55th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cybersecurity in space systems, risks and countermeasures (4)

Author: Mr. Antonio Carlo
Tallinn University of Technology, Estonia, ancarl@taltech.ee

Dr. Nebile Pelin Mantı
Space Generation Advisory Council (SGAC), Turkey, npmanti@gmail.com
Mr. Bintang A.S.W.A.M
Space Generation Advisory Council (SGAC), Indonesia, baswam95@gmail.com
Ms. Francesca Casamassima
Italy, fcasamassima8@gmail.com
Mr. Nicolò Boschetti
The Johns Hopkins University, United States, nbosche1@jhu.edu
Dr. Paola Breda
HyImpulse Technologies GmbH, Germany, breda@hyimpulse.de
Mr. Tobias Rahloff
Deloitte Germany, Germany, rahloff@gmail.com

UNDERSTANDING SPACE VULNERABILITIES: DEVELOPING TECHNICAL AND LEGAL FRAMEWORKS FOR AI AND CYBERSECURITY IN THE SPATIAL FIELD

Abstract

Over the past decades, industries and governments have progressively been relying upon spatial data-centric and data-dependent systems. Consequently, this led to the emergence of malicious activities, also known as cyber-threats, targetting such systems. To counter these threats, new technologies such as Artificial Intelligence (AI) have been implemented and deployed. Today, AI is highly capable of delivering fast, precise and reliable command-and-control decision-making as well as providing reliable vulnerability analysis using well-proven cutting-edge techniques. AI can also play a transformative and important role in the future of space cybersecurity, and it poses questions on what to expect in the near-term future. Challenges and opportunities, deriving from the adoption of AI-based solutions to achieve cybersecurity and later cyber defence objectives in both civil and military operations, bring a new framework and new ethical requirements. In fact, most of these technologies are not designed to be used or to overcome challenges in space. Because of the highly contested and congested environment, as well as the highly interdisciplinary nature of threats to AI and machine learning technologies, including cybersecurity issues, a solid and open understanding of the technology itself is required, as well as an understanding of its multidimensional uses and approaches. This includes the definition of legal and technical frameworks, ethical dimensions and other concerns such as mission safety, national security, and technology development for future uses. The continuous endeavours to create a framework and regulate interdependent uses of combined technologies, building resilient systems to counter "new" threats, in this case AI and cybersecurity, require the research and development of "living concepts" to determine in advance the vulnerabilities of the networks and the AI. This paper will develop a cybersecurity risk and vulnerability taxonomy for the future applications of AI in the space security field. Moreover, it will assess to what extent a network digital twins' simulation can still protect networks against relentless cyber-attacks in space, against users, and ground segments. This allows for conclusions to be drawn based

on the business impact (reputational, environmental, and social) of a cyber malicious activity. Since AI technologies are developing daily, a regulatory framework will be proposed using ethical and technical approaches for the technology and its use in space. Please note that the present abstract is submitted under the auspices of the Space Generation Advisory Council, as part of the activities of the Space and Cybersecurity Project Group.