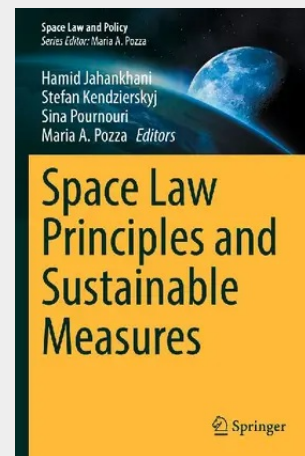


Space Law Principles and Sustainable Measures

This book helps to bridge the knowledge gap that currently surrounds space technology and its method of exploration and highlights much-needed awareness and attention to an increase in Space Law and sustainable measures. The ever-increasing usage of space-based solutions by both public and commercial entities is producing congestion in the radio frequency spectrum as well as orbital slots. The inevitable commercialization of satellite technology will certainly result in a proliferation of privately owned and managed satellite spacecraft in low-Earth orbits. Cyber vulnerabilities in the Air Force and the DoD frequently ignore satellite ground systems. Space ground system cyber security assaults and investigations include those involving satellite control, communications terminal hacking, and GPS spoofing. A continuous cyber security assessment technique is required for space systems to identify, assess, reduce, and address sophisticated cyber threats. Risk-based compliance, regular cybersecurity risk assessments, and a renewed focus on the elimination of system flaws at the time of design are all necessary for space ground and control systems.

Due to the absence of a rigid regulatory framework, satellites play a significant part in the production of space debris, which is a source of increasing worry. Such debris manufactured artificially contributes greatly to the destruction of the environment in Earth's orbit. There is not a single framework in existence that can appropriately govern contemporary concerns like the security of satellite data and debris in orbit. The Department of Defence (DoD) is now responsible for monitoring all objects in space; however, it cannot require satellite operators to take precautions against potential collisions.

This book helps to bridge the knowledge gap that currently surrounds space technology and its method of exploration and highlights much-needed awareness and attention to an increase in Space Law and sustainable measures. The ever-increasing usage of space-based solutions by both public and commercial entities is producing congestion in the radio frequency spectrum as well as orbital slots. The inevitable commercialization of satellite technology will certainly result in a proliferation of privately owned and managed satellite spacecraft in low-Earth orbits. Cyber vulnerabilities in the Air Force and the DoD frequently ignore satellite ground systems. Space ground system cyber security assaults and investigations include those involving satellite control, communications terminal hacking, and GPS spoofing. A continuous cyber security assessment technique is required for space systems to identify, assess, reduce, and address sophisticated cyber threats. Risk-based compliance, regular cybersecurity risk assessments, and a renewed focus on the elimination of system flaws at the time of design are all necessary for space ground and control systems. Due to the absence of a rigid regulatory framework, satellites play a significant part in the production of space debris, which is a source of increasing worry. Such debris manufactured artificially contributes greatly to the destruction of the environment in Earth's orbit. There is not a single framework in existence that can appropriately govern contemporary concerns like the security of satellite data and debris in orbit. The Department of Defence (DoD) is now responsible for monitoring all objects in space; however, it cannot require satellite operators to take precautions against potential collisions.



139,09 €

129,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783031640476

Medium: Buch

ISBN: 978-3-031-64047-6

Verlag: Birkhäuser

Erscheinungstermin: 15.09.2025

Sprache(n): Englisch

Auflage: Erscheinungsjahr 2025

Serie: Space Law and Policy

Produktform: Kartoniert

Gewicht: 318 g

Seiten: 198

Format (B x H): 155 x 235 mm

