A Perspective on Cyber in Space for National Security

R. Mazzolin

Luxembourg, Feb 2019

NATIONAL SECURITY CONSIDERATIONS

- Space and Cyber are new strategic enablers for nations
- Key to national security – both military and economic
- Commercial and economic competition versus national interests
- Applicability to wide array of actors – state/non-state for variety of interests: economic, military, terrorist…

CYBER CONNECTION TO SPACE

- Space systems intrinsically part of cyber environment and subject to many of the same vulnerabilities
- Space is central part of critical national infrastructure
- Cyber threats are rapidly expanding – state/non state actors
- Wide range of motivations – socio economic, military, terrorist…
- Complexity of technology makes attribution difficult
- Progressive response methodologies required to enable the integrity of future societal initiatives.

CYBER THREATS TO SPACE SYSTEMS

- Cyber threats manifest themselves against Space systems through:
  - Jamming, Spoofing
  - Ground infrastructure supporting control, telemetry systems, launch and mission control
  - Deployed outer space satellite infrastructure
  - Kinetic and Directed Energy capabilities
  - Evolving protocols
  - Transfer across IP networks
  - Corporate supply chain
  - International challenges

MITIGATION

- Tailored Security Information and Event Management systems
- Evolving Defensive and Response techniques
- Cyber security risk assessments
- Progressive system design methodologies integrating security
- Quantum techniques
- National security policies
- Address inadequate international legal regimes
- International cooperation to develop flexible, multilateral space and cybersecurity regime

QUESTIONS

Robert Mazzolin

r.mazzolin@rheagroup.com

+1 613 222 6870