



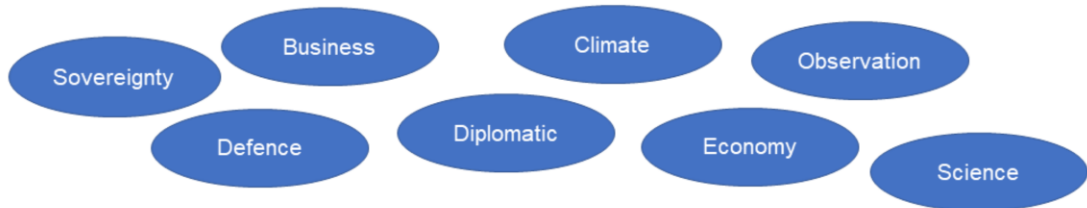
COMET Cybersecurity for Space systems operations

Day Introduction

Pierre Lods – Director of Security - CNES



Space as a critical sector



All our societies are dependent on space :

- ❖ A citizen uses in average 50 satellites per day (weather, GNSS, telecommunications)
- ❖ In 2018, in Europe, space industries generated 8,48B€ in sales and employed 45 000 FTE. Worldwide it was 261 B€, expected to be 2700 B€ in 2047.
- ❖ Considering this growth, space is evolving with new actors and systems to secure and operate.

Cyber context of space operations : “New” war zones

Space and cyber are far from being peaceful environments.



Many organizations have defensive and offensive capacities in both space and cyber environments.

How do space operators stand ?

But back to cyber, what is the context of space operations ?

What factors are impacting our field of operations ?

https://www.nato.int/cps/en/natohq/topics_110496.htm

Space, the new frontier

Space systems evolution is introducing new vulnerabilities...

- ❖ Supply chain complexity : many new actors, Commercial Off-The-Shelf.
- ❖ Convergence with operational technologies, automation, openness to the Internet, use of “cloud” services.

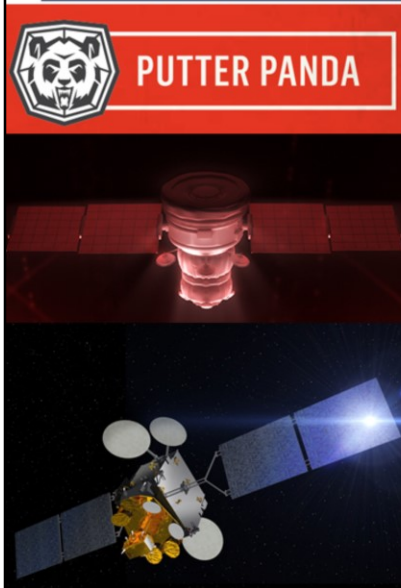
As security practitioner, we now face:

- ❖ Asymmetrical context:
 - threats with unlimited skills and means,
 - an increasing attack surface,
 - hard to protect systems.
- ❖ Unprecedented speed of attacks execution
- ❖ Unregulated space

Space, like any critical and competitive sector, became aware that time-to-market and production costs were a differentiator factor.

Space systems are more complex although this complexity aims at easing operations. Thus, they have increased surface attacks and could be considered in a way more fragile.

For the security practitioner, we face an asymmetrical context :



Space « Cyber » threats

Putter Panda (2014)

- ❖ Attributed to PLA Unit 61486 by CrowdStrike.
- ❖ Targets:
 - Space, satellite, and remote sensing technology (particularly within Europe);
 - Aerospace, especially European aerospace companies [...].

Turla group (2015)

- ❖ Used com-sat downlink hijack to hide command and control traffic from infected hosts to the attacker.
- ❖ Traffic was hidden in Middle East / Africa downstream Internet Service Provider

Luch-Olymp-K (2018)

- ❖ Conjunction with France-Italy military telecommunications GEO satellite Athena-Fidus.
- ❖ Qualified as « an act of hostile intelligence »

Articles :

Putter Panda :

Hat-tribution to PLA Unit 61486, <https://www.crowdstrike.com/blog/hat-tribution-pla-unit-61486/>, June 9, 2014, accessed 20190530

Turla :

Russian-speaking cyber spies exploit satellites, <https://www.kaspersky.com/blog/turla-apt-exploiting-satellites/9771/>, September 9, 2015, accessed 20190529

Satellite Turla: APT Command and Control in the Sky, Sephan Tanase,

<https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/>, September 9, 2015, accessed 20190529

Luch-Olymp-K

Cas du passé:

Last Call for SATCOM Security, IOActive, Ruben Santamarta, <https://ioactive.com/wp-content/uploads/2018/08/us-18-Santamarta-Last-Call-For-Satcom-Security-wp.pdf>, accessed

20190530

Prise de conscience

Viasat Exec on Cyber Threat to Satellite: We Must Take Action,

<https://www.satellitetoday.com/business/2018/12/11/viasat-exec-on-satellite-cyber-threat-we-must-take-action/undefined>, accessed 20190530

Satellite communications firms remain vigilant as cyber threats evolve, Debra Werner,
<https://spacenews.com/satellite-communications-firms-remain-vigilant-as-threats-to-their-satellites-networks-evolve/>, accessed 20190530

What's next ?

Let's talk about it today but :

- ❖ Embrace the convergence between Information Technologies and Operational Technologies (and discuss it at next COMET-CYB).
- ❖ Work together.
- ❖ Use standards and regulations opportunities to build strong and efficient security programs, to the service of OPS.
 - Evaluate and identify cyber risks, starting with threats.
 - Buy, build and operate secure technologies
 - Blend security in all missions during all their lifecycle.

