

## IAF SYMPOSIUM ON SPACE SECURITY (E9)

Cyber-security threats to space missions and countermeasures to address them (2.D5.4)

Author: Mr. Antonio Carlo

Space Generation Advisory Council (SGAC), Italy, antonio.carlo@spacegeneration.org

Ms. Lisa Lacroix

Space Generation Advisory Council (SGAC), Germany, lisa.lacroix@spacegeneration.org

Ms. Lea X

Space Generation Advisory Council (SGAC), Switzerland, laezar@protonmail.ch

## THE CHALLENGE OF PROTECTING SPACE-BASED ASSETS AGAINST CYBER THREATS

**Abstract**

After more than 60 years of space activities, society has become dependent on space based technologies. The proliferation of private actors in the last decade has resulted in an intense race, while States are showing a renewed interest in space by increasing their investments and supporting diverse types of operations. Access to space is no longer limited to big powers as there is an increasing number of countries and private actors that own and operate satellites for all types of uses, including sensitive military capabilities and vital civilian infrastructures.

Policy gaps are plentiful regarding the application of cybersecurity to space-based assets. This relates to the lack of global consensus on a precise definition of a use of force and on a clear threshold for what constitutes a use of force in cyberspace. National and global cybersecurity policy are still cautious when addressing digital security threats. Applied to space-based assets, this policy landscape lacks precision. As a matter of fact, a cyber operation targeting critical infrastructures could be the easiest and the most efficient way to disrupt essential services by inserting malicious codes aiming at stealing information or hindering any command and control systems. If not preempted, such attacks could become a serious threat to space missions. Additionally, even though signatures and codes gradually become easier to identify, States and commercial actors are not rushing to ameliorate the process of attribution regarding the identity of cyber attackers. However, protecting space missions would not only require resilient and flexible systems but also the identification of the potential cyber threats and exposed components within the whole infrastructure to mitigate the risks.

In this context, establishing clear mechanisms related to space-based assets security in the cyber world is not only important to build long-term sustainability in outer space. This is also necessary due to the lack of accepted international norms concerning unacceptable behavior in cyberspace.

This paper will first briefly review how cybersecurity is addressed at both national and international levels. It will then assess the most important shortfalls of the existing legal regimes and the need for mitigation measures. Finally, it will conclude with suggestions and best practices to strengthen the protection of space-based assets in the cyber world.

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.