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

Author: Mr. Júlio Santos
University of Beira Interior, Portugal

Mr. Daniel Resende
University of Beira Interior, Portugal
Mr. Diogo Peralta Cordeiro
University of Porto, Portugal
Mr. Tiago Rebelo
SIMPLYCONNECTED Lda (CONNECTED), Portugal

ANALYSING SPACE CYBERATTACKS WITH NIST AND SPARTA FRAMEWORKS

Abstract

News reports frequently address incidents of cyberattacks. Hacking is not new in the majority of industries, and it has been around for quite some time, however, we have always been led to believe that it only affects terrestrial assets and networks, ranging from individuals to large corporations. However, this idea is in the process of changing as the number of hacking attempts on space assets has increased.

With the actual dependency on space assets for the daily lives of the worldwide population (Communication, Navigation, Weather, and Earth Observation, among others), and with the democratisation of space, part of the so-called Newspace boom - where the number of satellites in orbit is exponentially growing, much like their complexity - an increasing concern about cybersecurity in space began to echo. The importance of satellites, not only for civilian purposes but also for military applications such as uncovering strategic advances of the troops in the field, requires augmented risk management efforts.

The growing concern about cyberattacks in the space sector is beginning to be visible, and there have been attempts in developing frameworks to help companies and government agencies create countermeasures for these cyberattacks. These frameworks aim at really understanding the potential threats in terms of tactics, techniques, and procedures (TTPs). For example, recently, the US National Institute of Standards and Technology (NIST) released the "Cybersecurity Framework tailored to the ground-based", also The Aerospace Corporation created the Space Attack Research and Tactics Analysis (SPARTA) matrix, both of which reinforce the focus on understanding potential threats in terms of common TTPs.

This paper, primarily, intends to pave the way for how to use the NIST and SPARTA frameworks and analyse the most significant space cyberattacks, in the light of these frameworks, by doing a comprehensive review of historical cyberattacks involving jamming, eavesdropping, hijack by spoofing the transmission, or control by using some malware, as well as attacks at the satellite backbone like ground infrastructures through terrestrial web attacks, service vulnerabilities, ransomware, denial of service, domain issues and phishing.

Finally, as a secondary objective, this paper attempts to summarise the general guidelines that could either have mitigated the consequences or completely avoided the attacks, thus highlighting the key aspects of risk management in a space cyber-ecosystem.