58th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cybersecurity in space systems, risks and countermeasures (4)

Author: Ms. Anna Metallinou
Charles University, Czech Republic

Ms. Angeliki Papadimitriou
Université Paris-Sud XI, France
Mr. Stefano Zatti
University of Rome "La Sapienza", Italy
Dr. Christina Giannopapa
Eindhoven University of Technology, The Netherlands

AN EVOLVING REGULATORY FRAMEWORK IN EUROPE IN THE FIELD OF CYBERSECURITY

Abstract

Cybersecurity, encompassing the security of network and information systems, plays a fundamental role in safeguarding critical infrastructure and ensuring economic stability in an increasingly digitalized world. In the space sector, cybersecurity is a key enabler for secure and resilient space-based services that support essential civilian, governmental, and military activities. The objective of this paper is to analyze the cybersecurity strategies and policies in Europe concerning space security, focusing on the role of the European Union (EU), and the Member States.

The first section of this paper examines the European cybersecurity strategies and regulatory frameworks currently in place, highlighting the role of key institutional actors such as the European Union Agency for Cybersecurity (ENISA) and other relevant EU and international bodies. The second section explores the intersection of cybersecurity with space and security policies in Europe and in cooperation with EU institutions to enhance cyber resilience in the space domain. The third section assesses the cybersecurity approaches adopted at the national level by European Member States, focusing on space-related cyber threats, vulnerabilities, and policy responses.

This paper identifies key challenges and vulnerabilities in the cybersecurity landscape for space, including threats to satellite systems, communication networks, and critical ground infrastructure. It further outlines the necessary security, industrial, and procurement policy measures required to mitigate risks and enhance Europe's strategic autonomy in space cybersecurity. By providing a comprehensive overview of legal, policy, and technological developments, this paper aims to contribute to the broader discourse on strengthening cybersecurity for space as an integral component of European security policy.

References

1. Council of the European Union. (2024). Council Decision (CFSP) 2024/XXX concerning restrictive measures against cyber-attacks threatening the Union or its Member States. Official Journal of the European Union. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX

2. European Union Agency for Cybersecurity (ENISA). (2023). EU cybersecurity certification framework. Retrieved from https://www.enisa.europa.eu/topics/standards/certification

3. European Union Agency for Cybersecurity (ENISA). (n.d.). EU-CyCLONe: European Cyber Crisis Liaison Organisation Network. Retrieved from https://www.enisa.europa.eu/topics/cyber-crisis-cooperation/eu-cyclone

4. European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union,

amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS-2 Directive). Official Journal of the European Union. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX