

PREVIEW PREVIEW PREVIEW PREVIEW

# PenTest — Hacking

ISSN 1733-7186



# SPACE CYBERSECURITY

**THE FUTURE OF SATELLITE COMMUNICATION:** OPTICAL COMMUNICATION AND **LASERS**. IS

CYBERSECURITY MEASURES IN **MODERN SPACE EXPLORATION**

**S-WAN:** SIMULATE THE TEST OF SPACE SYSTEMS **STORM**

END-TO-END SECURITY MANAGEMENT OF **SPACE SYSTEMS** USING

PREVIEW PREVIEW PREVIEW PREVIEW

**Cover Image**  
Wiktoria Bukowska

**Technical Editors**  
Lee Mckenziie

**Cover Design**  
Wiktoria Bukowska

### Reviewers

Jens Ulrich, Doug Haven, Alberto, Ivan Suarez, Gilbert Oviedo, Salman Aslam, Morgan Weetman, Emanuele Placidi, Carlos Said, Jay Kay, Alberto, Staford Titus, Stewart Wapwanyika, Matt Miller, Tim Hoffman, Sweta Chawla

04	THE FUTURE OF SATELLITE COMMUNICATION: OPTICAL COMMUNICATION AND LASERS. IS IT SECURE?
19	CYBER SECURITY MEASURES IN MODERN SPACE EXPLORATION
35	S-WAN: SIMULATE THE TEST OF SPACE SYSTEMS
42	SPACE THREATS AND OPERATIONAL RISKS TO MISSION (STORM)
50	END-TO-END SECURITY MANAGEMENT OF SPACE SYSTEMS USING COSMOS2
59	SAFEGUARDING EARTH'S FRONTLINE: THE CRUCIAL ROLE OF CYBERSECURITY IN SPACE OPERATIONS
66	SPACE CYBERSECURITY: A STRATEGIC ISSUE IN THE CURRENT GEOPOLITICAL CONTEXT
71	SPACE ODDITIES: WHAT IS 'SECURE-BY-DESIGN' AND WHY DOES IT MATTER FOR SATELLITES?

All trademarks, trade names, or logos mentioned or used are the property of their respective owners. The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

# EDITOR'S WORD

---

Dear Readers,

We are very proud to present you with a special edition, created in a collaborative process between experts in the field of space cybersecurity, PenTest, and Hakin9 magazines. The topic is currently getting more and more deserved attention, and we are more than happy to bring experts' voice to the table here. In the "Space Cybersecurity" eBook by PenTest & Hakin9 you will read about this fascinating area from a variety of perspectives: from the future of optical and laser communication and its security, through cybersecurity measures in modern space exploration, simulating the test of space systems with S-WAN, end-to-end security management system using COSMOS2, Space threats and operational risks to mission, security by design for satellites, to the relevant information about ASAT, geopolitical aspects of space cybersecurity, and cybersecurity in the ground segment for space industry. It is a great compendium of knowledge provided by the practitioners in the field. Special thanks to all the contributors, reviewers, and proofreaders involved in the creation of this issue.

Without further ado,

Let's launch and dive in the reading process.

PenTest & Hakin9 Editorial Team

# SPACE CYBERSECURITY: A STRATEGIC ISSUE IN THE CURRENT GEOPOLITICAL CONTEXT

*Anais Shay-Lynn Vydelingum*

by Anais Shay-Lynn Vydelingum

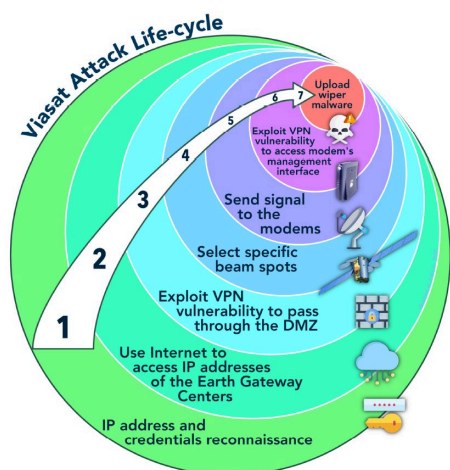
*The security of space infrastructures is a geopolitical issue, as space-based resources are increasingly used by our societies in all fields, from construction and financial markets to military capabilities. The rapid development of objects and services powered by satellites is contributing to a growing dependence on space in all fields. Being present in space has become a strategic issue over time, depending on the interest of decision-makers in the use of space. Protecting satellites in low, medium, or geostationary orbit is now a strategic asset for governments, the military, and commercial operators alike, to ensure continuity of service and guarantee a degree of resilience.*

## **The Viasat case (2022): the various impacts of a cyberattack via the satellite network**

On February 24, 2022, Viasat was the victim of a cyber-attack affecting their KA-SAT network. Due to its singularity and the context in which it

took place, this attack has become a textbook case in the field of space cybersecurity.

Several modems were hacked, and thousands of customers in Europe, particularly in the Ukraine, were left without internet access for around a month. The attack began about an hour before Russia began its invasion. The vulnerability used by the attackers was CVE-2018-13379, corresponding to a Fortinet firewall vulnerability discovered in 2019. The attackers selected specific beam spots and then sent a signal to the modems once on the trusted management segment of the KA-SAT network. They exploited VPN vulnerability to access the modem's management interface and then uploaded wiper malware (see scheme below).



*Viasat Attack Life-cycle. Nicolò Boschetti (Cornell University) and Gregory Falco (Cornell University) – 2022*

The EU, the UK, and the USA have estimated that Russia (the Russian military intelligence agency – GRU) is almost certainly responsible for this attack, which can be seen as a form of militarization of space (cf. ESPI Short Report 1 – The war in Ukraine from a space cybersecurity perspective, 2022).

The Viasat case shook the space community to the point where decision-makers began to discuss the cybersecurity of space systems more seriously since such an attack can damage different types of targets: government equipment, military capabilities, civilian equipment, and the living conditions of a population. In the Ukrainian context, civilians have

been further isolated by the loss of their Internet connection. Isolating a population is a strategic way of making it vulnerable, as the means of communication make it easier to organize and plan actions. The attack on Viasat also led to the loss of remote monitoring access to over 5,800 wind turbines belonging to a major German energy company, Enercon. Almost 9,000 subscribers in France to a satellite Internet service provider suffered an Internet blackout, just like 40,000 other subscribers across Europe in Italy, Poland, and Hungary.

This context shows the vulnerability of commercial space systems when used in armed conflicts for strategic purposes; a single attack can exploit several vulnerabilities. Added to this is the complexity of the supply chain organization for space services. The security vulnerabilities of third parties can, in the event of an attack, give rise to a snowball effect between players in the same ecosystem. Moreover, the duality of the space sector makes the analysis of cyber impacts more complex, given the cultural differences in infrastructure security between a civilian player and a military institution, for example.

Researchers Gregory Falco, Nathaniel Gordon, and Nicolo Boschetti were able to make recommendations regarding the Viasat attack, shedding light on possible improvements to be made within organizations using space technologies, such as the need for a dual-use technology to be used as a military technology (managerial solution) or the importance of track precursor indicators (technical solution). (See: Boschetti, Nicolò & Gordon, Nathaniel & Falco, Gregory. (2022). Space Cybersecurity Lessons Learned from The ViaSat Cyberattack.)

## **A slow but growing general awareness of the importance of spatial cybersecurity strategies**

From a security point of view, awareness of cyber risks and threats is evident in commercial and government space activities, on a European and international scale. From a general point of view, considering the duality of the domain, there is a lack of standardized security protocols across satellite developers used transversally and concomitantly. Added

to this are the obstacles posed by the cost of protecting satellites with onboard hardware-based security solutions.

Today, cybersecurity in space is a field in which governments and commercial organizations are unequal in terms of knowledge and resources. Few are aware of the issue, and there is a lack of understanding among cybersecurity experts of the particularities of the space domain.

The United States has a step ahead in this field with 'the inclusion of a sub-chapter on improving cybersecurity for space assets in the Trump administration cybersecurity strategy (September 2018); the launch by NASA of a cybersecurity guide for the space industry in December 2023; and the inclusion of space cybersecurity issues in standards, new national strategies and innovation through new cyber risk analysis methods for space (MITRE, SPARTA, etc.).

The European Union, for its part, is modernizing its space policies, with initiatives such as EU Space ISAC (European Space Information Sharing and Analysis Center), modeled on the American Space ISAC, the recognition of space as an area in which infrastructures are highly critical (NIS2 Directive on measures for a high common level of cybersecurity across the Union, December 2022), and the inclusion of cybersecurity issues in the European Union's space program (2021-2027). This awareness on the part of European entities is positive, since these initiatives are enabling the inclusion of startups specializing in this field, or the emergence of specialized companies to meet the growing challenge of cybersecurity in space.

The New Space phenomenon has led to the development of startups specializing in solutions for securing satellite communications. This security is often based on innovative methods that are constantly evolving. From a geopolitical point of view, we are witnessing the proliferation of technology hubs dedicated to the aerospace industry, such as Toulouse, which today has an increasingly international reach. Experts in the field are also eager to meet and exchange best practices. This is reflected in the creation of CYSAT, Europe's largest space cybersecurity event, organized by cybersecurity company CYSEC.

The geopolitical context – constantly demonstrating the relevance and need for security in space assets – is influencing the revolution in space cybersecurity innovation. If space is a fashionable subject, it's also one that decision-makers are unlikely to ignore any longer, given the aspirations of private players (to go to Mars, conquer the Moon, develop space tourism, exploit asteroids) and the growing power of China (space exploration, Mozi satellite, 6G...) and India in the field (ASAT, etc.).

Thus, cyberspace is a field of global conflict involving space infrastructures owned or operated by space players from all over the world and threatened by organizations, states, or cybercriminals independent from civil society. This imbalance between players highlights the need for innovation and the implementation of appropriate solutions (software/hardware, information sharing, etc.).



# 2024 HIT COURSE!




## AEROSPACE CYBERSECURITY: SATELLITE HACKING

THIS COURSE IS MEANT FOR ANYONE WHO WANTS TO LEARN MORE ABOUT SPACE-RELATED CYBERSECURITY SPECIFICALLY IN RELATION TO SATELLITE SYSTEMS, TO ANYONE OF ANY SKILL LEVEL WHO IS INTERESTED IN EXPANDING THEIR SKILL SET IN SATELLITE RECONNAISSANCE AND VULNERABILITY ANALYSIS.

# FUTURE IS NOW!

eForensics | VOL. 12  
NO. 01

ISSN 2300-6986



## SATELLITE FORENSICS

---

DIGITAL FORENSICS IN SATELLITE AND <b>UAV</b> TECHNOLOGY	THE WORLD OF SATELLITES: <b>UNLOCKING MYSTERIES</b> BEYOND EARTH	TOOLS USED FOR <b>SPACE SATELLITE FORENSICS</b>	WINDOWS DIGITAL <b>CYBER-CRIME</b> FORENSICS INVESTIGATION
--	---	--	--

SATELLITE TECHNOLOGY HAS BECOME A UBIQUITOUS FEATURE OF MODERN LIFE, PROVIDING INTEGRAL SERVICES SUCH AS COMMUNICATION, NAVIGATION, STREAMING, EARTH OBSERVATION, AND SCIENTIFIC RESEARCH.