1. Record Nr. UNINA9910874668403321

Autore	Oakley Jacob G
Titolo	Cybersecurity for Space : A Guide to Foundations and Challenges
Pubbl/distr/stampa	Berkeley, CA : , : Apress L. P., , 2024 ©2024
ISBN	9798868803390
Edizione	[2nd ed.]
Descrizione fisica	1 online resource (229 pages)
Disciplina	358.8
Soggetti	Space security Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di contenuto	Intro -- Table of Contents -- About the Author -- About the Technical Reviewer -- Foreword -- Chapter 1: Space Systems -- Tipping Point -- An Introduction to Space Systems -- The Ground Station Design -- SV Design -- Ground Station Functionality -- SV Functionality -- Space System Architectures -- Conclusion -- Chapter 2: Space Challenges -- Environmental Challenges -- Radiation -- Temperature -- Space Objects and Collisions -- Vacuum -- Gravity -- Operational Challenges -- Testing -- Launch -- Deployment -- Detumble -- Power -- Emanations -- Radio Frequency -- De-orbit -- Conclusion -- Chapter 3: Low Earth Orbit -- LEO, SmallSats, and the General Challenges of Space -- Environmental Challenges -- Radiation -- Temperature -- Space Objects -- Gravity -- Operational Challenges -- Testing -- Launch -- Deployment -- Stabilizing -- Power -- Unique Aspects of LEO and SmallSats -- Communications -- Ground Footprint -- Persistence -- Mission Persistence -- Communications -- LEO Mesh Space Systems -- The Challenge of the Mesh -- The Anomaly -- Conclusion -- Chapter 4: Other Space Vehicles -- Medium Earth Orbit -- Geostationary Orbit -- Multi-orbit Constellations -- Special Systems -- Weapons -- Human Aboard -- Extraterrestrial -- Deep Space -- Conclusion -- Chapter 5: Targeting -- Target Selection Methods -- Opportunity -- Ownership -- Function -- Specificity -- Intent -- Collection -- Redirection -- Subversion -- Theft -- Disable -- Mission

Classification Taxonomy -- Sensing -- Radio Waves -- Microwave Radiation -- Infrared Radiation -- Visible Light -- Ultraviolet Radiation, X-Ray, and Gamma Radiation -- Emitting -- Detrimental -- Overt -- Covert -- Beneficial -- Transit -- Cargo -- Passenger -- Communication -- Weapon -- Taxonomy -- Conclusion -- Chapter 6: Pre-operational Vectors -- Design -- Confidentiality -- Non-cyber -- Cyber -- Integrity.
Non-cyber -- Cyber -- Availability -- Non-cyber -- Cyber -- Development -- Confidentiality -- Non-cyber -- Cyber -- Integrity -- Non-cyber -- Cyber -- Availability -- Non-cyber -- Cyber -- Supply Chain Interdiction -- Confidentiality -- Non-cyber -- Cyber -- Integrity -- Non-cyber -- Cyber -- Availability -- Non-cyber -- Cyber -- Testing and Validation -- Confidentiality -- Non-cyber -- Cyber -- Integrity -- Non-cyber -- Cyber -- Availability -- Non-cyber -- Cyber -- General Interdiction -- Conclusion -- Chapter 7: Operational Vectors -- Between Ground and Space -- Confidentiality -- Non-cyber -- Cyber -- Integrity -- Non-cyber -- Cyber -- Availability -- Non-cyber -- Cyber -- Between Space and Space -- Confidentiality -- Non-cyber -- Cyber -- Integrity -- Non-cyber -- Cyber -- Availability -- Non-cyber -- Cyber -- Between Bus and Payload -- Confidentiality -- Non-cyber -- Cyber -- Integrity -- Non-cyber -- Cyber -- Availability -- Non-cyber -- Cyber -- Flight and Operation -- Confidentiality -- Non-cyber -- Cyber -- Integrity -- Non-cyber -- Cyber -- Availability -- Non-cyber -- Cyber -- Analysis and Dissemination -- Confidentiality -- Non-cyber -- Cyber -- Integrity -- Non-cyber -- Cyber -- Availability -- Non-cyber -- Cyber -- Consumers -- Confidentiality -- Non-cyber -- Cyber -- Integrity -- Availability -- Non-cyber -- Cyber -- Conclusion -- Chapter 8: Exploiting Spacecraft -- Safeguards -- Watchdogs -- Gold Copies -- Fall Back Encryption -- Resource Limits -- Power -- Non-cyber Threat to Power 1 -- Non-cyber Threat to Power 2 -- Cyber Threat to Power 1 -- Cyber Threat to Power 2 -- Communication -- Non-cyber Threat to Communication 1 -- Non-cyber Threat to Communication 2 -- Cyber Threat to Communication 1 -- Cyber Threat to Communication 2 -- Navigation -- Non-cyber Threat to Navigation 1 -- Non-cyber Threat to Navigation 2.
Cyber Threat to Navigation 1 -- Cyber Threat to Navigation 2 -- De-orbit -- Non-cyber Threat to De-orbit -- Cyber Threat to De-orbit 1 -- Cyber Threat to De-orbit 2 -- Non-LEO Space Systems -- Weapons -- Non-cyber Threat to Weapons -- Cyber Threat to Weapons -- Crewed -- Non-cyber Threat to Crewed -- Cyber Threat to Crewed -- Extraterrestrial -- Non-cyber Threat to Extraterrestrial -- Cyber Threat to Extraterrestrial -- Deep Space -- Non-cyber Threat to Deep Space -- Cyber Threat to Deep Space -- Conclusion -- Chapter 9: Exploiting Payloads -- Sensing Missions -- Radio Signal -- Non-cyber -- Cyber -- Terrestrial Photo-Imagery -- Non-cyber -- Cyber -- Terrestrial Thermal-Imagery -- Non-cyber -- Cyber -- Terrestrial Monitoring -- Non-cyber -- Cyber -- Space Monitoring -- Non-cyber -- Cyber -- Space Imaging -- Non-cyber -- Cyber -- Emitting Missions -- Positioning -- Non-cyber -- Cyber -- Jamming -- Non-cyber -- Cyber -- Communication Missions -- Broadcast -- Non-cyber -- Cyber -- Pipe -- Non-cyber -- Cyber -- Weapon Missions -- Non-cyber -- Cyber -- Life Support -- Non-cyber -- Cyber -- Other Mission Threats -- Watchdog Abuse -- Bus/Payload Comms -- Conclusion -- Chapter 10: Compromise Microanalysis -- A Series of Unfortunate Events -- The Plan -- Targeting -- Personal Computer -- How -- Why -- Phone -- How -- Why -- Lab Computer -- How -- Why -- Ground Station Computer -- How -- Why -- Payload Computer -- How -- Why -- Data

Handler -- How -- Why -- SDR -- How -- Why -- Conclusion -- Chapter 11: Compromise Macroanalysis -- Initial Ground Station -- How -- Why -- Payload Computer 1 -- How -- Why -- Payload Ground Network -- How -- Why -- Flight Computer -- How -- Why -- Flight Ground Network -- How -- Why -- Payload Computer 2 -- How -- Why -- Mesh -- How -- Why -- Conclusion -- Chapter 12: Architecture -- Data Classification Levels -- System Ownership. Architectural Segmentation -- Payload A -- Payload B -- Conclusion -- Chapter 13: Compromise -- TREKS -- SPARTA -- Mapping a Compromise -- Reconnaissance -- Resource Development -- Known Compromises -- ROSAT Hack -- NASA Landsat Hack -- VIASAT KA-SAT Hack -- Hack-a-Sat -- Conclusion -- Chapter 14: Summary -- The Cost Problem -- The Culture Problem -- Supply Chain Problems -- The Cyber Warfare Problem -- The Test Problem -- The Adaptation Problem -- The Defense in Depth Problem -- The Modernization Problem -- The Failure Analysis Problem -- The Disclosure Problem -- Conclusion -- Index.

Sommario/riassunto

Space is one of the fastest growing military, government and industry sectors. Because everything in today's world exists within or connected to cyberspace, there is a dire need to ensure cybersecurity is addressed in the burgeoning field of space operations. This revised and expanded edition will prime the reader with the knowledge needed to understand the unique challenges to space operations which affect the implementation of cybersecurity. Further, the reader will have foundational knowledge on what impacts cyber threats can have on space systems and how cybersecurity must rise to meet them. The author, who spent years in the United States Marine Corps, originally involved in satellite communications is now a seasoned cyber security practitioner who has provided cyber security vision and strategy to a large portfolio of systems and programs, many focused specifically in space. A published academic and experienced professional, he brings a practical, real-world and tempered approach to securing the final frontier. What You Will Learn Basic concepts of how different space vehicles operate in general. How such systems and their components integrate into cyberspace. A clear picture of the potential damage available via cyber-attacks to such systems. Basic efforts to mitigate such cyber threats will be presented through the various portions of space operations. Foundational issues at the intersection of the space and cyber domains Who This Book Is For This book is written for anyone curious about warfare in the era of cyber everything, those involved in cyber operations and cyber warfare, as well as security practitioners and policy or decision makers who are on the sending or receiving end of such activity.