56th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cybersecurity in space systems, risks and countermeasures (4)

Author: Mr. Giorgio Cardile
Ielo and Associates Law Firm, Italy

THE THREAT OF AI-DRIVEN CYBER ATTACKS ON SPACE SYSTEMS

Abstract

Law and AI have in common that they are useful tools for effective management of society. The increasing large-scale use of AI is leading to regulatory responses, including the AI Liability Directive, proposed by the European Commission. The breakdown of AI systems into risk levels, proposed within the forthcoming regulatory text, places those related to space infrastructure among those with high risk. This discussion will outline possible threats that already exist - and for which readiness is not fully established - that high-risk AI systems could pose to space activities. AI-driven cyber attacks include the use of convolutional neural networks, often with the intent of making Access and Penetration or Reconnaissance attempts. Also due to the increasing deployment of cloud technology, space infrastructure is among the targets at risk, along with all the industries that have not yet invested in enhancing their cybersecurity against AI-driven attacks. AI is not a nefarious tool, it depends on how it is used. AI systems first tested and developed in a sandbox, and of the "white box" model - that is, those that are able to explain how they arrived at a particular result - could serve both as countermeasures to attacks of this kind and as assistants to humans in numerous tasks, from analyzing and cataloging data to being used as a means of evidence in processes. Regulation presents two opposing risks: on the one hand avoiding possible underregulation; on the other, overregulation. As for the first risk profile, for most high-risk AI systems, verification of compliance with the requirements set by the Liability Directive is left to the self-assessment of providers. With the exception of systems for biometric identification and categorization, there is no requirement for public authorization to market an AI system. Referring to the second risk profile, the definition of an AI system as "software developed with one or more of the listed techniques and approaches [...], which can, for a given set of human-defined goals, generate outputs such as content, predictions, recommendations, or decisions that influence the environments with which they interact" risks, on the contrary, posing overregulation problems for some AI vendors and users. For example, AIs based on logical reasoning, which do not present particular critical issues from the standpoint of respecting fundamental rights. An attempt will be made to propose a scientific approach to the issue of regulating high-risk AI systems used in space activities.