“ESPI BRIEFS”
No. 26

ESPI
European Space Policy Institute

Cyber Security: High Stakes for the Space Sector

1. Outer Space: An Increasingly Critical Socio-Economic Infrastructure

Space systems are becoming closely intertwined with and critical for an increasing number of economic sectors. Be it remote sensing data used for weather forecast, satcom links for emergency services or GNSS signals employed in the energy, transportation or financial sectors, advanced economies thrive and prosper on these brilliant technological advancements.

However, as a result of this increasing reliance, the socio-economic consequences of an even partial disruption of the availability or integrity of space data and signals could be dramatic. As an example, it was highlighted during the 2018 “EUSpace for Business” conference that up an estimated 10% of the European Union’s GDP - around 1.6 T€ - rely on the availability of the GNSS signal. Its disruption or halt, however briefly, would by all means have the same effect of a power grid blackout, throwing back to decades ago the functioning of a large number of associated services and economic activities, when not impeding them outrightly.

As such, awareness of this interdependence has raised the issue of security of space activities high in the priorities of decision-makers, be it due to space weather or human actions, becoming one of today’s most-discussed topics; and with cyber security undoubtedly being one of the crucial components.

With the advent of new ground-based applications enabled by space systems, such as autonomous vehicles, and emerging space activities such as in-orbit servicing missions, as well as enlarged SSA programmes, it is clear that the stakes for the space sector are as high as ever.

2. Cyber Space: The (not so) New Battleground

In recent years, cyber-attacks have become ever more complex, frequent, with an increasing number of targets and motivations, and perpetrated by a growing number of actors. From classic stealing of personal and financial (big) data to corporate espionage, from state-sponsored cyberwarfare activities to indiscriminate destructive attacks (or just a mix of all this), this decade has witnessed a blossoming number of increasingly bold offensive manoeuvres in cyber space – a trend only poised to continue. Just in 2017, a major event caused massive disruptions in global production, supply and logistic chains, wreaking havoc to the tune of several billion euros in just a matter of hours.

Public agencies as well as private companies have been tackling the issue of safety and integrity of their space infrastructure since years, extremely aware on the cyber threat level at every point of the value chain, from system components’ design to operations. Despite a handful of notable events, cyber-attacks on space systems, (in the form of signal jamming, spoofing, ground and/or space segment attacks), while taking place daily at various degrees of severity, have not reached (yet?) such critical mass in terms of damage, at least not enough to cause widespread alertness.

Yet, the space sector is today undergoing a fast-paced and unprecedented expansion which could also have relevant implications on how cyber security has to be dealt with in the future.

3. *Cyber Security in Emerging Outer Space Activities*

In the contemporary context of "New Space" and Space 4.0, space activities are becoming more and more accessible (for private entities and nations alike) and commercialised. When looking at this development through the lens of cyber security, one of the factors of concern is not just an increase in the number of actors and operated systems (i.e. possible targets, so to speak), but also in the level of attention paid to make these systems secure and resilient against cyber-attacks.

For example, start-ups for which time to market is of essence to survive might be less inclined to adopt or abide to cyber security standards potentially expensive and time-consuming to implement. Recognising the risk of having thousands of small satellites to be launched in the next few years not cyber-resilient enough to potential hijacking, some experts went as far as suggesting a "*no encryption no fly*" policy for small satellites.

These new developments, on top of the ever-increasing dependency on space activities, call for further and rapid development of apt policies and measures (also to avoid potential *ex-post* over-regulation following a space cyber incident), necessarily to be addressed in a cooperative framework among all involved stakeholders.

4. *Enhancing European Preparedness through Encompassing Policy Actions and Dialogue*

In this regard, European efforts are today manifold, and undoubtedly progressing in the right direction: starting from key capabilities at Member State level; to the ESA-EDA cooperation framework; the upcoming ESA CM/19 proposals on (cyber) security; a strengthening of EU initiatives including of its cyber security Agency, ENISA; and increased EU-NATO strategic dialogue among several others.

Considering the interdependency of all the actors, cyber security should indeed be tackled as an integral and horizontal component in space activities. A number of additional measures could also be envisioned, in order to further strengthen and enhance European strategic positioning, preparedness and resilience:

a) Further reinforcing cyber education programmes and awareness, as the human factor often remains the weakest link;
b) Defining space as a critical infrastructure, like transportation and the energy sector, in all European MS, allowing it to be granted the full benefits in terms of provisions and measures that this status entails;
c) Continuous sharing of best practices, experiences and information (e.g. on a voluntary basis, to overcome a potential lack of trust) among different players – operators, manufacturers, institutions – for example, in a permanent "European Outer Space Cyber Info Council";
d) Breaking down of "competency silos" to allow for increased exchanges between domains: civil and military, space and nonspace, national and intergovernmental, private and institutional;
e) Identifying technological backup options in case of emergency situations; and prepare contingency plans and crisis management scenarios involving various degrees of incapacitation or loss of European space assets.

The upcoming European initiative on GovSatCom, which itself has a strong security component and envisions a pooling and sharing of different systems and assets belonging to a variety of actors, could also represent an ideal test bed for putting into practice state-of-the-art cyber security policies, common requirements and agreed-upon advanced standards.

Available for download from the ESPI website:
www.espi.or.at

Short title: "ESPI Briefs" No. 26
Published in: November 2018

Editor and publisher:
European Space Policy Institute, ESPI
Schwarzenbergplatz 6 • A-1030 Vienna • Austria
Tel: +43 1 718 11 18 -0 / Fax: -99
Email: **office@espi.or.at**