Published 24 June 2020

AFCEA Europe WORKSHOP

Cyber Security in and for Space Operations

Preliminary Programme Overview

Space, as an operational domain in defense and as a specific part of critical infrastructure and its importance to the welfare of nations and its people are rather new thoughts in the Brussels arena.
Recent political and technological developments such as the European Union’s “New Space” approach, NATO’s new space policy, nano satellites and internet via space are adding pressure on one of the most unknown but critical elements of space operations - enhanced cyber security. As cyber attacks can impede operations in or via space physically as well as virtually and in many ways, developing a sophisticated defense stance is of increasing importance.

Therefore this workshop on Cyber Security in and for Space Operations is focusing on raising awareness on specific cyber security requirements, fostering mutual understanding between strategists, space operators and cyber defenders, and intends to identify steps to be taken in support of a new, more cyber-secure space era.

The newest challenges, concepts and technologies will be discussed with representatives from NATO, the EU, national governments, research institutions and industry during this workshop. In addition, this workshop may also help to establish a Brussels-based group of like-minded experts for space-related questions in defence for both NATO and the EU.

Session I: Cyber Threats to Space Missions

Introductory Fireside Chat: ***Wonderful New Space: Are Small Satellites Opening Big Gates for Cyber Attacks***?

Referring more to the commercial approach, this discussion will highlight the role and vulnerabilities which might arrive with the widespread use of low-cost satellites (“cubesats”) now and which will greatly increase in the near future. Such easily deployable, numerous small satellites will play an increasing role for the commercial use of space and for governmental space operations. Building the foundation of a new internet architecture in space underlines the importance of this specific critical infrastructure.
The discussion might explore to what extent built-in cyber security is part of this infrastructure and if there are risks, how retroactively added security features might mitigate. The role of a secure supply chain will

have to be visited in this regard as well. Any other relevant aspects of future cyber threats for the New Space will be discussed.

Panel 1: ***Thinking the Opposite Direction: How Could Cyber Penetration of Space Assets Benefit the Aggressor?***

Satellites are long-lasting objects, designed times ago with state- of-the art technology and architecture. Cyber threats may not have been of major concern some decades ago. In assuming a different role and changing perspective, the panel should think as a “red team”. The core question is to identify what range of operational effects could be imparted by cyber penetration of space assets.
Thus, the known and the hidden cyber threats to highly sophisticated and specially designed space objects might become clear. Specific vulnerabilities to elements of a space systems (satellites, links, ground-based networks, user interfaces) can be identified. Threats and attack vectors may change over the lifetime of space systems. The additional and worsening impact of simultaneously executing such attacks by interfering via the electromagnetic spectrum can also be addressed. The special role of Advanced Persistent Threats (APTs) towards governmental satellites might be worth mentioning.

Session II: What Needs to be Done?

Panel 2: ***Technology, Policy and Governance to Fix Old and Prevent New Vulnerabilities***

The central role of this panel is to identify options and suggestions on how to mitigate risks for existing or future satellite systems in all applications. Beyond technological means, the question is how the increasing reliance of governments on commercial capabilities and the use of private-public partnership (PPP) will offer additional options—and possible or risks. How to organise effective cyber defence in such a PPP or in cooperation with commercial providers should be addressed.
Managing a secure supply chain, defining and agreeing on standards, requirements and certification procedures including cryptology for space assets is not only a question for the international market, but for the survivability of essential services and space based strategic means.
Finally, the question of resilience in PNT Satcom systems has gained high topicality, also resilience under the additional aspects of attacks from the electromagnetic spectrum.