"ESPI BRIEFS"
No. 44

ESPI
European Space Policy Institute

U.S SPD-5: towards a better coordinated approach on space cybersecurity

1. The U.S. SPD-5: general principles and guidelines for space systems

On September 4th 2020, President Trump signed the Space Policy Directive 5 (SPD-5), establishing the first cybersecurity policy for space systems. Building on SPD-3 and the 2018 National Cyber Strategy, it outlines five cybersecurity principles that space systems should adhere to:

- cybersecurity should be considered across the mission's lifecycle;
- space systems should develop cybersecurity plans to protect satellites, ground stations and information processing systems against unauthorized access, jamming and spoofing, attacks on command and control systems, as well as supply chain and physical threats;
- adoption of best practices and norms of responsible behaviour;
- collaboration towards best practices and information-sharing on threats and attacks;
- adoption of cybersecurity measures adapted to mission requirements without being an undue burden.

The release of SPD-5 puts cybersecurity as a priority on the US space agenda. However, contrary to other SPDs, it only contains general, non-binding recommendations and does not define roles, responsibilities or implementation measures. There is no mention of specific US systems, missions or the Space Force's cyber operations. Yet, it is understated that a cyberattack can trigger countermeasures as cybersecurity arises out of *"active defense"*, which is another word for counter-offensive actions. SPD-5 seems to rather be a policy effort to establish common cybersecurity fundamentals and ensure consistency and coordination among all space stakeholders to possibly leverage commercial systems (including New Space) for governmental use.

2. Space cybersecurity: a critical component of national security

SPD-5 should also be understood within a geopolitical, operational and technological context.

First, jamming and spoofing, often classified as electronic warfare, are outlined as potential cyber threats in SPD-5. Electronic attacks target RF signals to interfere with satellites whereas cyberattacks target data, networks and software to interfere, compromise or control space systems. However, with the increasing digitalization of space systems, the effects of electronic attacks can now also be obtained through cyber means. In this sense, SPD-5 could be understood from a military doctrine perspective with the progressive adoption of the concept of multidomain operations (MDO). MDO are usually understood as joint operations conducted across multiple domains (including space and cyberspace) and contested spaces to overcome an adversary's Anti Access Area Denial capabilities (including jamming and spoofing). Cyberspace and space are essential for MDO as they link and synchronise actions across domains within a digital architecture as outlined in the new Space Force doctrine: *"cyberspace operations … are a crucial and inescapable component of military space operations and represent the primary linkage to the other warfighting domains"*. MDO create an even stronger dependency on space and cyberspace. Therefore, the cybersecurity of space systems is paramount, especially since 80% of US military operations rely on commercial satellites for non-critical missions.

Then, SPD-5 states that space operators should follow the National Institute of Standards and Technology (NIST) Cybersecurity Framework. This is particularly interesting with regard to the race for quantum supremacy between the US and China. Indeed, in 2016, NIST decided to engage in the development of post-quantum encryption standards to mitigate the risks of quantum computing which might be capable of decrypting today's encryption algorithms and easily hack into classic computers, including satellites. Quantum is one of the many future cyber threats on space systems. By encouraging

operators to follow NIST standards, SPD-5 is a first step to coordinate space cybersecurity among all stakeholders.

3. Space Cybersecurity in Europe: emerging policies from the bottom-up

The general issue of cybersecurity is taken into account at the EU level with the 2014 EU Cyber Defence Policy Framework which aimed at protecting communications (satellite and terrestrial) in the context of Common Security and Defence Policy (CSDP) actions, among other things. Additionally, the 2017 Cyber Diplomatic Toolbox enables the EU to apply sanctions against individuals responsible for cyberattacks. In case of a cyberattack against a European satellite, the toolbox could conceivably be implemented.

However, there is no EU legislation or policy dedicated to the cybersecurity of space systems. Regulations and information-sharing are still limited. For example, the EU Agency for Cybersecurity has never mentioned space systems in its analyses. Yet, space cybersecurity emerges as a serious concern at the EU level but in a scattered manner. Indeed, the 2018 Space Programme Regulation states that the European Commission is responsible for the protection of the space infrastructure against cyber-attacks but does not specify how. It also states that the upcoming European Union Agency for the Space Programme will have to establish an advisory body to provide expertise regarding cyber threats. The 2020 EU Security Union Strategy recognises space systems as essential services that should be protected against potential threats (including cyber) and states that the commission is working with Member States to create an end-to-end space-based and terrestrial quantum infrastructure.

At the Member State level, cyber threats on space systems have been recently taken into account, in particular:

- In France, the 2019 Space Defence Strategy recognises the cyber threat on satellites. Military satellites have to be hardened, protected and redundant. Also, France's cyber policies consider satellites as part of cyberspace.
- In the UK, the Space Agency issued a Cybersecurity toolkit for space companies in 2020, detailing the types of threats, attackers, incidents reporting and cyber security standards to apply.
- In Italy, the 2019 security strategy for space recognises cyber threats on space and ground segments.
- In Estonia, the 2020 Space Policy is based on 3 pillars: innovation, cybersecurity and AI.

For its part, ESA has improved its cybersecurity standards applicable to its own systems in the last few years. However, ESA is not meant to define a Europe-wide cyber policy as it is not mandated by its Member States to frame security-related matters. Yet, given its experience, it might be the appropriate body to draft a set of general principles on space cybersecurity.

4. Rising stakes for Europe at multiple fronts

With the release of SPD-5, US companies and systems might get a competitive advantage on the market at the detriment of European industries/systems as they are taking the lead towards the definition of global standards. As a matter of fact, with the increasing number of attacks, cybersecurity is now a strong component of non-price competitiveness.

The EU and its Member States are dependent on vulnerable space systems. General space cybersecurity guidelines might urgently become a necessity as European stakeholders need to improve coordination and consistency. Also, European programs such as Galileo and Copernicus are now fully operational and essential to a number of EU policies. A cyberattack on one system could result in major economic loss, disturbances and increased security threats. An extensive policy on the matter might also boost the European cybersecurity industry whose promotion is a core objective of the 2013 EU Cybersecurity Strategy.

However, it remains to be seen to what extent a top-down policy similar to SPD-5 is feasible in the European current context. Security interests are part of EU space policies but priorities are predominantly on socio-economic benefits while security matters remain mostly addressed at the national level.

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

Short title: "ESPI Briefs" No. 44
Published in: September 2020

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