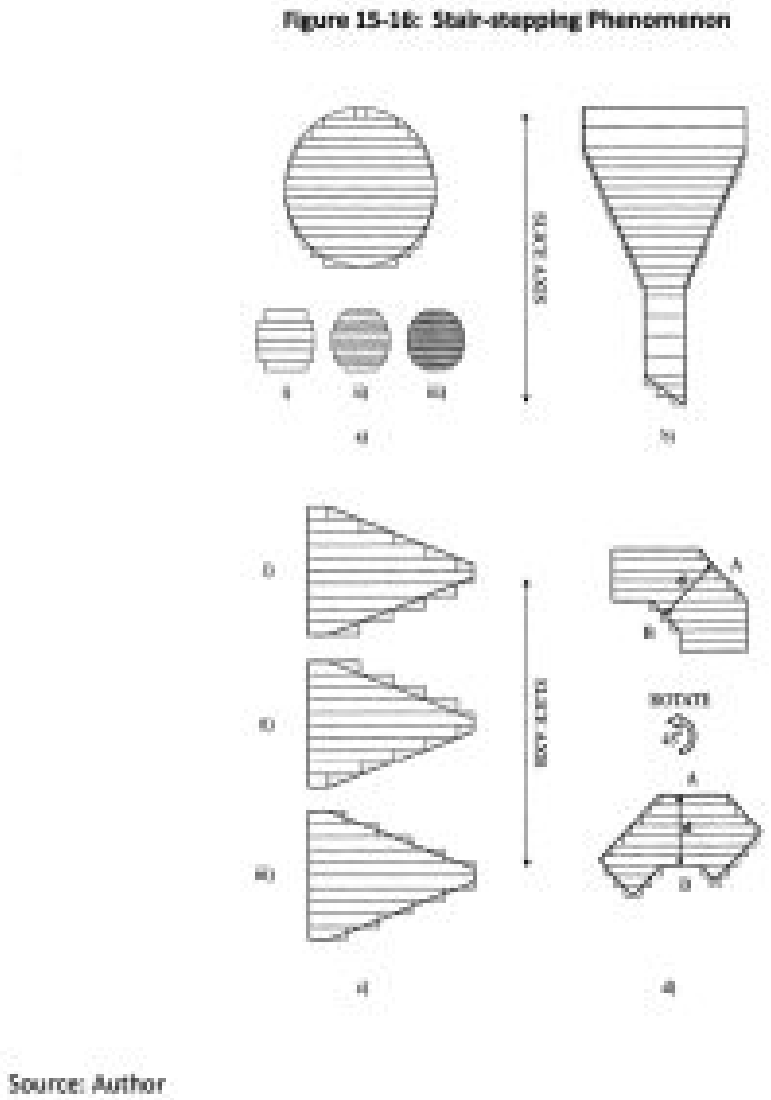
The method of manufacturing objects as a series of horizontal layers poses a unique set of problems, irrespective of the techniques involved in the fabrication of each layer. This section is intended to provide the reader with some insight into the considerations that must be made when building parts by layered manufacturing techniques.

STAIR-STEPPING PHENOMENON

The slicing process described earlier produces a set of horizontal cross sections, each of these sections conforms to the geometry of the original CAD model to a degree of accuracy, which is significant to the entire process. However, each layer is of continuous cross section through its thickness (i.e., in the Z-direction), and therefore

parts cannot accurately conform to the CAD geometry in the vertical plane. This is best illustrated by considering the situation shown in Figure 15-16. A cylinder has been built with its circular cross section parallel to the slice axis, i.e., perpendicular to the layers. If any single part layer is considered, slicing software has produced a layer, the top surface of which conforms precisely to the CAD geometry. However, because the layer is rectangular in cross section it cannot conform to the curved surface across its entire thickness, the largest deviation at its bottom surface. This results in the stepped effect shown which has been termed the stair-stepping phenomenon.

Figure 15-16: Stair-stepping Phenomenon



Source: Author

Source: Author

LAYER THICKNESS

It is clear from the example shown in Figure 15-16 (a) that the smaller the slice thickness, the greater the resolution of the final part (as shown by cylinders (i) to (iii)). It may seem sensible to use the smallest possible layer thickness that can be physically created by the system, but the smaller the layer thickness, the more slices are required resulting in longer data processing time, larger data files and a longer build time. To optimize the process, variable layer thickness may be used over different ranges of the part. The example of the funnel shown in Figure 15-16 (b) has a fine layer thickness where the surfaces are sloped, and stair-stepping is more pronounced, and thicker layers on the vertically sided sections.

EFFECTS OF CAD GEOMETRY

In the two examples provided so far it is the top surface of each layer that conforms to the CAD geometry, and this is the case in many of the commercially available systems. The reason for this can be seen if we consider the SLA process in which a laser beam is guided across the surface of a vat of liquid polymer, tracing out the geometry of each layer, and whenever the laser strikes the resin surface, a small volume is cured and solidified to a depth dependent on laser power and scan speed. The top surface of the layer must conform to the CAD geometry because that is what is drawn on the resin surface, with a continuous depth cured below it provides the layer thickness.

Figure 15-16 (c) shows three different ways in which the layers might conform to the CAD geometry, in each case the shaded areas represent the deviation from the true geometry. Example (i) shows the case where the top of each section conforms to the required layer outline, and example (ii) shows the opposite case in which layers are formed from the bottom up. It is clear from these examples that extent of deviation will be dependent of the gradient of the sloping surface, and whether the error is positive or negative will depend on the direction of slope. In many cases the most favorable situation would be where all deviation was positive and excess material could then be carefully removed to leave the accurate part. However, the additional processing power required to produce the necessary data corrections ensures that only positive deviations may prove prohibitive over the layers. The situation shown in example (iii) represents the intermediate case where the center of each layer conforms to the CAD geometry, resulting in smaller deviation in both directions. This would produce the most accurate parts in terms of maximum deviation, but again a large amount of additional processing power would be required.

PART ORIENTATION

The manual finishing of parts built by layered manufacturing to remove the stair-stepping effect is the most labor-intensive phase of the process, and great skill is required if dimensional accuracy is to be maintained. The only part surfaces that will not exhibit stepping are those built parallel to the slice plane, and therefore parts should be oriented so that cosmetically important faces are built in this direction and important dimensions are built parallel to the slice axis. Figure 15-16 (d) shows how a simple 45O rotation improves the surface finish of faces A and B, and maintains the accuracy of dimension. However, this may have a detrimental effect on other features of the part and so a suitable balance must be found. This analysis assumes that the 'as built' geometry is more accurate than the hand finished geometry, but this depends on the skill of the model maker and the accuracy of the process.

The build time involved in the fabrication of any part is principally dependent on the number of layers involved, and may therefore be minimized through careful selection of the part orientation. However, it is not simply a matter of choosing the orientation with the smaller z-height because all the other effects discussed must also be considered, and a compromise must be made. In many layered manufacturing systems, the degree of part distortion occurring as a result of the layer generation process is department on the orientation of the part with respect to the slice axis. Therefore, another consideration is introduced in selecting the most suitable build orientation.

SUPPORT STRUCTURES

In any manufacturing technique the workpiece must be mounted or supported in some way in preparation for processing, for example held in the vice of a machine tool or the chuck of a lathe. AM processes also require to be mounted to hold it in position, and further structures are often required to support unstable geometry as they are built. The principal benefits achieved by these systems stem from the fact that the processes are fully automated, and that part specific fixtures or tooling are not required, and therefore it is not possible to manually position prefabricated fixtures and still reap the same benefits. However, the fact that rapid prototyping systems fabricate whatever is described by the CAD input means that they can build any support structures in the way that they build the parts, thereby maintaining their flexibility and automated nature.

Initially, support structures were designed on the CAD systems in conjunction with the part, but this was labor intensive, and the operator was required to have a full understanding of the part building process. Software packages have been developed which generate the design of any required supports automatically by inspecting the part geometry and assessing what is required. The support designs are then sliced in the way as the part and incorporated into the build information sent to the fabricator. The supports are fabricated in the same way as the part and are incorporated into it, but are normally in the form of grids of very thin webs that may easily be removed once the part is complete.

Support structures perform the following important functions:

Act as a mounting device holding the part in position as it is built.

This is particularly important in those techniques that form parts from a vat of liquid resin (e.g., stereolithography) where the bottom layer must be firmly attached to the build platform to stop the part floating away.

Act as a constraint reducing part distortion

In many rapid prototyping processes, the procedures involved in creating individual layers from their raw materials involves either a total phase change (e.g., liquid resin cured to solid resin) or localized heating and cooling cycles (e.g., selective sintering of powdered materials). In either case the degree of material shrinkage causes some part distortion. Supports may be used to constrain these distortions to some extent thereby improving part accuracy. Part distortion can also occur due to faulty STL files. Missing points, missing facets or just poor data manipulation algorithms may cause distortion in the final object. However, with the right procedures in place, the problems associated with the building process can be minimized.

SPACE STRUCTURES AND SPACE COMPLEXES

The exploration of space for manufacturing purposes is enabled by systems and complexes that provide physical infrastructure, technologies, and operations required for space exploration. The complexes play a crucial role in enabling manufacturing processes and systems to operate beyond the confines of Earth to manufacture products in space using the advantages provided by an environment that promulgates innovations in products and processes.

Space systems refers to hardware, software, and communications designed to operate in the space environment. Space systems are needed for scientific research, satellite deployments, interplanetary missions, and space exploration. Satellites form a fundamental part of space systems and monitor weather, communications, etc., (Figure 15-17). Orbiting spacecraft provide data for weather forecasting, communications, and monitoring the Earth environment. Advanced propulsion systems, navigation, and communication protocols are integrated into space systems to ensure the successful and efficient process of manufacturing in space.

Figure 15-17: NASA's Earth Science Satellite Fleet

Source: Image Courtesy of NASA, July 12, 2023. (https://earthobservatory.nasa.gov/images/81559/nasas-earth-science-satellite-fleet).

Space complexes, known as spaceports or launch facilities, serve as the gateways to space and the manufacturing environment. These facilities include launch pads, control centers, and assembly buildings. They provide the infrastructure and resources to prepare, test, and launch spacecraft. Space complexes, such as Kennedy Space Center in Florida (Figure 15-18), Baikonur Cosmodrome in Kazakhstan, and the European Spaceport in French Guiana, are space complexes that coalesce scientists, engineers, and technicians from different countries to work towards refining the processes associated with space manufacturing. Space complexes are not only vital for government space agencies such as NASA, Roscosmos and ESA, but also for private space companies like SpaceX, Blue Origin, and Virgin Galactic, companies that are pioneering space travel that creates opportunities to manufacture in space products that cannot be made on Earth such as immiscible alloys, high purity pharmaceuticals and defect free semiconductors.

Figure 15-18: Kennedy Space Center's Vehicle Assembly Building on April 29, 2021

Source: Credits: NASA/Frank Michaux.

The preparation of materials on Earth using simulated conditions of space have been developed based on weightlessness and numerical models of material behavior using facilities on Earth. Ground facilities include drop towers, buoyancy pools, air-borne laboratories, and balloons. Space complexes on Earth includes short span microgravity experiments up to 10 minutes, but the real measure of the ability to manufacture in space is due to experiments conducted on space complexes.

The International Space Station (ISS) is a space complex (Figure 15-19) that serves as a manufacturing laboratory. Here, highly specialized materials have been created for the purpose of manufacturing products and secondary work has been done to understand the conditions of manufacturing in space, i.e., heat and mass transfers and solidification processes that involve the formation of dendrites and grains.

Space systems and space complexes are set to increase the significance of the development of manufacturing processes that take advantage of zero gravity conditions in a vacuum with the elimination of convection currents. Exploration projects, such as NASA's Artemis, aim to return to the Moon to prepare for missions to

Mars. This will require the development of advanced launch systems, habitats, manufacturing processes and systems and life support systems.

Figure 15-19: The International Space Station

Source: Image courtesy of NASA, July 13, 2023 (https://www.nasa.gov/press-release/nasa-administrator-statement-on-russian-asat-test).

The emergence of private companies such as Space Forge has added a new dimension to space manufacturing. With the advent of reusable rockets and satellites, space complexes are witnessing a surge in activity that is driving innovation, making space more accessible, and pushing the boundaries of what is possible in space manufacturing (Weinzierl and Acocella, 2016). The conditions required to produce high performance materials include understanding gaseous and liquid phase processing of feedstocks, converting to a liquid phase followed by solidification and casting. These are energy intensive processes and so the space complex must be designed to provide the required energy needed to manufacture products in space. Early studies of manufacturing in space relied on space complexes operating in a weightless environment, with a limited size and power limitations. Therefore, the design of space systems and complexes specifically for manufacturing need to be developed to advance space exploration where items are made rather than taken from Earth.

ECONOMY-ORIENTED SPACE MISSIONS AND STRATEGIES

Economy-oriented space missions and strategies refer to initiatives and approaches that focus on using space resources and activities to stimulate economic growth and development. Economy-oriented space missions and strategies include:

Space Manufacturing: Using the conditions of space, such as microgravity and vacuum, so that private enterprises can manufacture products that cannot be made on Earth, such as pharmaceuticals, materials, advanced semiconductors, and the production of advanced nanotechnologies. Commercializing these activities can lead to economic benefits and technological advancements (Weinzierl and Sarang 2021, Weinzierl et alia 2021).

Resource Extraction: There are various resources in space that can be mined, including rare metals, water, and oxygen. Developing technologies and strategies for extracting and using these resources will lead to a new space-based economy (Weinzierl and Acocella 2017, Weinzierl and Haddaji, 2019, Weinzierl et alia 2021).

Space-based Energy: Capturing solar energy in space using large-scale solar arrays, suing it for manufacturing purposes in space or transmitting it back to Earth wirelessly is a goal that is highly desirable. Space-based energy systems could provide a virtually unlimited and clean energy source, revolutionizing the energy sector and creating new economic opportunities for manufacturing industries.

Space Debris Cleanup: As space debris poses a growing threat to satellites and space missions, there is a need for technologies and missions aimed at removing or mitigating debris. Developing cost-effective cleanup strategies could not only improve space operations but also create a feedstock for circular manufacturing systems in space (Weinzierl et alia 2016).

Space Tourism and related development of consumer goods: The rise of space tourism presents significant commercial opportunities. It could create demand for consumer goods and products specifically designed for the space environment. This could range from clothing and food to entertainment and personal care products. Manufacturing these goods in space could cater to the emerging space tourism market and create new economic opportunities. Further, space manufacturing can contribute to the development of space tourism infrastructure, including the production of spacecraft, habitats, and life support systems specifically designed for space tourists (https://hbr.org/2021/02/the-commercial-space-age-is-here).

These are just a few examples of economy-oriented space missions and strategies. As technologies advances and space exploration continues, new opportunities will emerge, enabling the development of a strong space economy.

ECONOMIC FEASIBILITY OF SPACE-RELATED ACTIVITIES AND MISSIONS

Economic feasibility largely depends on technological and infrastructure readiness, regulatory framework, and market dynamics.

Technological and infrastructure readiness is a required condition for commercialization of space which includes activities such as low-cost, frequent launch capabilities; in-space manufacturing; scalable habitats; in-space resource extraction and energy collection; and reliable radiation shielding and debris mitigation. This is evidenced related to space transportation with the public-private partnership called Commercial Orbital Transportation Services (COTS) developed by NASA in 2005. COTS allowed NASA to adopt a more targeted role focused on space exploration and basic science, leaving economic development of space largely to the private sector. It also made NASA a customer and partner of its private contractors. Thus, this public-private partnership approach allowed for a self-reinforcing virtuous cycle of development that could support the space economy. As an example, Weinzierl (2018) explains cheaper and more frequent rocket launches might facilitate short-term tourism, along with industrial and scientific experimentation on suborbital and orbiting spacecraft. Routine activities could lead to demand for commercial habitats and longer flights, leading to increased demand for resources in space and opportunities for complementary activities.

Space missions are often funded by governments through space agencies like NASA (United States), ESA (European Space Agency), Roscosmos (Russia), and others. These agencies allocate budgets for research, development, and space exploration. Government funding is driven by various factors, including national interests, scientific objectives, defense considerations, and international collaborations. *Regulatory framework* could encompass multiple dimensions, from property rights considerations to distributional concerns, and mitigating negative externalities that can arise due to space-related activities. The space debris problem hints at the tragedy of commons scenario and threatens to become unmanageable if regulatory oversights are not exercised. It is a classic example of negative externalities, and conventional remedies suggested by economic theory such as standard Pigouvian price on debris fails in this case since there is no established space taxing authority (Hansen 2016). Lack of delineated property rights additionally make it harder to quantify and internalize externalities related to space debris. With respect to regulatory purview, a concerted effort to enact international treaties and agreements would be instrumental in resolving many potential challenges associated with space activities currently and in the future. Some policy questions that need to be considered when developing a commercial space sector in a country include government's role in coordinating and subsidizing interdependent technologies, nature of subsidies to implement such as cost-sharing, revenue guarantees, incentives etc. (Weinzierl 2018).

Market dynamics considerations play out when a centralized model is transformed to a decentralized one. Typically, public goods provisions are guaranteed in a centralized model and typically left underprovided if left to the market. High demand and cost conditions in a sector can be instrumental in paving the way for a decentralized model. For example, the COTS program allowed NASA to leverage private capital to acquire required services cheaply. Apart from subsidizing commercial launch vehicles, a competitive market structure

was developed due to a diversified set of award contracts. Additionally, decentralization also spurred activities and innovations, broadening the space economy. Market structures and functioning depend on analyzing demand conditions and associated costs:

1. a) Market demand and revenue generation opportunities for space-manufactured products need an assessment of the market potential, competitive landscape, pricing strategies, and potential partnerships or customers. Some factors beyond the conventional needs such as space manufacturing, resource extraction etc. that can stimulate demand for space activities are potential for spin-off technologies that have applications beyond space exploration. Many everyday technologies and innovations have been derived from space-related research and development, including satellite communication, miniaturized electronics, improved materials, and medical advancements. These spin-off technologies can have significant economic impacts across various industries. New markets and industries can also develop which could include space-based construction, manufacturing facilities in space, space-based agriculture, and manufacturing goods specifically tailored for space habitats or off-world settlements. These new markets can foster economic growth and provide novel business opportunities.
2. b) Various factors that need to be considered when analyzing costs towards space activities such as in-space manufacturing and space missions include:

- Cost of Development: The development and construction of space missions includes costs associated with research and development, design, engineering, manufacturing, and testing spacecraft, launch vehicles, ground infrastructure, and other necessary equipment.
- Launch Costs: Some of the expenses could include launching manufacturing equipment, raw materials, and supplies from Earth to space, payloads into space using rockets or other launch vehicles. The development of reusable rockets and in-space refueling infrastructure could potentially reduce these launch costs.
- Operations and Maintenance Costs: Space missions would include costs associated with tracking and communication systems, data analysis, mission control operations, ground support, and maintaining the health and functionality of the spacecraft. In-space manufacturing costs would include the costs of personnel, power supply, monitoring and control systems, waste management, and regular maintenance and repairs of the manufacturing equipment and facilities.
- Resource Acquisition Costs: In-space manufacturing often relies on utilizing local resources, such as asteroid mining or lunar resource extraction. Evaluating the expenses associated with identifying, extracting, and processing these resources, development of resource prospecting technologies, mining techniques and refining processes would be required.
- Labor Costs: Assessing labor costs is essential when considering human involvement in in-space manufacturing operations and space missions. Costs include training and supporting astronauts or space workers, as well as potential automation and robotic systems that could reduce labor requirements

and associated expenses.

- Cost Reduction Strategies: International collaborations and public-private partnerships can help distribute costs and share resources. Launch costs can be reduced by utilizing local resources, avoiding transportation expenses, and minimizing reliance on Earth-based supply chains. Other strategies include reusable rockets, 3D printing of spacecraft components, miniaturization of satellites, and increased automation in manufacturing and operations. Instead of relying on Earth-based supply chains and waiting for resupply missions, astronauts or automated systems could produce and repair parts, tools, or equipment as needed, leading to on-demand manufacturing and repair capabilities. This reduces the need for stockpiling and improves mission sustainability.
- Scale and Efficiency: Economies of scale can be realized when average costs fall by increasing production. The company Space Exploration Technologies (SpaceX) demonstrates both economies of scale and efficiency characterized by reusability, reusability without over-engineering, and vertical integration. Even though reusability imposes new costs such as research and development to establish vertical landing capabilities, operating expenses to recover spacecraft and fairings, and refurbishment efforts between launches; enough demand and low average costs were instrumental for its successes. SpaceX sought to take advantage of a virtuous cycle in which growth led to cost reductions and, thus, more growth through lower prices (Weinzierl et al. 2021). Cost efficiency was realized by focusing on reliability without over-engineering and vertical integration. SpaceX used off-the-shelf components, and previously used, proven technologies wherever possible rather than developing new, custom-built technology. Highly vertically integrated structures allowed them to eliminate transaction costs throughout the supply chain.

CONCLUSIONS

The developments of manufacturing in space are wide and include planetary mining and manufacturing on planet, asteroid mining and manufacturing, and manufacturing in orbit. The challenges to integrate systems to minimize waste and effort are significant. The space environment develops materials that cannot be made on Earth owing to differences in gravity or environmental factors. The scientists of the future will need to design and build systems and complexes to support the economy-oriented approach to manufacturing products in space and the complexities associated with costs associated with this activity need to be fully understood and their effects quantified.

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. Why is manufacturing in space different to manufacturing on Earth? Compare and contrast the differences.
6. Why is the application of systems engineering principles critical to manufacturing in space?
7. Describe space missions for manufacturing in space.
8. What are the initiatives that make up the economy-orientation space missions?
9. Explain how space missions are funded and why they are funded in the first place.
10. Why did Blue Origin and SpaceX become so successful in such a short space of time and how did they reduce the costs associated with space travel?

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 be 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

Hansen, Ward. 2016. "Pricing Space Debris." New Space 2 (3): 143-44.

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.

https://www.cape.osd.mil/files/OS_Guide_Sept_2020.pdf

https://www.nasa.gov/pdf/140643main_ESAS_12.pdf

https://ntrs.nasa.gov/api/citations/20170009900/downloads/20170009900.pdf

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>

Jackson, M. J., Additive Manufacturing Technologies, Kansas State University Course Notes for MET 231 Physical Materials and Metallurgy, Kansas State University, January 2023.

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

Nicholls, R. K., et alia, Space Systems: Emerging Technologies and Operations, New Prairie Press, Kansas State University Libraries, Manhattan, Kansas, USA. October 2022. ISBN: 978-1-944548-48-3. https://newprairiepress.org/ebooks/47/

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 and 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, 2023. *SpaceX Homepage*. https://www.spacex.com/. (cited 12 July 2023).

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.

Werkheiser, Niki. "In-Space Manufacturing: Make It, Don't Take It!" October 7, 2017

Weinzerl, M., Acocella, A. and Yamazaki, M., Astroscale, Space Debris and Earth's Orbital Commons, Harvard Business School Case Study, 9-716-037, May 10, 2016.

Weinzerl, M and Acocella, A., Blue Origin, NASA and New Space, Harvard Business School Case Study, 9-716-012, May 31, 2016.

Weinzerl, M and Acocella, A., Planetary Resources Inc., Property Rights, and the Regulation of the Space Economy, Harvard Business School Case Study, 9-717-053, April 5, 2017.

Weinzierl, M. 2018., "Space, the Final Economic Frontier." Journal of Economic Perspectives, 32 (2): 173-192.

Weinzerl, M and Haddaji, A., Space Angels, Multiple Equilibria, and Financing the Space Economy, Harvard Business School Case Study, 9-719-070, May 2, 2019.

Weinzierl, M., and Sarang, M., Made In Space, Expectations Management and the Business of In-Space Manufacturing, Harvard Business School Case Study, 9-721-025, March 30, 2021.

Weinzerl, M., et al., SpaceX, Economies of Scale and a Revolution in Space Access, Harvard Business School Case Study, 9-720-027, October 5, 2021.

16.

THE QUANTUM FUTURE OF SPACE WARFARE [DREW]

OBJECTIVES

- Students shall comprehend the foundational differences between quantum technology and legacy computing, communication, encryption, and measurement technologies.
- Students shall assess the capabilities and limitations of quantum computing, communication, encryption, and measurement to the field of space operations.

INTRODUCTION

In this chapter, we provide a brief introduction to quantum technologies, including quantum computing, quantum communications, quantum encryption, and quantum sensing. We will explore the physical principles behind the quantum technologies and the potential applications of these quantum technologies to space operations. Because quantum technologies and the quantum mechanics behind them are highly technical disciplines, this chapter does not endeavor to explain them in any level of technical detail. Rather, it provides a basic overview of some of the fundamental ideas behind quantum technologies in order to allow the reader an appreciation for what is currently happening in space with regard to these fields and what could realistically happen in the future. Thus, the reader should leave with an appreciation of the state of the art of quantum technologies as they apply to space operations.

The state of the art is evolving rapidly, and space-related applications of quantum technologies still depend on government funding. As a result, these programs are subject to budgetary, developmental timelines, and flight scheduling considerations. The nature of fundamental science development became apparent to me when, as a junior space operations officer, I visited the Applied Physics Laboratory at Johns Hopkins University in the autumn of 2011. They were, at the time, experimenting with quantum computing, and I asked our guide when he thought they would have an operational quantum computer. Our guide was prepared for the question and responded that he thought the technology would be operational in about twenty years.

While the guide and I did not agree on a definition of "operational," now past the halfway point of that twenty-year period, it looks like my guide had estimated conservatively. Quantum technologies continue

to evolve rapidly, and the applications of those technologies promise revolutions in complex computation, cryptography, and precision measurement. Think-tanks, consulting firms, defense organizations, industry, and academia are awash with studies on these subjects, and there is a justified concern that existing systems and methods are vulnerable—or will be vulnerable in the near term—to attacks by actors with advanced quantum technologies. More private capital investment is on the horizon. For quantum computing specifically, the industry is expected to grow from "$412 million in 2020 to $8.6 billion in 2027" (Campbell, 2023). Among nations and corporations, there is an obvious desire to master these technologies as quickly as possible because doing so provides first-mover advantages in science, defense, and business.

But just what are these quantum technologies and what makes them different from legacy digital methods? Furthermore, what are the implications of these technologies for space operations? As stated, the aim of this chapter is not to make the reader an expert on quantum mechanics or space operations but to provide a basic understanding of how quantum computing, quantum communications, quantum encryption, and quantum measurement work and how those technologies are already affecting or will affect space operations.

To that end, it may be valuable to address some limitations about quantum technologies up front. First, in most cases, quantum technologies are more likely to augment rather than supplant classical computing, communication, encryption, and measurement methods; we will still need traditional methods for the foreseeable future. Second, digital computers, the networks that connect them, and their data are not helpless against quantum intrusion. Quantum intrusions can be defended against, as we will see in the discussion on post-quantum cryptography (Bernhardt, 2019). Third, quantum technologies are not always the most practical option; searching large amounts of data, for example, may be best accomplished by either classical or quantum methods, depending on the conditions (Bernhardt, 2019). Like any other tool, both digital tools and quantum tools must be applied in the ways that are best suited to their strengths while minimizing their vulnerabilities. In other words, it is important to assess the capabilities and limitations of these technologies objectively, recognizing that they are neither a panacea for all our problems, nor are they harbingers of certain doom.

To begin considering the strengths and vulnerabilities of these tools, it is necessary to understand some fundamentals about digital and quantum technologies, and while this discussion begins with a focus on quantum computing, the ideas apply across quantum applications. The primary difference between digital and quantum technologies lies in what physical phenomenon are used to convey information. Digital computers encode information in a binary system that uses the presence or absence of an electrical signal to represent ones and zeros. If an electrical signal is present, the value of the bit is one; if there is no electrical signal, the value of the bit is zero. Different combinations of ones and zeros correspond to different symbolic values. For example, the numbers zero through five can be represented by the strings of ones and zeros as shown in Table 16-1 below.

Table 16-1: Representation of numbers zero through five as binary numbers.

Number	Binary representation
0	0
1	1
2	10
3	11
4	100
5	101

Source: (Math is Fun, "Binary Number Systems," , 2023)

Whereas traditional computing uses electrical signals to generate ones and zeros, quantum computers use the physical properties of elementary particles: electrons or photons (Bernhardt, 2019). For electrons, the physical property is called *spin*. Like the Earth or a dipole magnet, electrons have a north and a south pole, and spin is a measurement of how far the electron's polar axis is tilted from the vertical (Bernhardt, 2019). For photons, the measured property is polarization; the angle of a polarized light particle (a quanta) as it passes through a filter is measured (Bernhardt, 2019). While both particles are available for quantum technologies, it is important to note that the ongoing investigations related to space operations discussed in this chapter primarily employ photons.

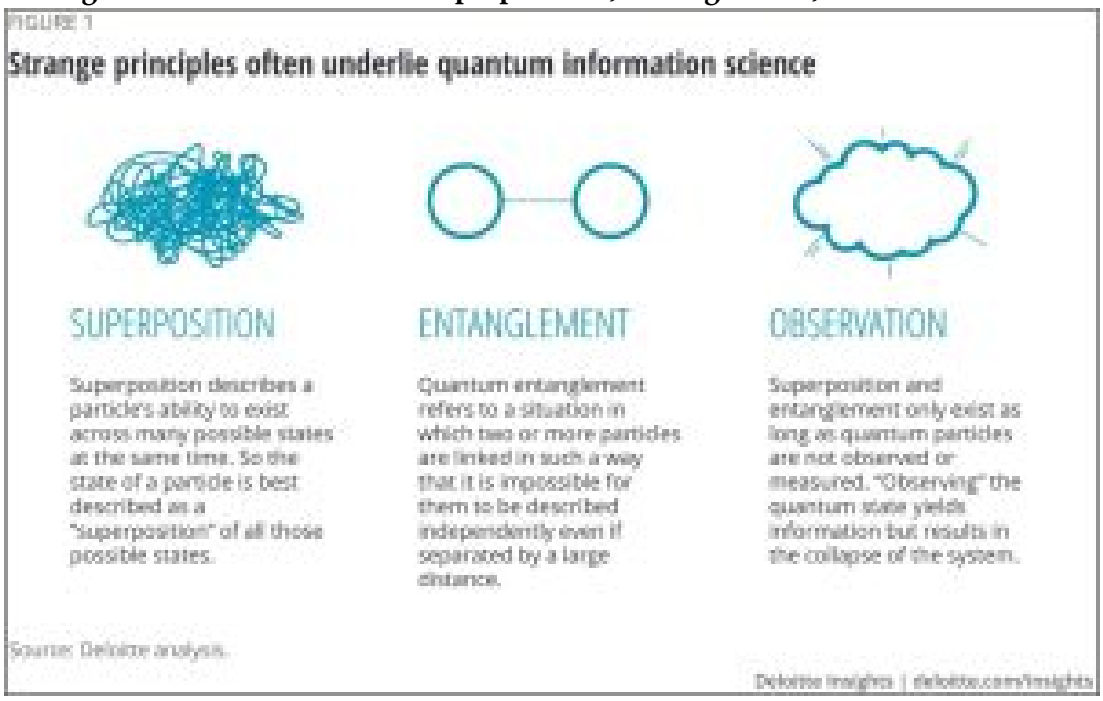
Whether measuring electrons or photons, the way in which the measurements occur influences the outcome of the measurement and must be accounted for (Bernhardt, 2019). Furthermore, the outcomes of the measurements can only be assessed probabilistically (rather than with certainty as in the case of measuring whether an electrical switch is deterministically either on or off). This information is encapsulated in a quantum bit, or qubit, which then may be translated into a string of traditional bits (Van Amerongen, 2021). Traditional computing and quantum computing, therefore, are complementary technologies but before delving into the topic of quantum computing specifically, it is necessary to discuss the unusual properties of quantum particles.

UNUSUAL QUANTUM PROPERTIES

Electrons and photons behave in non-intuitive ways. The below figure describes these properties: superposition, entanglement, and observation. Each of these properties creates challenges and opportunities for how quantum systems may be used. First, to put it in terms of a classical computing analog, superposition means that a qubit can be *both* a one and a zero at the same time (Van Amerongen, 2021). The challenge is that

this physical state requires extremely low temperatures, only about 15 millikelvins above absolute zero (Van Amerongen, 2021). The opportunity is that superposition potentially enables quantum computers to perform multiple calculations simultaneously, allowing them to solve problems so complex that they are beyond the capacity of even the most powerful supercomputers (Van Amerongen, 2021).

Figure 16-1: Definitions of Superposition, Entanglement, and Observation



Source: (Buchholz & Mariani, 2020)

Entanglement means that when one particle is entangled with one or more other particles, what happens to one particle—a change in spin, for example—will simultaneously affect the other particle, even when separated by vast distances without any apparent physical way of exchanging information—what Albert Einstein famously called "spooky action at a distance" (Simonite & Chen, 2023). Being able to "produce and detect pairs of entangled photons" is essential for transmission of information among quantum computers and other relay nodes like satellites, but doing this, and producing the number of terminals and nodes needed for a quantum internet involves a series of complicated scientific and engineering tasks that are only now becoming feasible (O'Neill, "Space station to host 'self-healing' quantum communications tech demo." NASA Jet Propulsion Laboratory. , 2022); (Buchholz & Mariani, 2020)

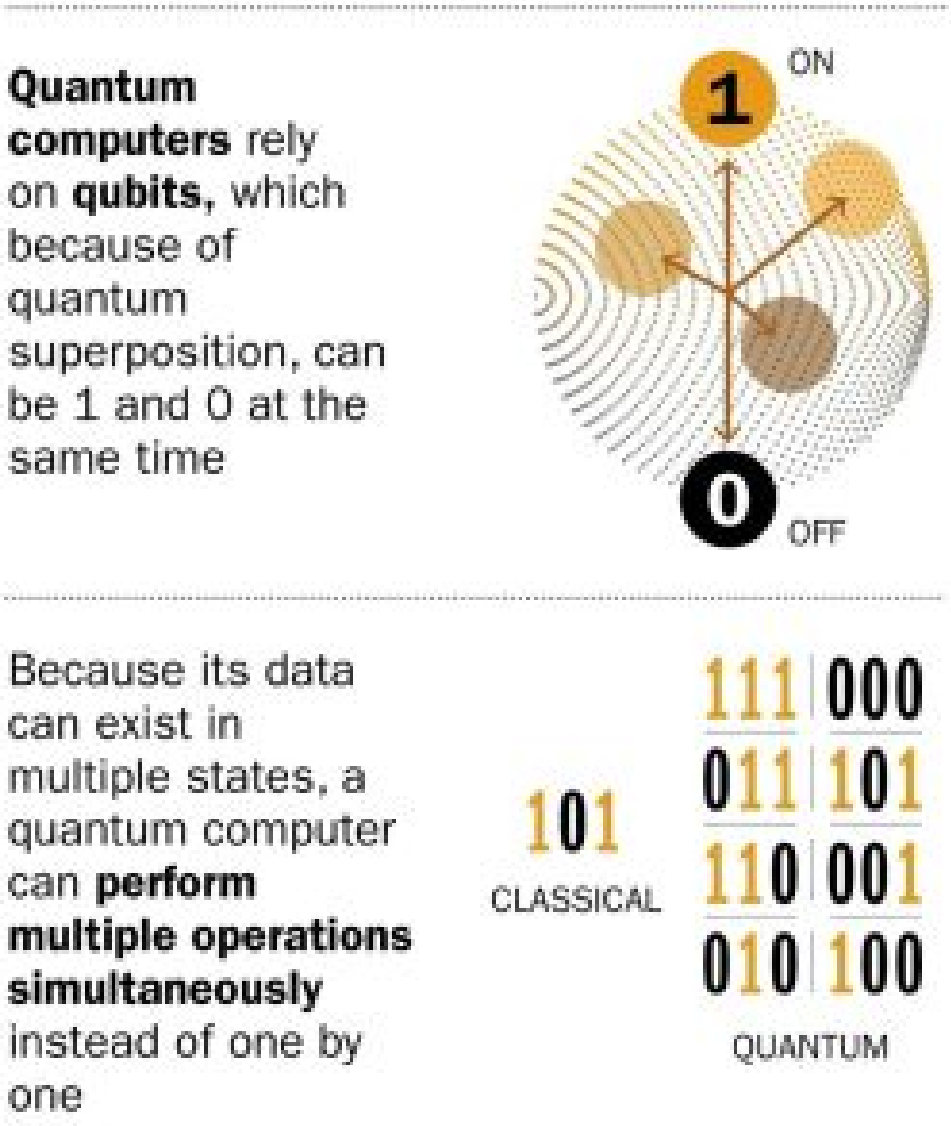
Finally, once entangled particles are observed, they cannot be read again. The act of observing them changes their natures, which "can be a great advantage for secure communications" but also makes copying computer code impossible in the classical way and testing programs exceedingly difficult (Buchholz & Mariani, 2020). Furthermore, because photons and electrons exist everywhere in nature, entangled particles are subject to

interference from the natural environment, limiting the distances over which they can be transmitted on fiber optic networks without "trusted nodes" to function as repeater stations (Kwon, 2020).

QUANTUM COMPUTERS

In the discussion of quantum technologies, the place to begin is with a discussion of quantum computers. As mentioned in the introduction, quantum computers have been under development for quite some time, and their power and sophistication are increasing at significant rates. The International Business Machine Corporation (IBM) is currently the industry leader with its Osprey chip (Campbell, 2023). Unveiled in 2022, Osprey's capacity is 433 qubits, and IBM plans to create a 4,000-qubit chip by 2025 (Campbell, 2023). As long as quantum computers continue to double in processing power every six months—"four times faster than Moore's law for classical chips"—IBM's goal remains realistic (Buchholz, Mariani, & Routh, 2020). While quantum computing is not a topic of household conversation, quantum computers have already exceeded the capacity of traditional supercomputers.

Figure 16-2: Because qubits can exist in multiple states simultaneously, they can perform multiple operations simultaneously



Source: *(Campbell, 2023)*

The point at which quantum computing power outpaces traditional computing power is called quantum supremacy and was first demonstrated in a combined effort of the National Aeronautics and Space Administration (NASA), Google, and Oak Ridge National Laboratory in 2019 (Tavares, 2019). In this experiment, Google's Sycamore quantum processor outlasted NASA's Electra petascale (quadrillions of operations per second, or a thousand trillion calculations) supercomputer in a test of computing complexity with only 53 qubits—less than an eighth of the computing power of Osprey (Tavares, 2019); (Savage, 2019). To verify that the advanced calculations of Sycamore were correct, the team used Oak Ridge National Laboratory's Summit supercomputer, at that time the "most powerful supercomputer in the world," to

check Sycamore's math—until the point where not even Summit could keep up (Tavares, 2019). Sycamore can achieve rates of about 200,000 trillion calculations per second, or 200,000 teraflops (Remmel, 2022). Interestingly, since the Sycamore experiments, Oak Ridge's newest supercomputer, called Frontier, was the first to achieve exascale computing—a performance three orders of magnitude beyond petascale or more than one million trillion operations per second (Remmel, 2022). As of April 2023, Argonne National Laboratory's Aurora supercomputer and Lawrence Livermore National Laboratory's El Capitan supercomputer—both petascale computers—have yet to be completed but may reach operational status by the end of the year (Moss, 2023); (Bartman, 2023).

As Electra, Sycamore, Summit, and Frontier demonstrate, advances in traditional computer science are progressing alongside advances in quantum computing, and the two efforts often go hand-in-hand. One application of Frontier is simulating "molecular models with more atoms with greater complexity and on longer timescales than ever before" to gain new insights into chemical theory (Remmel, 2022). One might easily imagine that such advanced calculations will shed light on the behavior of not only atoms, but also of electrons and photons, the very behaviors of which are necessary for quantum computing. In a practical sense, such advanced calculations open up a host of other possibilities. It may be possible to "invent novel fuel sources and design new climate-resilient materials;" to visualize the millions of atoms in a virus, as was done with COVID-19 (Remmel, 2022); to enable advanced testing of the nation's nuclear stockpile without detonation (Bartman, 2023); to optimize shipping routes or patient medical care (Campbell, 2023), or to simulate the fluctuations of financial markets more accurately (Bova, 2021). Calculations that "involve finding an arrangement of items that optimizes some goal" are called combinatorics and are a particular strength of quantum computers (Bova, 2021).

As we will see shortly, encryption is a combinatorics problem that has particular utility in space operations applications. First, however, it is necessary to discuss how space might be involved in connecting the information created and stored by quantum computers. Then we may discuss how this information can be secured through quantum encryption. Finally, quantum sensors can feed into this network either using satellites to relay their observations or as payloads on the satellites themselves.

SATELLITES: NODES ON THE NETWORK

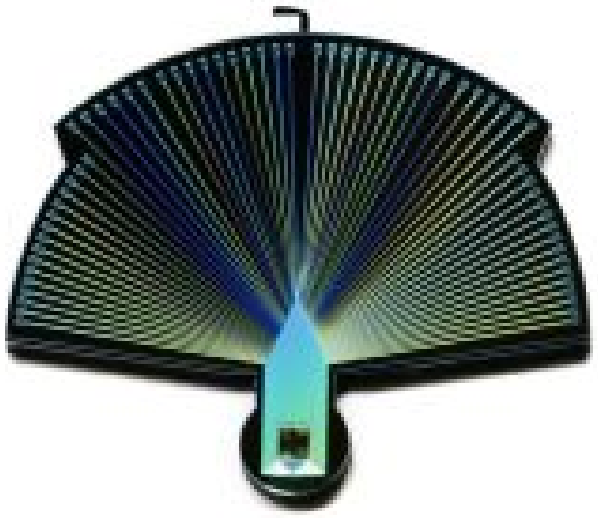
As with the early analog-computation satellites and with the current digital-computation satellites, satellites are nodes on a network. They must receive commands from ground stations to conduct their normal operations, and they must pass data down to ground stations or to other satellites to provide utility. All satellites regardless of their size or function share these characteristics, and they employ on-board computers to process information and radio or laser transmitters and receivers to relay it.

The way in which information is relayed between a satellite and a ground-station computer changes significantly with the employment of quantum technology. To relay information between quantum computers, entangled photons need to be generated and sent to two different quantum computers, each

capable of receiving and measuring the photon (O'Neill, "NASA's quantum detector achieves world-leading milestone." NASA Jet Propulsion Laboratory. , 2023). Indeed, this is the way that ground-based quantum computers relay the quantum keys necessary to decrypt and encrypt streams of information, and this is how China's *Micius* satellite was able to successfully distribute quantum keys to two ground stations in 2017 and conduct "the world's first quantum encrypted virtual teleconference between Beijing and Vienna" (Kwon, 2020).

One limitation of *Micius* was the need for exceptionally low error-detection rates (Kwon, 2020). Two separate NASA projects are working on both the transmission and the receiving technologies necessary to enable space-based relay between quantum computers. First, the Space Entanglement and Annealing Quantum Experiment (SEAQUE) will demonstrate the ability to produce and internally measure entangled photon pairs on the International Space Station (O'Neill, "Space station to host 'self-healing' quantum communications tech demo." NASA Jet Propulsion Laboratory. , 2022). Second, the Performance-Enhanced Array for Counting Optical Quanta (PEACOQ) has demonstrated the ability within a laboratory to detect 1.5 billion photons per second and measure "the precise time each photon hits it, within 100 trillionths of a second" (O'Neill, "NASA's quantum detector achieves world-leading milestone." NASA Jet Propulsion Laboratory. , 2023).

Figure 16-3: NASA's PEACOQ Detector



Source: *(O'Neill, "NASA's quantum detector achieves world-leading milestone." NASA Jet Propulsion Laboratory. , 2023)*

Detectors like PEACOQ must retain the ability to make accurate measurements over time—a task that is a challenge in the space environment because everything in space is continuously bombarded by various forms of radiation that can degrade sensors (O'Neill, "Space station to host 'self-healing' quantum communications tech demo." NASA Jet Propulsion Laboratory. , 2022). SEAQUE is demonstrating the additional technology of an on-board laser to repair degradation to the sensor (O'Neill, "Space station to host 'self-healing' quantum communications tech demo." NASA Jet Propulsion Laboratory. , 2022). With these two technologies, NASA is investing in the foundational technologies necessary to produce and measure entangled photons. But these two experiments only provide hardware for the distant ends of the link. To connect the ends, laser communications will be necessary.

Satellites typically communicate with the ground by using radio frequencies, but laser communications are becoming more common. NASA's Lunar Laser Communications Demonstration (LLCD) in 2013 and the Optical Payload for Lasercomm Science (OPALS) in 2014 demonstrated in-space data transfer, and the Optical Communications and Sensor Demonstration (OCSD) demonstrated space-to-ground laser transmission in 2017 (Schauer, 2022). The Laser Communications Relay Demonstration (LCRD), "the agency's first technology demonstration of a two-way relay system," launched in 2021 aboard the Defense Department's Space Test Program Satellite-6 (Schauer, 2022). Most notably within the commercial sector, Starlink satellites use laser crosslinks to communicate with one another, but in-space laser communication is less challenging than trying to send lasers over vast distances through Earth's atmosphere (Rainbow, 2021).

Laser communications promise greater data transfer rates, greater information security, less massive hardware, and lower power inputs (Schauer, 2022). Although laser communications work without quantum technology, optical networks are needed to transfer qubits among quantum processors, and this means using lasers as the "highway system" for free space transmission (that is, the transmission of information without fiber optics) (Baird, 2021). In other words, the goal of networking multiple quantum processors across the globe, the quantum internet, will require laser communications.

ENCRYPTION

For data that needs to be secured—everything from sensitive intelligence collections to common electronic funds transfers—encryption is essential. Encryption allows a user to receive information securely from another user, know that it has not been altered in the transfer process, decrypt the information into a useful form, and keep external observers from interpreting it (Bernhardt, 2019).

One of the most common types of encryption is called Rivest-Shamir-Adleman (RSA) encryption (Buchholz & Mariani, 2020). To paraphrase the explanation from (Buchholz & Mariani, 2020), RSA encryption works in this way for a bank transaction:

- Your computer generates a key (a number called *K*)
- The bank's computer generates a large number, *N*, with at least 300 digits, which is the multiple of two prime numbers, *p,* and *q*.
- The bank's computer also generates another number, a puzzle piece that your key needs to operate, *e*.
- The bank sends you *N* and *e.* Your computer performs a calculation, creating a number called "Ke mod *N*."
- Your computer sends Ke mod *N* back to the bank. They already know *e* and *N*, so they can easily calculate your key, *K*, and access your data.
- Anyone trying to steal your data would need to be able to calculate *p* and *q*, which is exceedingly difficult for conventional computers.

These calculations are so difficult, in fact, that a "a regular computer needs billions of years to crack RSA, [but] a fast quantum computer would take just hours" (Campbell, 2023). At the beginning of the decade, this achievement was thought to be possible by 2030 using a process called Shor's algorithm (Buchholz & Mariani, 2020); Bernhardt, 2019), but a team of researchers from China in 2022 claimed to have cracked RSA using quantum methods (Campbell, 2023). Even if their claims are inflated or false, it is still currently possible to save RSA-encrypted data until such a time that it can be easily decrypted, raising significant concerns for national security, the financial industry, and the protection of proprietary information (Buchholz & Mariani, 2020); (Campbell, 2023).

Just as quantum technology can be used to decrypt information, it can also be used to encrypt information. One method of employing quantum technology in support of data security is called Quantum Key Distribution (QKD). In fact, it was QKD technology that allowed the Chinese and Austrians to communicate securely via the *Micius* satellite in 2017 (Barnhardt, 2019), but because *Micius* itself "'knew' the sequences of photons, or keys, for each location, as well as a combined key for decryption," the satellite itself was a vulnerability (Kwon, 2020). To eliminate that risk, the next step was to employ entanglement-based quantum key distribution, a technique that simultaneously sends "two strings of entangled photon pairs" to two different ground stations such that the satellite itself does not have to serve as a trusted node (Kwon, 2020).

As in the case of comparing quantum computers with traditional supercomputers, quantum encryption and traditional encryption are best viewed as complementary technologies rather than competing ones, and each should be employed in the manner that makes the most sense for a given application and to maximize the strengths of one while minimizing the weaknesses of the other. Furthermore, quantum computers—although a serious threat to traditional encryption—are unlikely to make traditional encryption obsolete. They will, however, be much more capable of cracking traditional encryption unless preventative measures are taken to make them quantum-resistant (Bernhardt, 2019). For the United States, the National Institute of Standards and Technology has the responsibility to "devise postquantum security" (Campbell, 2023), but the National Security Agency (NSA), the intelligence community entity responsibility for cryptography, has already

implemented "quantum-resistant algorithms" on "existing platforms" with the assurance that they will update their protocols as required (National Security Agency).

MEASUREMENT

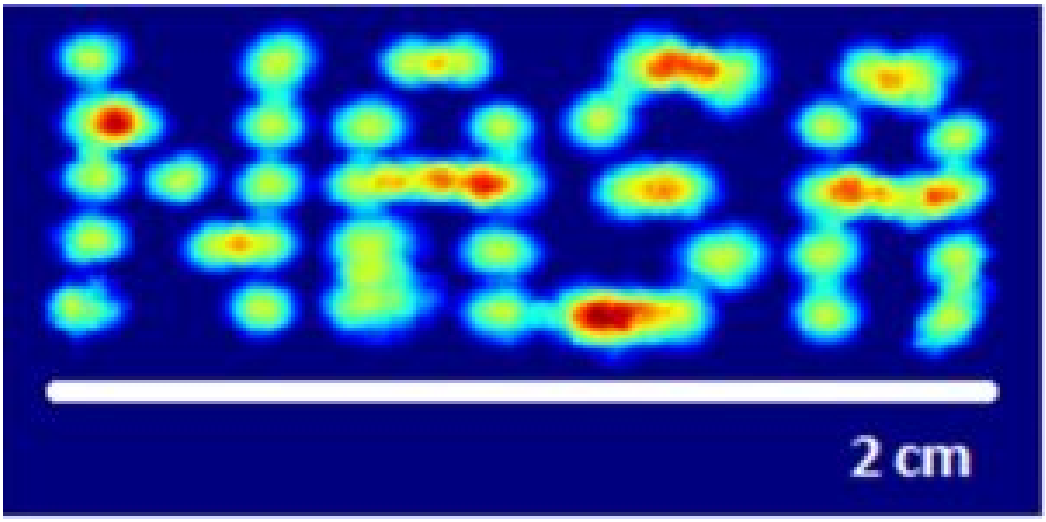
Because quantum measurement devices leverage elementary particles to perform their measurements, they promise never-before-seen levels of precision. Their potential applications are numerous, and the understanding garnered from these measurement campaigns is likely to fundamentally alter our understanding about nature and the way we approach scientific, economic, and security problems.

Foundational to this effort is the development of optical clocks to offer greater precision over traditional atomic clocks. While atomic clocks on Global Positioning System (GPS) satellites have long been the standard for global timing, quantum entanglement promises clocks that are even more precise (Merali, 2010). Recalling the PEACOQ photon detector, the need for a very precise time to register those detections becomes apparent. As in PEACOQ, individual photons are detected with time increments as precise as 100 trillionths of a second (O'Neill, "NASA's quantum detector achieves world-leading milestone." NASA Jet Propulsion Laboratory. , 2023).

In fact, the development of these "optical atomic clocks" is an essential complement to the development of other technologies that require such precise measurements. Quantum LIDAR, for example, bounces laser light off of an object, and receives back individual photons—rather than reflected pulses as in traditional LIDAR or radar (Bowler, 2019). A potential military application of this technology is the detection of stealth aircraft (Buchholz & Mariani, 2020), but it is also likely to find application in fields where traditional LIDAR has proved invaluable like archaeology, shoreline monitoring, and urban planning (American Geosciences Institute. , 2023). Additionally, quantum versions of interferometers, magnetometers, and Rydberg sensors for radio-frequency measurement are other technologies under investigation, and like quantum LIDAR and quantum radar, they allow for finer measurements than are possible with traditional technologies (Manu, 2023).

Although interferometry can be applied to many disciplines, the most intriguing applications come in the field of gravimetry. In 2018, a company called AOSense, Inc. built a gravity interferometer that is small enough to be hosted on a satellite and could be the precursor of sensors used to measure gravity waves from black holes or to "measure the interior structure of planets, moons, asteroids, and comets" (Keesey, 2018). Similar applications for Earth include using quantum gravimetry to monitor glacier and water flow as part of the study of climate change (Keesey, 2018), sensing the shift of magma within volcanoes, and surveying underground mines and tunnels prior to beginning construction projects (Bowler, 2019). Potential military applications of this technology include detection of underground bunkers, tunnel complexes, or storage facilities and even the detection of submarines underwater (Buchholz, Mariani, & Routh, 2020).

Figure 16-4: Goddard Space Flight Center and AOSense, Inc. control atoms to spell "NASA."



Source: *(O'Neill, "Space station to host 'self-healing' quantum communications tech demo." NASA Jet Propulsion Laboratory. , 2022)*

IMPLICATIONS FOR SPACE OPERATIONS

This chapter has discussed the unusual physical properties that underlie quantum technology and provided insights into the efforts to advance quantum computing, communications, encryption, and sensing. These categories are vast and are each worthy of deeper investigation. Like the products of the digital revolution before it, quantum technologies are likely to transform every aspect of society from defense to the economy. For space operations, the transformations are likely to fall into two broad categories. The first set of implications concerns applications that will help us gain new knowledge or apply new methods to our current ways of doing things. The second set of implications involves those applications that are likely to entirely supplant our current methods.

To begin once again with computing, it is anyone's guess what kind of new fuels, materials, or chemical compounds advanced quantum computers and simulations may develop for space applications. One might most obviously apply such technologies in the design and construction of satellites or in the optimization of orbits or sensor collection tasking. One might even envision a satellite with quantum computers on board to process the vast amounts of data gathered by quantum sensors or to communicate with other quantum computers on the ground. The extreme cold in space would aid the supercooling needed for quantum computers to operate, and it has been suggested that the lunar surface would provide an excellent location for the construction of quantum computers (Cannon, 2022).

Meanwhile, NASA's Laser Communications Roadmap outlines a plan to continually advance laser communications capabilities, employing them in future Artemis and deep-space missions for high-capacity video feeds and sensor data relay (Schauer, 2022). When coupled with the high-data-rate production of quantum sensors, this infrastructure will provide unprecedented amounts of information about the space environment, planets, gravity, and the Earth. It is likely that this technology will continue to expand in the commercial sector, as well, and just as there are numerous applications for commercial space-based sensing, there are likely to be remarkably similar applications for quantum sensors in those same fields.

If the data produced by these quantum devices requires encryption for transmission back to Earth, then quantum encryption may be applied to the transmission of digital data. China's *Micius* satellite has already demonstrated QKD encryption at transcontinental distances, so we should expect broader application of similar techniques to secure data transiting among satellites and ground stations (Bernhardt, 2019). Of course, data created by traditional computers can also utilize quantum encryption to enhance security, so broader applications in that area are likely, as well.

Finally, with the tremendous amount of data already collected by remote sensing satellites, quantum computers operating quantum algorithms, such as Grover's algorithm, could offer a "quadratic speedup" in data processing under certain conditions—that is, at a power of two faster than classical algorithms (Bernhardt, 2019). The vast data stores produced by the quantum LIDAR or quantum gravitational sensors of the future might require similar data processing.

The second set of implications for space operations concerns the way in which quantum technologies may supplant traditional space operations roles and functions. For the near term, all current satellite systems and missions will remain necessary, but there is a chance that quantum technologies may lead to reduced reliance on satellites in two key areas. First, because they can account for the extremely complex interaction of multiple variables over time, quantum computations promise better-than-ever modeling of complex weather patterns (Swayne, 2022). If sufficiently accurate, such models may reduce requirements for weather satellites. Similarly, quantum accelerometers may make satellite constellations like GPS, Russia's Global Navigation Satellite System (GLONASS), Europe's Galileo, or China's Beidou obsolete. There is already significant interest in this technology to enhance inertial navigation accuracy of submarines that operate out of range of GPS's radio signals and for ships that may have to operate in environments with electromagnetic interference (Papadopoulos, 2022). Indeed, the role of positioning, navigation, and timing satellites may eventually be eliminated entirely, and plans for such enhancements from the lunar surface (see, for example, NASA's Lunar GNSS Receiver Experiment (LuGRE) program) or GPS-like constellations around the Moon may prove unnecessary.

CONCLUSIONS

The evolving technologies of quantum computing, quantum communication, quantum encryption, and quantum sensing promise to affect every aspect of our lives. As discussed, these technologies operate differently

than their digital counterparts, but that does not necessarily make them incompatible with the computation, communications, encryption, and sensing methods currently in place. On the contrary, because quantum technologies operate on foundational principles of the physical world that are *more* fundamental than their digital counterparts (Bernhardt, 2019), the two can often go hand-in-hand, and it is an emerging best-practice that quantum and digital methods are made to join forces when the capabilities of one complement the limitations of the other. Such a complement occurs in the use of QKD encryption used to secure digital information.

We have further explored the utility of these technologies for space operations purposes. While NASA is a leading agency in these development efforts, industry, academia, and defense entities are also keen to exploit these technologies for their particular uses. While these representative technologies, like quantum LIDAR and gravitational measurement, have obvious reconnaissance potential for the detection of disturbed soil or submarines, they may also be applied to civil uses like the mapping of archeological sites from a distance. The technologies are thus dual-use, and it seems quite likely that we are only scratching the surface of potential applications of the technology.

Still, quantum technologies are not a panacea for all civil, military, or space operations problems. Significant challenges remain with largescale computing, the application of encryption to existing data, the protection of existing communications methods to quantum incursion, and the scaling and ruggedizing of laboratory equipment into more operationally useful packaging. Even when these challenges are overcome, it is almost certain that classical computing, communications, encryption, and sensing will continue to have their uses—sometimes even surpassing their quantum counterparts in usefulness or practicality. Whatever the future may hold for these technologies, they will constitute only a handful of the countless options in the space portfolio, but this handful of options promises to transform the technology landscape moving forward and thus demands attention from experts in all fields of application.

REFERENCES

American Geosciences Institute. . (2023). *"What is LIDAR and what is it used for?"* . Retrieved from www.americangeosciences.org/: https://www.americangeosciences.org/critical-issues/faq/what-LIDAR-and-what-it-used.

Baird, D. (. (2021, December 29). *LCRD—the Future [Audio podcast episode]. In The invisible network. NASA.* . Retrieved from www.nasa.gov/: https://www.nasa.gov/mediacast/goddard/2021/22-lcrd-the-future-nasas-the-invisible-network-podcast.

Bartman, J. (2023). *"Cutting-edge science keeps the nation's nuclear deterrent safe, secure, and effective in an era without nuclear testing." Lawrence Livermore National Laboratory.* . Retrieved from discover.lanl.gov/: https://discover.lanl.gov/publications/national-security-science/2023-sp

Bernhardt, C. (2019). *Quantum-Computing-for-Everyone.* Boston: MIT PRESS. doi:https://doi.org/10.7551/mitpress/11860.001.0001

Bova, F. G. (2021, January 7). *"Quantum computing is coming. What can it do?" Harvard Business Review.* . Retrieved from hbr.org/: https://hbr.org/2021/07/quantum-computing-is-coming-what-can-it-do.

Bowler, T. (2019). *"How quantum sensing is changing the way we see the word." British Broadcasting Corporation.* . Retrieved from www.bbc.com/: https://www.bbc.com/news/business-47294704.

Buchholz, S., & Mariani, J. &. (2020). *"The realist's guide to quantum technology and national security: What nontechnical government leaders can do today to be ready for tomorrow's quantum world," Deloitte.* Retrieved from www2.deloitte.com/: https://www2.deloitte.com/us/en/insights/industry/public-sector/the-impact-of-quantum-technology-on-national-security.html.

Campbell, C. (2023). *"Quantum computers could solve countless problems—and create a lot of new ones.".* Retrieved from time.com: https://time.com/6249784/quantum-computing-revolution/

Cannon, K. (2022). Resources of the Moon. . Golden, CO.: Recorded lecture, Colorado School of Mines, Golden, CO.

Keesey, L. (2018). *"NASA-industry team creates and demonstrates first quantum sensor for satellite gravimetry." NASA Goddard Space Flight Center.* . Retrieved from www.nasa.gov/: https://www.nasa.gov/feature/goddard/2018/nasa-industry-team-creates-and-demonstrates-first-quantum-sensor-fo

Kwon, K. (2020). *"China reaches new milestone in space-based quantum communications."* . Retrieved from www.scientificamerican.com/article/: https://www.scientificamerican.com/article/china-reaches-new-milestone-in-space-based-quantum-communications/.

Manu, S. (2023). *"Atomic quantum sensor and clocks." NASA Goddard Space Flight Center.* Retrieved from sbir.nasa.gov/: https://sbir.nasa.gov/content/atomic-quantum-sensor-and-clocks.

Math is Fun, "Binary Number Systems," . (2023). Retrieved from www.mathsisfun.com: https://www.mathsisfun.com/binary-number-system.html.

Merali, Z. (2010). *"Atomic clocks use quantum timekeeping." Scientific American.* . Retrieved from www.scientificamerican.com/: https://www.scientificamerican.com/article/atomic-clocks-use-quantum-time/.

Moss, S. (2023). *"Sunspot mini-supercomputer launched as testbed for Aurora exascale system." Data Center Dynamics.* . Retrieved from www.datacenterdynamics.com/: https://www.datacenterdynamics.com/en/news/sunspot-mini-supercomputer-launched-as-testbed-for-aurora-exascale-system/.

National Security Agency. (n.d.). *"Quantum key distribution (QKD) and quantum cryptography (QC)."* . Retrieved from www.nsa.gov/: https://www.nsa.gov/cybersecurity/quantum-key-distribution-qkd-and-quantum-cryptography-qc/

O'Neill, I. (2022). *"Space station to host 'self-healing' quantum communications tech demo." NASA Jet Propulsion Laboratory.* . Retrieved from www.nasa.gov/: https://www.nasa.gov/feature/jpl/space-station-to-host-self-healing-quantum-communications-tech-demo.

O'Neill, I. (2023). *"NASA's quantum detector achieves world-leading milestone." NASA Jet Propulsion Laboratory.* . Retrieved from www.jpl.nasa.gov/: https://www.jpl.nasa.gov/news/nasas-quantum-detector-achieves-world-leading-milestone.

Papadopoulos, L. (2022). *"Researchers invent first ever 3D quantum accelerometer for use in ships and submarines. " Interesting Engineering.* . Retrieved from interestingengineering.com/: https://interestingengineering.com/innovation/first-ever-3d-quantum-accelerometer

Rainbow, J. (2021). *"All future Starlink satellites will have laser crosslinks." SpaceNews.* . Retrieved from spacenews.com/: https://spacenews.com/all-future-starlink-satellites-will-have-laser-crosslinks/.

Remmel, A. (2022). *"What exascale computing could mean for chemistry." Computational Chemistry 100 (31).* . Retrieved from cen.acs.org/: https://cen.acs.org/physical-chemistry/computational-chemistry/exascale-computing-mean-chemistry/100/i31.

Savage, N. (2019). *"Hands-on with Google's quantum computer." Scientific American. https://www.scientificamerican.com/article/hands-on-with-googles-quantum-computer/.* . Retrieved from Scientific American. https://www.scientificamerican.com/: https://www.scientificamerican.com/article/hands-on-with-googles-quantum-computer/

Schauer, K. (2022). *"NASA laser communications innovations: A timeline." NASA Goddard Space Flight Center.* Retrieved from www.nasa.gov/: https://www.nasa.gov/feature/goddard/2021/nasa-laser-communications-innovations-a-timeline.

Swayne, M. (2022). *"BASF, PASQAL to use quantum computers for weather prediction." The Quantum Insider.* . Retrieved from thequantuminsider.com/: https://thequantuminsider.com/2022/07/20/basf-pasqal-to-use-quantum-computers-for-weather-prediction/.

Tavares, F. (2019). *"Google and NASA achieve quantum supremacy." NASA Ames Research Center.* . Retrieved from www.nasa.gov/: https://www.nasa.gov/feature/ames/quantum-supremacy.

Van Amerongen, M. (2021, June 03). *NATO Review: Opinion, Analysis and Debate on Security Issues: quantum-technologies-in-defence-security.* Retrieved from https://www.nato.int/: https://www.nato.int/docu/review/articles/2021/06/03/quantum-technologies-in-defence-security/index.html.

17.

WIRELESS POWER FOR SPACE APPLICATIONS [KHAN]

EXECUTIVE SUMMARY

Nearfield wireless power transfer (WPT) systems can benefit satellites having either standard or functional-modular architecture because of their high efficiency when compared to a laser or microwave system. A practicable wireless power transfer (WPT) system needs to maintain high transfer efficiencies while containing electric and magnetic near fields for wireless satellite power applications. Nodes that do not have shielding can become susceptible to electromagnetic interference (EMI) both as a source and as a receiver. One way to deal with this problem is to mitigate lateral emission in the unprotected zone between transmitter and receiver. Early results show chiral ordering of a 4-tier WPT system can limit the unprotected lateral emissions by beam shaping in the zone between transmitter and receiver during the charging process.

Keywords— Helical antennas, parasitic elements, wireless power transfer (WPT), near field, chirality, frequency selective surfaces (FSS), satellite systems

INTRODUCTION

WPT systems can bring certain advantages to satellite systems having different architectures. Satellite wireless buses help reduce cabling weight. To reduce EMI interference, while maintaining efficient power transfer in a crowded field of electronic devices, one needs the near field shaping capability discussed here. The chapter begins with a general discussion of WPT options and moves quickly on to the design and research conducted of a system capable of beam shaping while maintaining high efficiency.

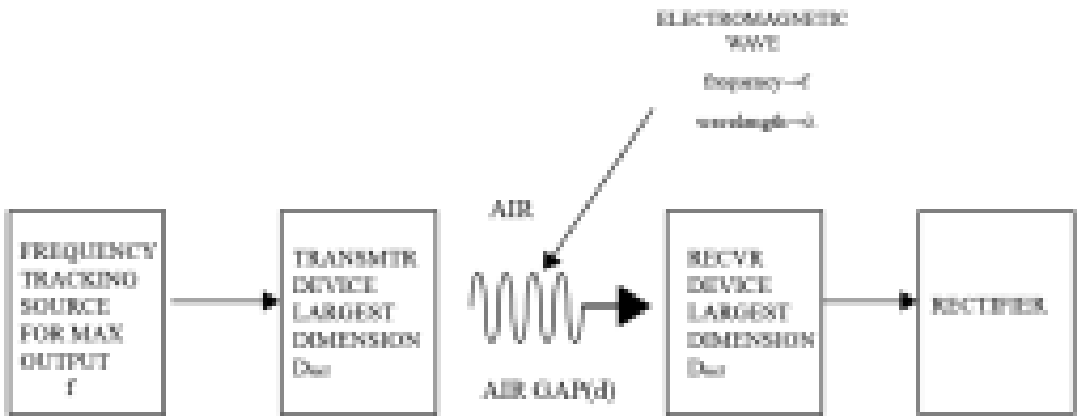
BASICS OF WPT SYSTEMS

WPT systems can be classified as near-field, mid-range, or far-field based on coupling distance (Triviño-Cabrera et al., 2020). In near-field operation can be inductive or capacitive. Inductive systems can be further broken down into magnetic resonant or non-resonant. In mid-range operation WPT systems use strongly coupled magnetic resonant system (SCMR) which is similar to the resonant inductive systems but has greater range

generally achieved by adding parasitic components to the coupling system. Far-field systems such as optical and microwave systems have low efficiencies and require a larger payload volume and are therefore not suitable for satellite deployment (Zhang et al., 2019). Our chosen application lies between magnetic resonant and SCMR systems Table 17-1 compares these two technologies based on frequency of operation (f), wavelength(λ), and largest dimension of coupling device (DMAX≈d).

Table 17-1 Comparison Magnetic Resonance and SCMR Systems

Table 17-1 Comparison Magnetic Resonance and SCMR Systems



Basic WPT System (source Author)

Technology	Operation	D_{MAX}	Air Gap (d)	Size	Coupling
Magnetic Resonance	Near-field $< 0.62\sqrt{\frac{D_{max}^3}{\lambda}}$	< d	< D_{MAX}	$D_{MAX} << \lambda$	Magnetic Field
SCMR	Mid-range $< 2\frac{D^2}{\lambda}$	> d	1 < d < 10*D_{MAX}	$D_{MAX} << \lambda$	

MOTIVATION

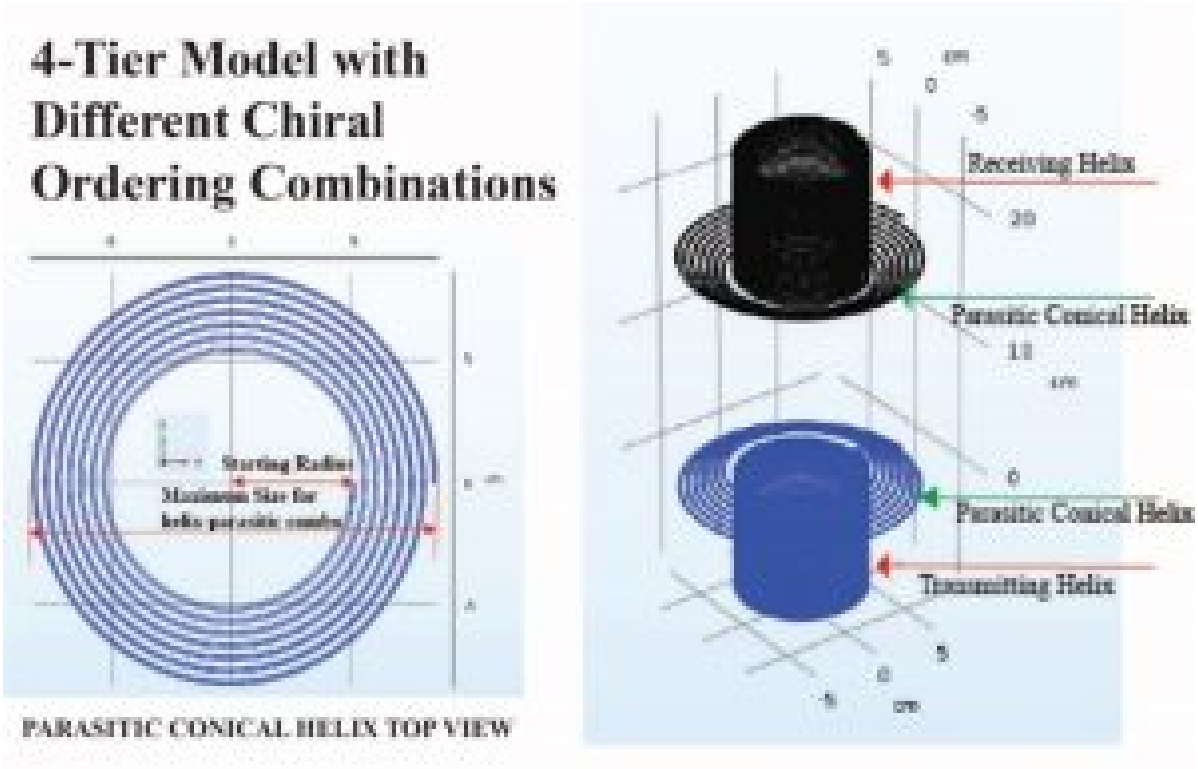
Depending on the architecture of the satellite system(s) WPT technologies can provide better immunity to EMI and reduced weight from not using cabling. In a traditional architecture it can be used to transfer power from solar panels to a receiver while in a modular spacecraft WPT can be used to provide power between the modules. Our designed system has the ability to shape near fields which is critical to avoiding EMI interference in satellites and can help reduce losses.

NEAR FIELD SHAPING

The primary goal of this research has been to limit near-field emissions for an efficient resonant WPT system (Karalis et al., 2008; Kurs et al., 2007) i.e. to *optimize transfer efficiency* while keeping *human safety in mind*. More specifically, our paper would like to further expand on early results that show, chiral ordering of a 4-tier WPT system can limit the unprotected lateral emissions in the zone between transmitter and receiver (Khan, Saeed & Bailey, Chad, 2021).

The 4-tier system (Figure 17-1) is composed of chiral objects that are right-hand (RH) or left-hand (LH). Both the helical transmitter and receiver can be considered to be chiral metaparticles (Caloz & Sihvola, 2020), i.e. it has a length close to half a wavelength and a height that is much smaller than its length. The parasitic elements are RH or LH chiral objects but do not necessarily meet the length requirements for metaparticles. With sixteen possible arrangements are possible, the research will focus on two arrangements holding the most promise from the perspective of field containment and efficiency. We assume that shielding (Wang, Zuming & et. al., 2021) can be employed in other zones that do not impede the path of direct energy transfer which is further clarified in the section on background.

Figure 17-1 4-Tier WPT system where the chirality of helices and parasitic elements are ordered in different combinations of right-hand and left-hand chirality



Source: Author

EARLY RESULTS

Table 17-2 shows impact on field containment happening in the unprotected area between transmitter and receiver (*Note: RRRR indicates for four-tier system components are all right-handed; RLLR indicates only parasitic elements are left-handed*). Figure 17-3 shows field closer view of a system where all tiers are right-hand. Also, efficiencies of the WPT system depend on the- chirality (right/left hand) order of the system (Table 17-2). Proper ordering can lead to 70-80+% measured efficiencies for distances of 5-20 cm. Higher efficiencies (90%+) have been recorded through COMSOL simulations without accounting for measurement setup losses. Resonant frequencies of the system have also been shown to depend on the chirality order of the four-tier system. Frequency tracking capability is assumed (Chaidee et al., 2017; Liu et al., 2018; Nam Yoon Kim et al., 2012).

The paper describes the work of a four-tier (transmitter-parasitic element-parasitic element-receiver) resonant WPT system consisting of two helical antennas each with a conical helix serving as a parasitic element. It focuses on E-field and H-field containment at high efficiencies through simulation and experimental work. Based on the novel work (Khan, Saeed & Bailey, Chad, 2021) performed, there is a good possibility this investigation will lead to a safe and efficient near-field transfer systems.

BACKGROUND

The successful design of a system that can safely transfer 100 kW or more of power over a 100-200 mm gap under varying conditions of humidity, while maintaining high efficiencies, is a challenge for any person or team. Effective implementation of the above specifications will be rewarded with a resonant (Kurs et al., 2007; Barman et al., 2015) wireless power transfer system (WPT) that can support the charging of devices such as electric vehicles (EIVs), drones (UAVs), and robots (UGVs) comfortably, even with the current state of storage technology. In addition, a good wireless charger (Ahmad et al., 2018; Chittoor et al., 2021) is expected to enable interoperability with a large tolerance for misalignment while meeting safety requirements.

The basic structure of the proposed system (Figure 17-1) consists of a center-fed transmitting normal mode helical antenna (NMHA) and an identical receiving NMHA helix loaded at the center (Imura et al., 2009). Multiturn-helical antennas form efficient WPT systems (Barman et al., 2015; Imura et al., 2009) and while NMHA mode requires the helix to be electrically small in height the overall length, using multiple turns, it can be made to be about half a wavelength to qualify as a chiral metaparticle (Caloz & Sihvola, 2020). The parasitic elements are conical helices which are at their minimum radius flush with the side facing the transfer gap.

The use of parasitic elements in the structure is supported partially supported by the work by Andre Kurs *et al* (Kurs et al., 2007) where efficient indirect WPT was reported between self-resonant transmitter and receiver coils by way of using a feeder loop and loaded receiver loop. In another case, work done by K. Firdaus *et al* shows (Firdaus et al., 2015) that a spiral slot with length comparable to half a wavelength has good transmission

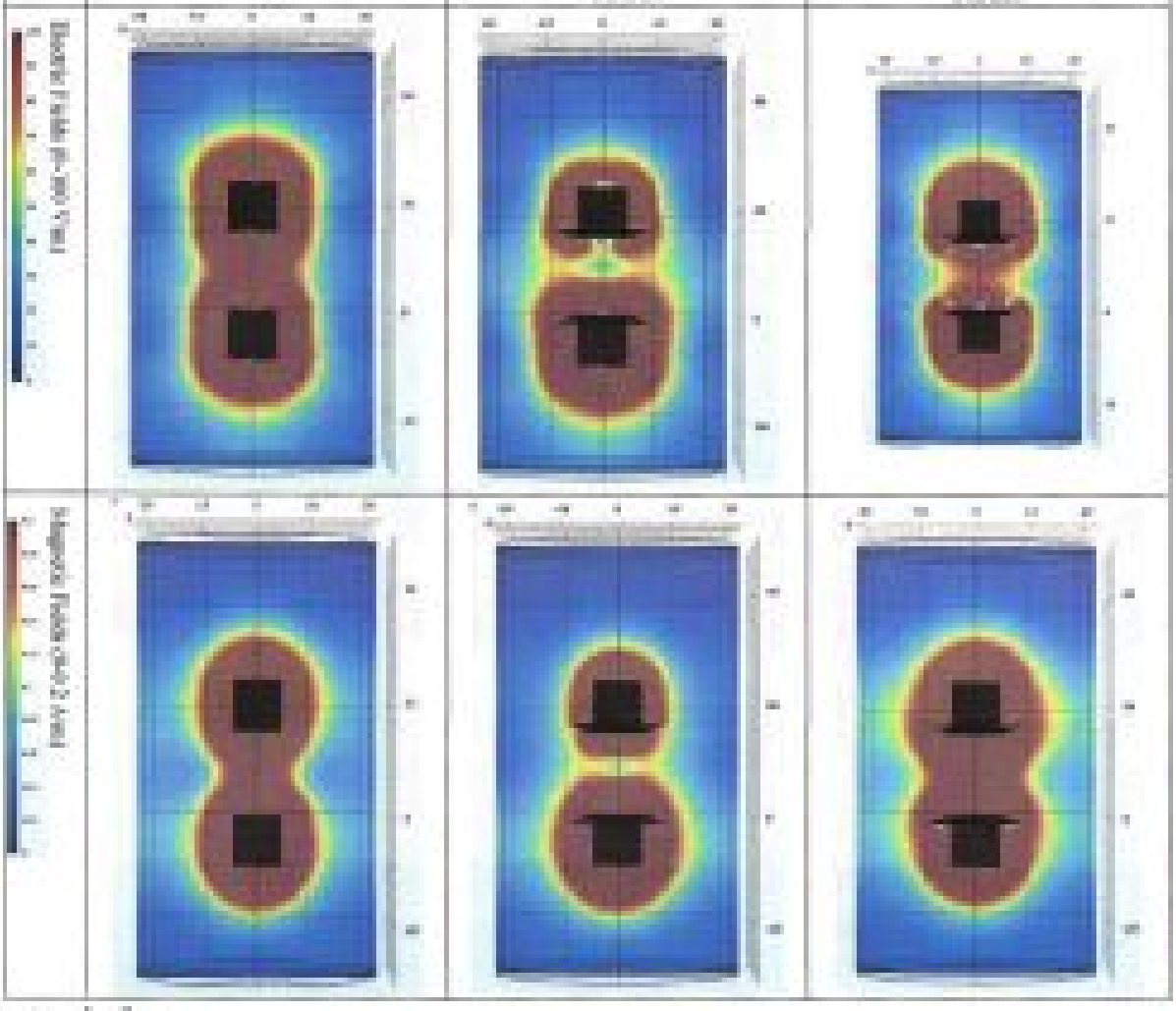
characteristics when placed between two identical right-handed helical antennas in a WPT system where the transmitting helix and receiving helix are equidistant from the slot. The choice of 3-D chiral metaparticles as parasitic elements seems to be the next step from placing planar objects between receiving and transmitting helices, which have demonstrated a positive impact on coupling. Indeed, the parasitic elements in our design are 3-D version of an achiral Archimedean spiral forming a chiral conical helix.

ANALYSIS OF PRELIMINARY RESULTS

Of the total sixteen possible 4-tier chirality orders eight can be considered to be equivalent to the other eight e.g., RLLR is the chiral equivalent of LRRL. Measurements and simulations were run on eight structures of which two (RRRR & RLLR) were found promising in terms of their efficiency (Figure 17-4). *Note: Both measurements and simulation results account for cable and connector losses. Comparing measured (with PVC cylinder for alignment) and simulated (without PVC cylinder) has a mean efficiency difference of 5%.*

Table 17-2 -FIX shows impact on field containment happening in the unprotected area between transmitter and receiver (*Note: RRRR indicates for four-tier system components are all right-handed; RLLR indicates only parasitic elements are left-handed*).

TABLE 17-2
ELECTRIC AND MAGNETIC FIELD PATTERNS
OF NEAR-FIELD

	Transmitter-Receiver Order (R for right-hand and L for left-hand) RR	Transmitter-Parasitic-Parasitic-Receiver Order (R for right-hand and L for left-hand) RRRR	Transmitter-Parasitic-Parasitic-Receiver Order (R for right-hand and L for left-hand) RLLR
			

Source: Author

Source: Author

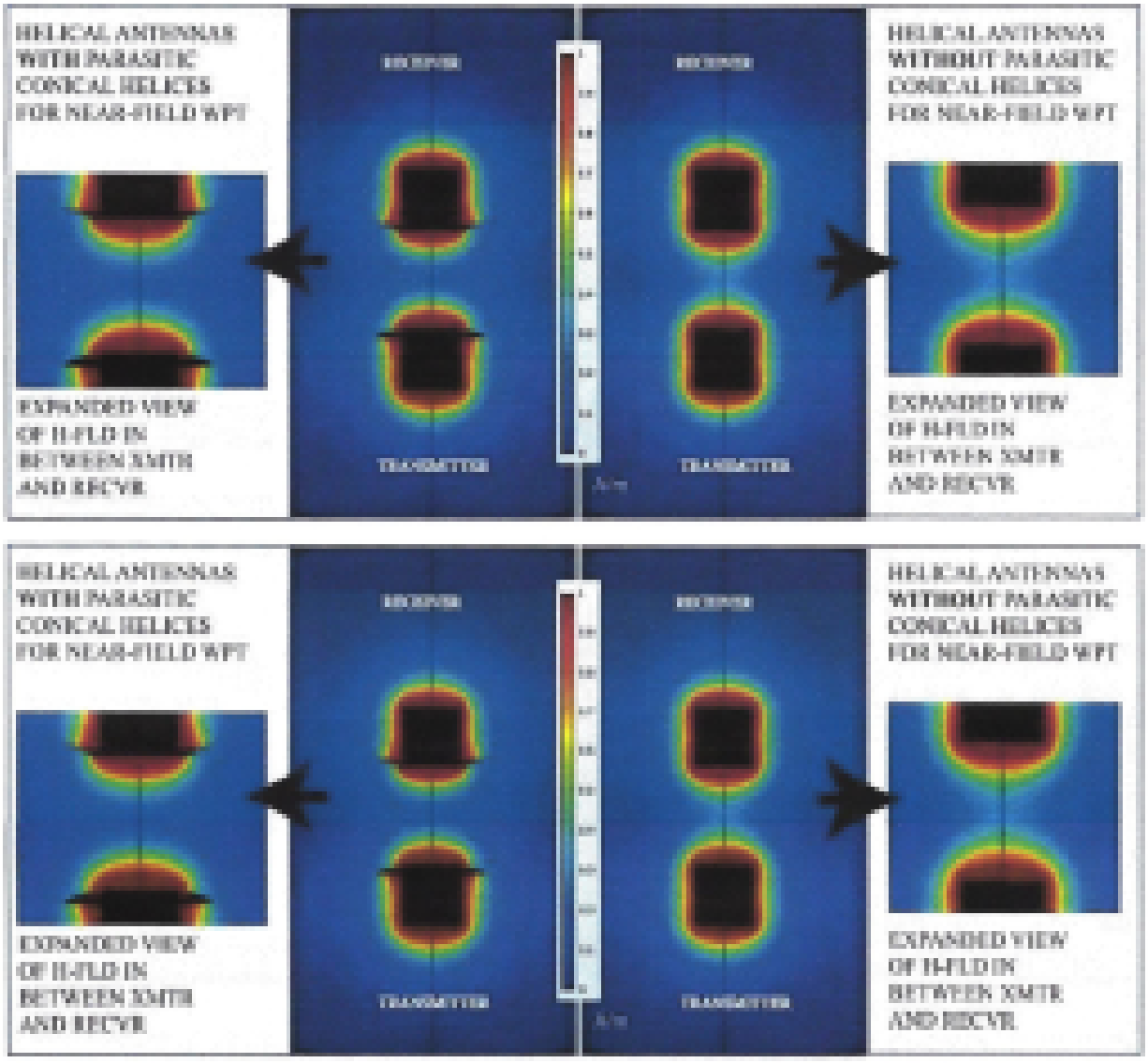
These structures were also examined for their ability to control lateral emissions in the unprotected zone. Simulation results from Table 1 compares two different 4-tier WPT chiral arrangements with a 2-tier one that

does not employ parasitic elements. From inspection, both RRRR and RLLR ordered systems provide better electric field containment in the unprotected zone when compared to a system operating without parasitic elements (RR). The RRRR order provides the best containment for the magnetic field. Figure 17-2 provides a closer look at both the E-field and H-field containment by the RRRR arrangement.

Figure 17-2 H-Field and E-Field near field studies

.Figure 17-2 provides a closer look at both the E-field and H-field containment by the RRRR arrangement.

Figure 17-2 H-field and E-field near-field studies with and w/o parasitic elements 90+% efficiency at 16.8 MHz with a gap of 20 cm (all four tiers right hand, RRR). Cable and connector losses ignored

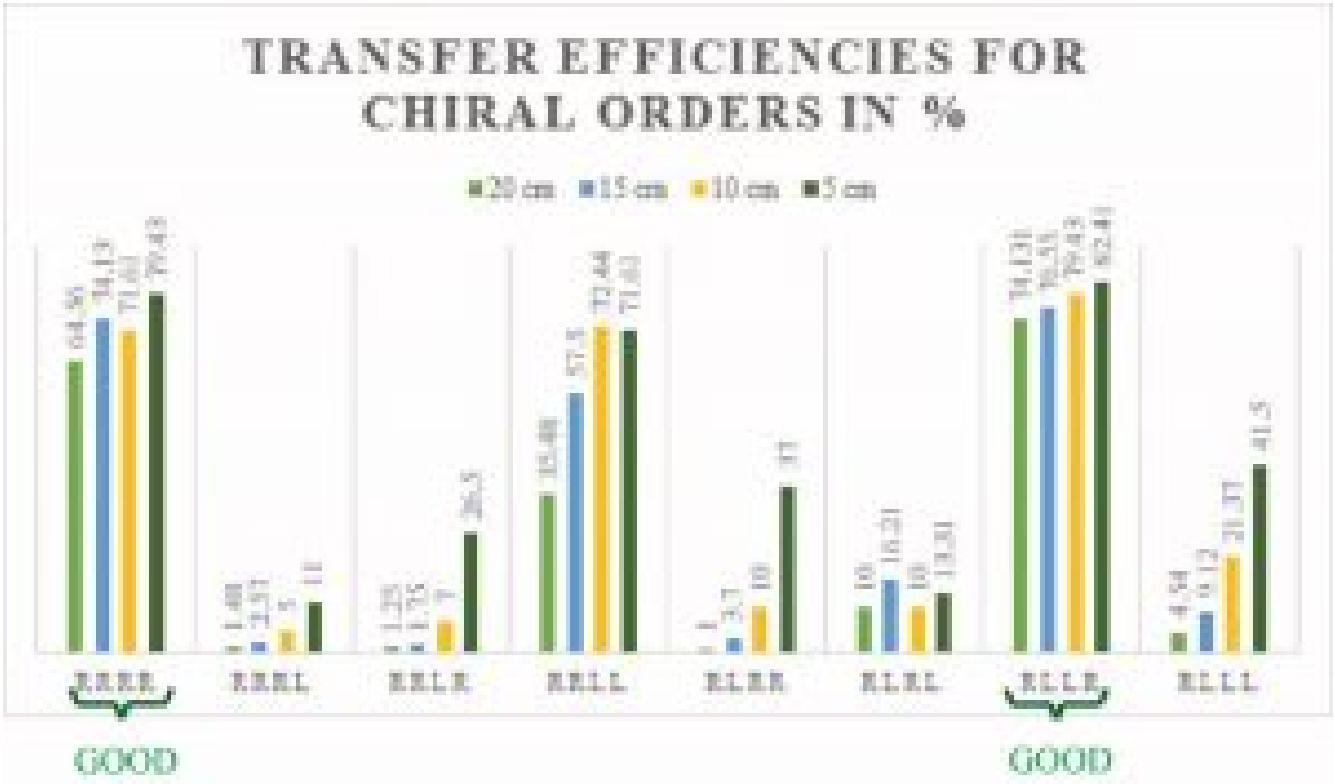


Source: Author

Source: Author

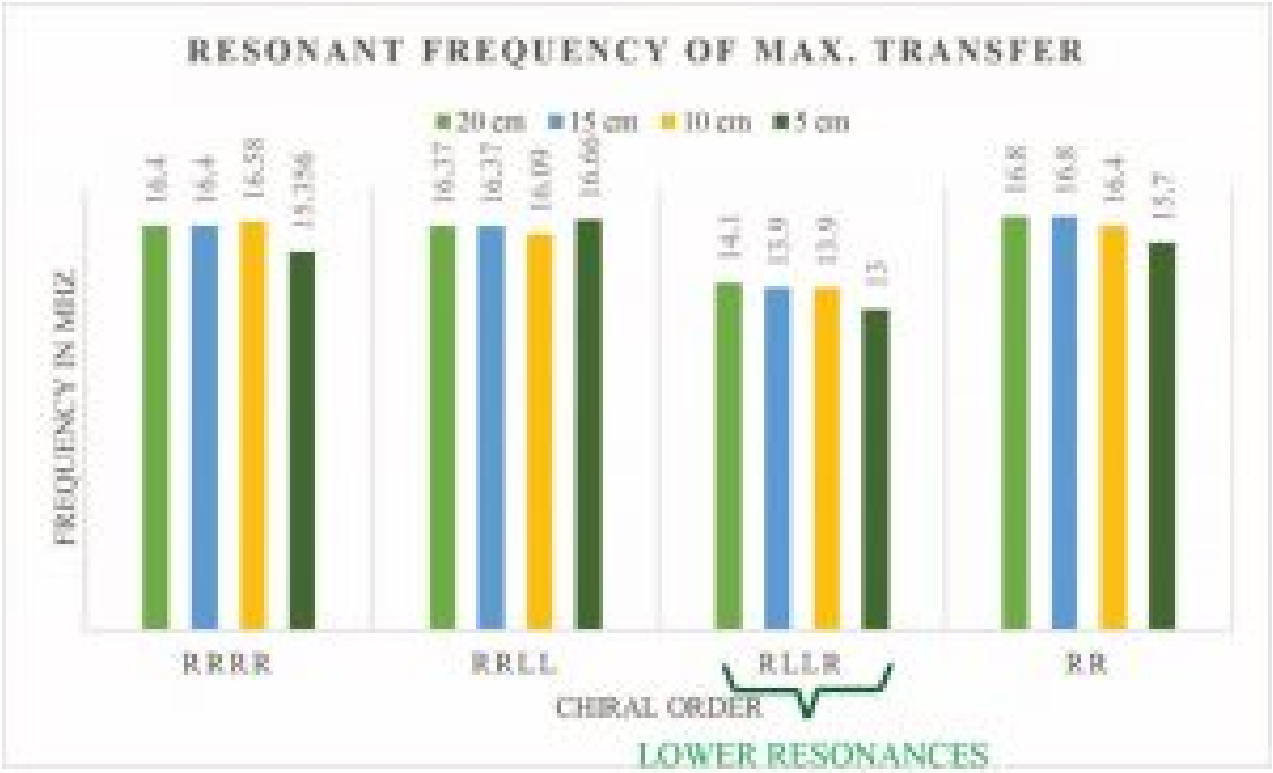
Table 17-3 summarizes and compares RRRR and RLLR systems with a 2-tier RR system from observations made from Table 17-2 and Figures 17-3 and 17-4. Table 17-3 also provides us with a possible task list that could lead to better understanding of the difference in efficiencies, field-containment, and resonant frequencies (Figure 17-5), that occur for chiral ordering of the WPT systems.

Figure 17-3 Transfer Efficiencies in % for different 4-Tier Arrangements. Best results are indicated for RRRR and RLLR arrangements



Source: Author

Figure 17-4 Resonances for different chiral orders



Source: Author

Table 17-3 summarizes and compares RRRR and RLLR systems with a 2-tier RR system from observations

TABLE 17-3
Summary of Preliminary Work
(Comparison of RRRR, RLLR, and RR)

Chiral Order	Efficiency 5-20 cm Range *Tables 17-2 & Fig. 17-4*	E-field Containment in unprotected zone *Table 17-1 & Fig. 17-3*	H-field Containment in unprotected zone *Table 17-1 & Fig. 17-3*	Resonant Frequency *Table 17-2*
RRRR 4-Tier	60-80 %	Provides similar protection	Best Containment	Generally Higher than RLLR but lower than RR
RLLR 4-Tier	70-80+%		Less Containment	Generally lower than RRRR
RR 2-Tier	50-80+%	Less Containment		Generally higher than RRRR

Source: Author

Table 17-3 summarizes and compares RRRR and RLLR systems with a 2-tier RR system from observations made from Tables 17-1 & 17-2 and Figures 17-3 and 17-4. Table 17-3 also provides us with a possible task list that could lead to better understanding of the difference in efficiencies, field-containment, and resonant frequencies (Figure 17-5), that occur for chiral ordering of the WPT systems.

EXPERIMENTAL METHODS

Measurement of Efficiency and Unprotected Fields:

- 1 Introduction: WPT efficiency measurement has so far been conducted using a network analyzer using S-parameters and compared with simulation data while the study field emissions in the unprotected zone has been performed only through simulation. The purpose of this task is to design a Faraday cage experiment that measures both transfer efficiency and emissions in the unprotected zone for small amounts of power.

- 2 Measurement Setup Design: Figure 17-5 shows schematic for how both efficiency and unprotected zone emissions are to be measured (Chakarothai et al., 2018). The design has been adapted from previous instrumentation (Figure 8) setup for measuring near-field transfer efficiencies for helical antennas (Khan & Maresch, 2013a) and includes the ability to measure lateral emissions.
- 2.1 Measurement of Efficiency: The switch (Figure 17-5) should be connected to the power management system and a rectifier circuit while trying to find the efficiency of the WPT system. The following assumptions can be made during the process,

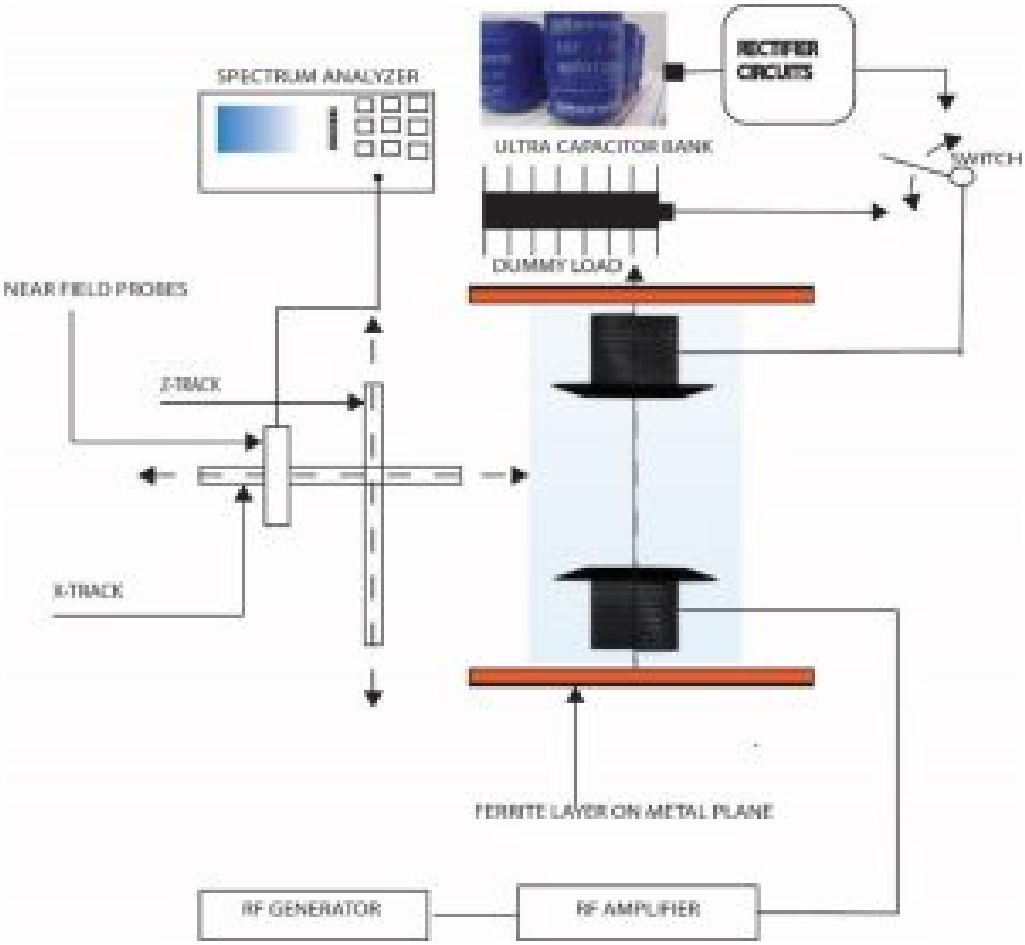
1. The placement of the ferrite sheets does not significantly impact efficiency. Simulations run with and without this metal backed sheets seem to back up this assumption.
2. The matching circuits of the rectifier system can be fine-tuned to the frequency of maximum transfer.

- The amount of transfer time is chosen such that the charging does not exceed the storage capacity of the ultracapacitor bank.

Like most modern battery chemistries, ultracapacitors require balancing if placed in series. This prevents the overcharging of one or more individual capacitors in a series string, which would cause a failure due to the breakdown of the dielectric material. Balancing, therefore, adds extra circuitry, and with-it inefficiencies, which could be avoided if the capacitors were placed in parallel. For this reason, and since capacitors add when in

parallel, the prototype initially used a bank of parallel capacitors in series with a battery. Previous testing resulted in longer than expected charging times. This was due to the RC time constant, as the DC resistance of the circuit significantly contributes. Future designs will use series capacitors with balancing circuitry, or some series/parallel combination.

Figure 17-5 Proposed Measurement Setup For Measuring WPT Efficiency And Lateral Emissions



Source: Author

- 2.2 Measurement of Near-Fields: For this measurement the switch should be connected to the dummy load with about 200 W dissipation capability. The following points can be made for this measurement:

1. The x-track (Figure 17-5) H-field and E-field measurements are going to be made adjacent to the WPT system in a horizontal line midway between receiving and transmitting antenna. Based on simulation results the fields should die off rapidly in this zone.

2. The z-track field measurement will also take place in a vertical line adjacent to the WPT system.

- Both electric and magnetic probes can be adjusted for x, y, and z, field measurements.

Figure 17-6 Previously used instrumentation for efficiency measurement. Clockwise from left, adjustable stand, transmitter cart, receiving antenna. An adjustable height test stand supports a breadboarded power management circuit and a receiving antenna, suspending it above a transmitter cart/antenna at set distances

Source: Author

- 2.3 Expected Outcomes:

1. Characterization of coupling efficiency measurements using low power source (up to 13 dBm) for separation distances of 5-20 cm using network analyzer.
2. Characterization of coupling efficiency measurements using higher power source (50-100 W) for separation distances of 5-20 cm inside Faraday cage.

- E-field and H-field measurements in an XZ plane close and adjacent to the WPT systems for different power levels.

From the list above items I-II will enable us to judge the impact on efficiency with/without a rectifier and power management system included. Item III will characterize the field penetration in the unprotected zone.

- 3 Potential Problems and Alternative Approaches: The expected outcomes (I & II) which relate to efficiency measurements are unlikely to run into problems given prior experience in the required setups. While the design for near field measurements (outcome III) will certainly require careful planning and proper orientation of both electric and magnetic probes, the data is being gathered in a zone adjacent to the WPT system that is unlikely to impact power transfer. While some re-design may be needed for field measurements the results should be corroborated by simulation.

2 Study of Field Containment and Chiral Ordering:

2.1 Introduction: The importance of field containment has been discussed in prior sections. This task can focus on understanding the phenomenon by which parasitic conical helices are able to minimize field penetration in the unprotected zone which is defined as the lateral shielded zone between transmitter and receiver.

- 2 Study of Simulated and Measured Data: The data gathered in Task 1 will be critical in establishing the field containment patterns from simulation by making experimental measurements. Relationships between field penetration, coupling distance and the frequency of maximum coupling are to be analyzed in this study. Initial studies conducted already indicate that the resonant frequency is lowered by 4-tier RLLR systems when compared to RRRR arrangements and 2-tier RR systems (Table. 3) and leads to the following questions,

1. Why is there a difference in resonant frequency between RLLR and RRRR systems that have the same size?
2. Is it possible that the parasitic elements in RLLR couple more strongly with the active elements than in the RRRR case as the lowering of resonant frequency might suggest?

- What explains the better magnetic field containment in the RRRR case when compared with the RLLR case (as indicated by simulation results in Table. 1)?

1. Why do both RRRR and RLLR have similar containment for the electric field?
2. What role does chirality order play in questions I-IV?

The answers to questions I-V will help develop an understanding of the mechanism of field containment using WPT systems using chiral ordering leading to a more efficient and safe design.

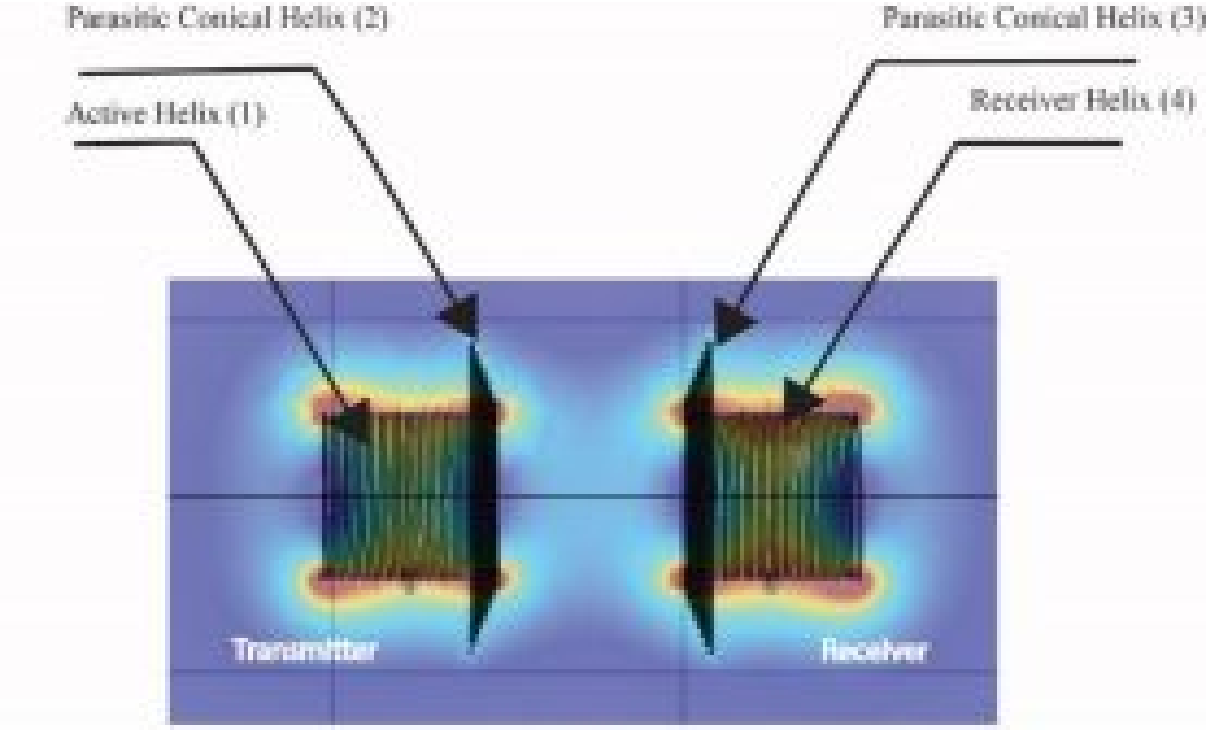
- 3 Study of Semi-analytical Approach: The approach taken thus far has relied on experimental measurements and simulation results, another approach might be to take a semi-analytical route. More specifically, explain the reason for differences in resonant frequency by studying coupling between the antenna and its parasitic element on the receiver side (I-II sec 2.2). Work done in calculating the mutual impedance of a dipole and a parasitic element suggests the proposed approach.

Questions I-III from the previous section can be better understood by calculating mutual impedance between the transmitting dipole and the near parasitic element. The higher resonant frequencies imply less coupling in the RRRR case and is a likely cause of narrower beam, but this can be investigated further by calculating the mutual impedance of a dipole and a parasitic element suggests a semi-analytical approach can be useful in this process.

Using a similar process (Visser & Lulu Chan, 2014) for near field WPT employing parasitic elements and an active receiver and transmitter dipole for our design. It is possible to calculate the impedances Z11, Z12, Z13, and Z14, by using 4 different values of ZL using simulation to provide for I1, I2, I3, and I4 for each of the load impedances (Figure 17-7). The currents can be determined by simulation results using (using 4Nec2) and then the results can be verified by experimental means using accessible ports. It is expected that the value of Z12 will provide clarity to beam shaping and resonant frequency differences discussed earlier for RRRR and RLLR. Experimental results conducted thus far seems to indicate lower levels of coupling between the transmitter and its nearest parasitic element (Z12) from relatively higher resonant frequency in RRRR case.

Some initial results using the semi-analytical is provided below (Figure 17-8-9) using the technique described in the previous section. These results indicate that RLLR (ZM= 6951Ω) is more strongly coupled than the RRRR (ZM= 5619 Ω) 4-Tier structure at no load condition and possesses a lower resonant frequency and the receiver voltage (V1) is higher assuming Z11=Z22 for the identical antennas. This approach needs to be further examined using a loaded condition.

Figure 17-7 Relationship Between Self-Impedance, Mutual Impedances, Load Impedance, Currents, And Applied Voltage



$$V_{IN_{LOAD}} = Z_{11} \cdot I_1 + Z_{12} \cdot I_2 + Z_{13} \cdot I_3 + Z_L \cdot I_4$$

I_1, I_2, I_3, I_4 are the currents for elements 1 to 4, where 1 is the transmitter, 4 is the receiver, 2 is the parasitic element closest to 1, and 3 is the parasitic element closest to 4.

$V_{IN_{LOAD}}$ is the input voltage

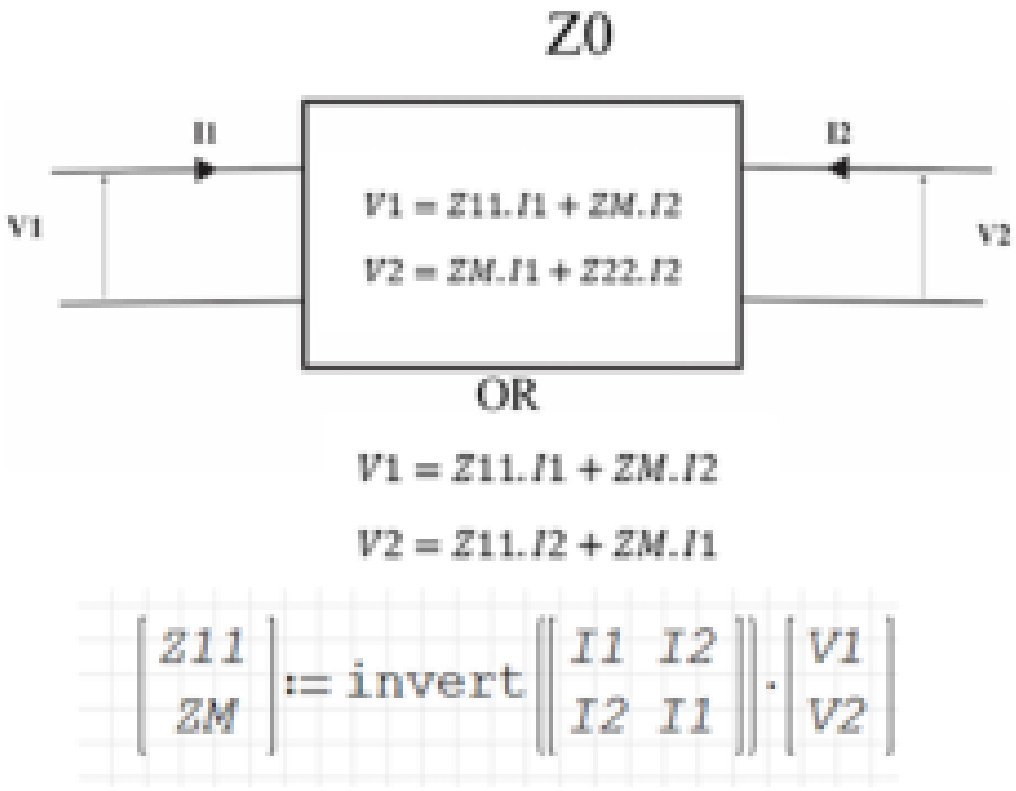
Z_{1n} are the mutual impedance between active element 1 and $n = 2, 3, 4$

Z_L is the load impedance

Z_{11} is the self impedance of 1

Source: Author

Figure 17-8 Equations For Finding Coupling Using Simulated Or Measured Results



Source: Author

Figure 17-9 Mutual Inductance Calculated With Semi-Analytical Approach

Max Transfer Frequency in MHz	Gap Size cm	Chiral Order	Mutual Impedance Ohms	Mutual Inductance μH
17.1	15	RRRR	0.1262+ j 56.2469	52.3
15.1	15	RLLR	0.3883+ j 69.5132	73.267

Source: Author

- 4 Expected Outcomes: A better understanding of these important questions (sec. 2.2) will help design safe and efficient near field WPT systems i.e., a better understanding of chiral layering in near field coupling and how this 4-tiered systems impacts field containment and resonant frequencies.
- 5 Potential Problems and Alternative Approaches: Measurements added by Task 1 will enhance our understanding of the questions posed in section 2.2. The approach takes a deeper dive into these questions from section 2.3 in and the calculation of mutual impedance between transmitting dipole and its parasitic element using similar technique used for dipoles (Visser & Lulu Chan, 2014).

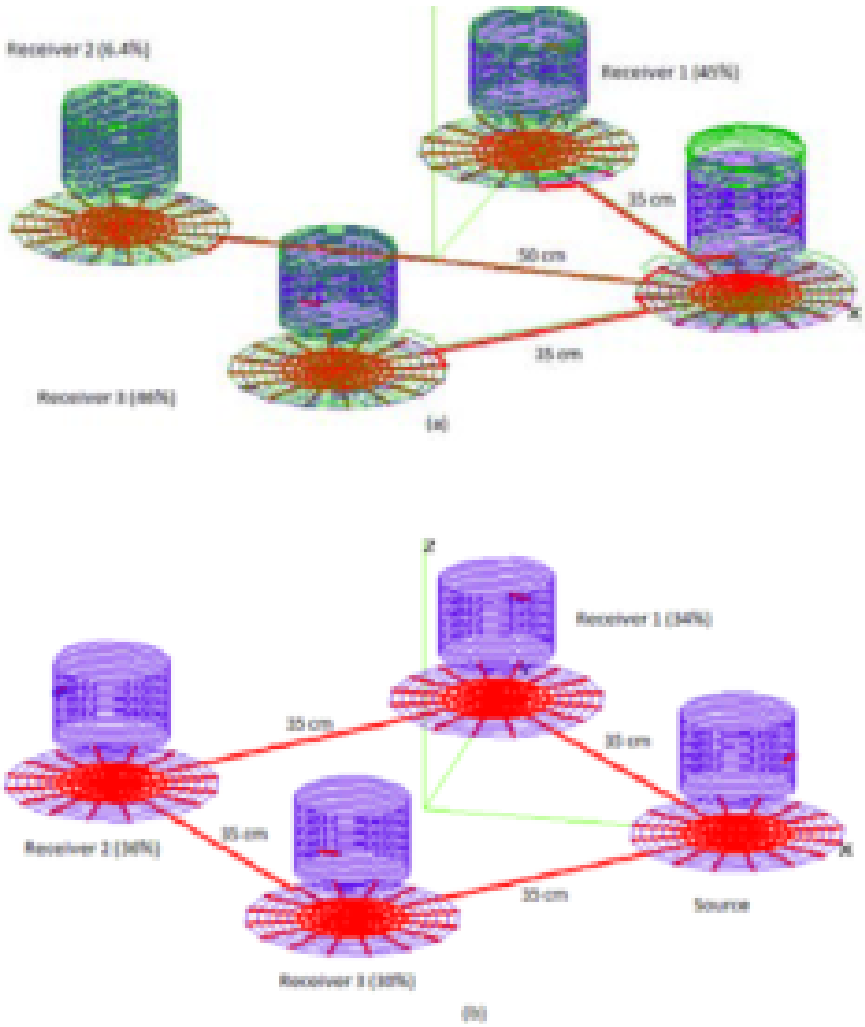
FUTURE WORK

A past research endeavor (Khan, 2017, 2019; Khan & Maresch, 2013b) regarding resonators connected to the same ground plane (Saeed Khan et. al., 2018) indicates the possibility that multiple devices can share wireless power from the same receiver without rectification at the transfer frequency (Figure 17-10). This will allow the advantage of using different power management systems within the payload i.e. if power can be transferred from one receiver to several others without the need for rectification and DC conversion.

Between the two configurations of single source multi-receiver architecture (Figure 17-10) the coupling between the source and any receiver is seen to depend on the distance and is proportional to as would be expected in the near field region of a radiator.

A point of interest is in the connecting wires between ground planes. As seen in Figure 17-11 the thin connecting wires behave as a single wire WPT line where the magnetic field seems to be contained. Also, these wires are less likely to get impacted by EMI when exposed to impinging electrons and ions on the satellites in orbit.

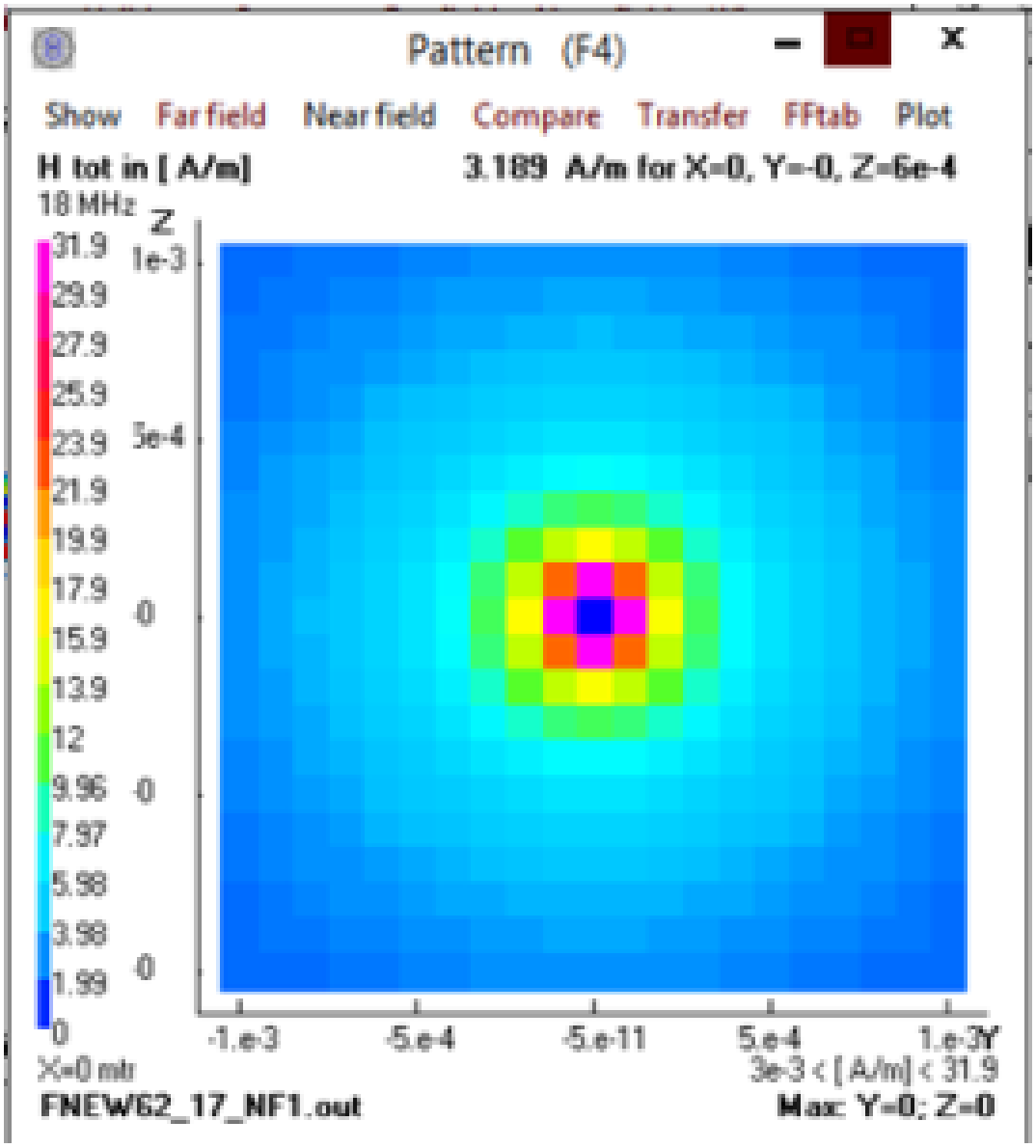
Figure 17-10 From a single WPT receiver Nec4 simulation shows system (a) and (b) are operating at almost 100% efficiency. All receivers are within the same near-field zone of the source



Source: Author

Another future research objective is to study the impact of using frequency selective (Bresciani et al., 1992; Kuse et al., 2015; Luo et al., 2015; Mandal et al., 2020; Marhefka et al., 2007; Xing et al., 2020) surfaces (FSS) as ground connectors specially designed to immunize against unwanted frequencies for an orbiting space vehicle.

Figure 17-11 Magnetic Field Containment Within Connecting Wire



Source: Author

SUMMARY

It has been shown that WPT with beam shaping can deliver EMI immunity and beam shaping with our design. We began by describing how parasitic elements can help achieve high efficiencies and beam containment by proper layering based on chirality of a 4-tier system using both measured results and simulations. A semi-analytical approach was then used to gage the impact of parasitic components both from the resonant frequency and mutual coupling point of view.

We discussed the WPT systems that deploy connected ground planes in a single source multi-receiver system.

The simulation (Figure 17-10) demonstrates that configuration is also a near-field technique since the coupled power to loads vary as 1/(distance)3 which agrees antenna theory. The application of this system can be used to transfer power throughout the entire satellite and therefore a good target for future work. Some of the research can be focused on ground plane connections using frequency selective surfaces (FSS).

ACKNOWLEDGEMENT

The author wishes to thank Chad Bailey, Instructor for the Electronic and Computer Engineering Technology (ECET) program Kansas State University Aerospace and Technology campus for his help with instrumentation, and measurement related to this work.

REFERENCES

Ahmad, A., Alam, M. S., & Chabaan, R. (2018). A Comprehensive Review of Wireless Charging Technologies for Electric Vehicles. *IEEE Transactions on Transportation Electrification*, *4*(1), 38–63. https://doi.org/10.1109/TTE.2017.2771619

Barman, S. D., Reza, A. W., Kumar, N., Karim, Md. E., & Munir, A. B. (2015). Wireless powering by magnetic resonant coupling: Recent trends in wireless power transfer system and its applications. *Renewable and Sustainable Energy Reviews*, *51*, 1525–1552. https://doi.org/10.1016/j.rser.2015.07.031

Bresciani, D., Cosentino, S., & Mantica, P. G. (1992). Inductive FSS for ground station applications. *IEEE Antennas and Propagation Society International Symposium 1992 Digest*, 1787–1790 vol.4. https://doi.org/10.1109/APS.1992.221503

Caloz, C., & Sihvola, A. (2020). Electromagnetic Chirality, Part 1: The Microscopic Perspective [Electromagnetic Perspectives]. *IEEE Antennas and Propagation Magazine*, *62*(1), 58–71. https://doi.org/10.1109/MAP.2019.2955698

Chaidee, E., Sangswang, A., Naetiladdanon, S., & Mujjalinvimut, E. (2017). Maximum output power tracking for wireless power transfer system using impedance tuning. *IECON 2017 – 43rd Annual Conference of the IEEE Industrial Electronics Society*, 6961–6966. https://doi.org/10.1109/IECON.2017.8217217

Chakarothai, J., Wake, K., Arima, T., Watanabe, S., & Uno, T. (2018). Exposure Evaluation of an Actual Wireless Power Transfer System for an Electric Vehicle With Near-Field Measurement. *IEEE Transactions on Microwave Theory and Techniques*, *66*(3), 1543–1552. https://doi.org/10.1109/TMTT.2017.2748949

Chittoor, P. K., Chokkalingam, B., & Mihet-Popa, L. (2021). A Review on UAV Wireless Charging: Fundamentals, Applications, Charging Techniques and Standards. *IEEE Access*, *9*, 69235–69266. https://doi.org/10.1109/ACCESS.2021.3077041

Firdaus, K., Sakakibara, K., Amano, Y., Hirayama, H., Kikuma, N., Tabata, T., & Kojima, S. H. (2015). Design of spiral-slot frequency selective surfaces for shielding from noises of wireless power transfer. *2015*

International Workshop on Antenna Technology (IWAT), 345–347. https://doi.org/10.1109/IWAT.2015.7365280

Imura, T., Okabe, H., & Hori, Y. (2009). Basic experimental study on helical antennas of wireless power transfer for Electric Vehicles by using magnetic resonant couplings. *2009 IEEE Vehicle Power and Propulsion Conference*, 936–940. https://doi.org/10.1109/VPPC.2009.5289747

Karalis, A., Joannopoulos, J. D., & Soljačić, M. (2008). Efficient wireless non-radiative mid-range energy transfer. *Annals of Physics*, *323*(1), 34–48. https://doi.org/10.1016/j.aop.2007.04.017

Khan, S. M. (2017). Analysis of wireless power transfer (WPT) scheme with connected ground planes. *2017 USNC-URSI Radio Science Meeting (Joint with AP-S Symposium)*, 21–22. https://doi.org/10.1109/USNC-URSI.2017.8074877

Khan, S. M. (2019). Practical Considerations for Resonant Near Field Wireless Power Transfer over Common Ground. *2019 USNC-URSI Radio Science Meeting (Joint with AP-S Symposium)*, 75–76. https://doi.org/10.1109/USNC-URSI.2019.8861832

Khan, S. M., & Maresch, N. D. (2013a). Near field wireless power transfer (WPT) between helical antennas under different conditions of orientation and ground plane construction. *2013 USNC-URSI Radio Science Meeting (Joint with AP-S Symposium)*, 116–116. https://doi.org/10.1109/USNC-URSI.2013.6715422

Khan, S. M., & Maresch, N. D. (2013b). Near field wireless power transfer (WPT) between helical antennas under different conditions of orientation and ground plane construction. *2013 USNC-URSI Radio Science Meeting (Joint with AP-S Symposium)*, 116–116. https://doi.org/10.1109/USNC-URSI.2013.6715422

Khan, Saeed, & Bailey, Chad. (2021). Efficient Wireless Power Transfer (WPT) and Field Containment Through Chiral Ordering of a Four-Tier WPT System. *2021 IEEE International Symposium on Antennas and Propagation and North American Radio Science Meeting*, 9–10.

Kurs, A., Karalis, A., Moffatt, R., Joannopoulos, J. D., Fisher, P., & Soljacic, M. (2007). Wireless Power Transfer via Strongly Coupled Magnetic Resonances. *Science*, *317*(5834), 83–86. https://doi.org/10.1126/science.1143254

Kuse, R., Hori, T., & Fujimoto, M. (2015). Filtering characteristics of FSS for realizing perfect magnetic conductor without frequency dependence. *2015 International Workshop on Antenna Technology (IWAT)*, 194–195. https://doi.org/10.1109/IWAT.2015.7365371

Liu, S., Shen, Y., Wu, Y., Lin, J., & Hu, M. (2018). Study on frequency tracking for wireless power transfer system using magnetic resonant coupling. *2018 13th IEEE Conference on Industrial Electronics and Applications (ICIEA)*, 2569–2572. https://doi.org/10.1109/ICIEA.2017-8398144

Luo, H., Wu, W., Meng, T., Huang, J., & Yuan, N. (2015). An absorptive/transmissive FSS radome with lumped resistors loaded. *2015 IEEE Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, 494–497. https://doi.org/10.1109/IAEAC.2015.7428602

Mandal, B., Chatterjee, A., Rangaiah, P., Perez, M. D., & Augustine, R. (2020). A Low Profile Button Antenna with Back Radiation Reduced By FSS. *2020 14th European Conference on Antennas and Propagation (EuCAP)*, 1–5. https://doi.org/10.23919/EuCAP48036.2020.9135328

Marhefka, R. J., Young, J. D., & Towle, J. P. (2007). Design, fabrication and measurement of an FSS antenna ground plane. *2007 IEEE Antennas and Propagation Society International Symposium*, 3972–3975. https://doi.org/10.1109/APS.2007.4396410

Nam Yoon Kim, Ki Young Kim, Young-Ho Ryu, Jinsung Choi, Dong-Zo Kim, Changwook Yoon, Yun-Kwon Park, & Sangwook Kwon. (2012). Automated adaptive frequency tracking system for efficient mid-range wireless power transfer via magnetic resonance coupling. *2012 42nd European Microwave Conference*, 221–224. https://doi.org/10.23919/EuMC.2012.6459399

Saeed Khan et. al. (2018). *Helical antenna wireless power transfer system* (Patent No. US10050475B2). https://patents.google.com/patent/US10050475B2/en

Triviño-Cabrera, A., González-González, J. M., & Aguado, J. A. (2020). *Wireless Power Transfer for Electric Vehicles: Foundations and Design Approach*. Springer International Publishing. https://doi.org/10.1007/978-3-030-26706-3

Visser, H. J. & Lulu Chan. (2014). Active dipole coupling in an array environment. *2014 Loughborough Antennas and Propagation Conference (LAPC)*, 285–288. https://doi.org/10.1109/LAPC.2014.6996377

Wang, Zuming, & et. al. (2021). Wireless Charging Shielding Structure with Periodic Slots in UAVs for Weigh Reduction. *2021 IEEE International Symposium on Antennas and Propagation and North American Radio Science Meeting*, 11–12.

Xing, Z., Yang, F., Yang, P., Yang, J., & Jiang, C. (2020). A Novel High-Performance FSS-AMC Radome Unit. *2020 IEEE International Symposium on Antennas and Propagation and North American Radio Science Meeting*, 777–778. https://doi.org/10.1109/IEEECONF35879.2020.9329852

Zhang, L., Wang, L., Yu, H., Zong, Y., Zhang, Y., Ming, X., & Zhang, Z. (2019). Research on Wireless Power Transfer in Modular Spacecraft. *2019 IEEE Wireless Power Transfer Conference (WPTC)*, 470–474. https://doi.org/10.1109/WPTC45513.2019.9055628

APPENDIX A DB MATH AND PLANE / SPHERICAL TRIGONOMETRY PRIMER

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.[1] 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. A-1

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

10 log (2) = 3 dB (rounded)

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

10 log (0.5) = – 3 dB 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) Eq. A-2

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: ; Eq. A-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.

The Law of Cosines for Sides: $a2 = b2 + c2 - 2bc \cos A$ Eq. A-4

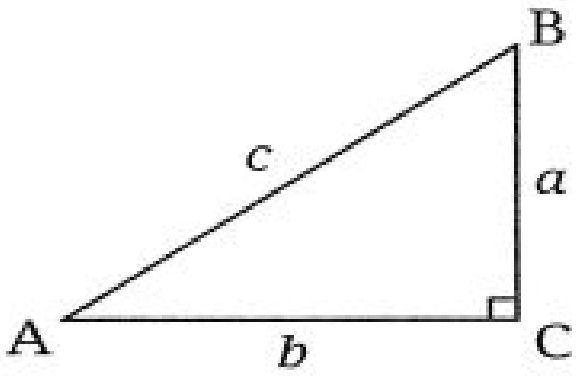
The Law of Cosines for Angles: $A = b \cos C + c \cos B$ Eq. A-5

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 A-1: Right Triangle

Figure A-1: Right Triangle



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

Spherical Trigonometry:

The Law of Sines for Spherical Triangle: Eq. A-6

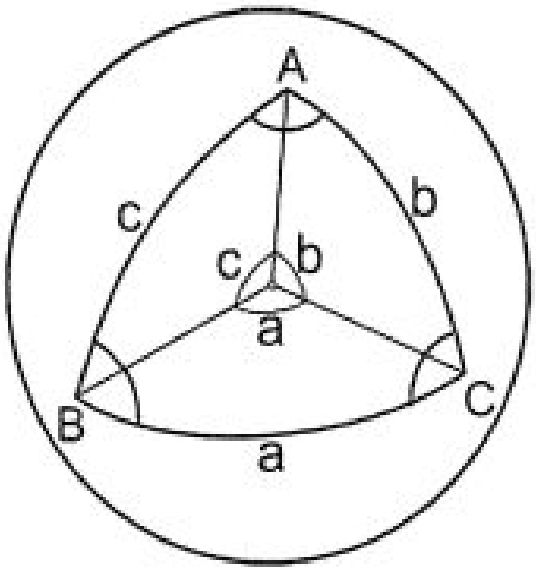
The Law of Cosines for Sides: $\cos a = \cos B \cos C + \sin B \sin C \cos a$ Eq. A-7

The Law of Cosines for Angles: $\cos A = -\cos B \cos C + \sin B \sin C \cos a$ Eq. A-8

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

Figure A-2: Triangle on a Sphere

Figure A-2: Triangle on a Sphere



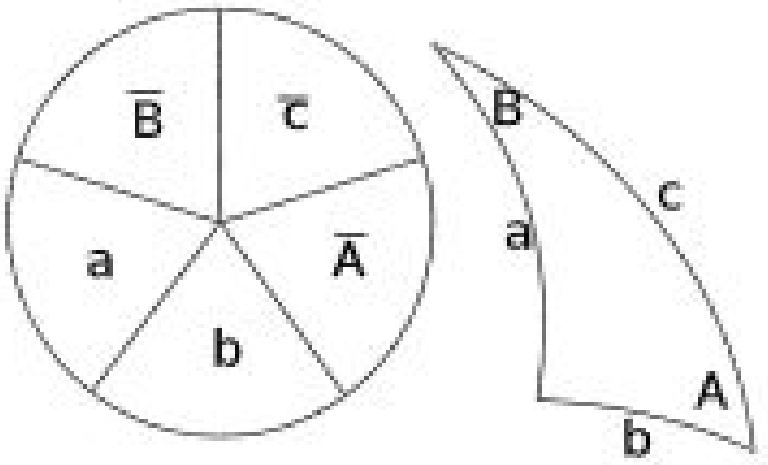
Source: Courtesy of: (Adamy D. L., Space Electronic Warfare, 2021)

Napier's Rules:

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

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

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



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

Rules for Napier's right spherical triangles

sin a = tan b cotan B; Eq. A-9

cos A = cotan c tan b; Eq. A-10

cos c = cos a cos b; Eq. A-11

sin a = sin A sin c Eq. A-12

[1] To multiply linear numbers, add their logarithms; to divide linear numbers, subtract their logarithms; to raise a linear number to the nth power, multiply its logarithm by n; and to take the nth root of a linear number, divide its logarithm by n.