Paper ID: 78751
oral

56th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cybersecurity in space systems, risks and countermeasures (4)

Author: Mr. Shane Bennett
Australia, sbennett156@msn.com

DEVELOPING RISK BASED CYBER MISSION ASSURANCE ONTOLOGIES FOR SPACE LAUNCH MISSION SYSTEMS

Abstract

With the rising of New Space and the emergence of commercial space industry increasingly digital and data-dependent, the management of cyber-related risks and protection against cyberattacks has become a priority requiring the identification and deployment of relevant cybersecurity measures and solutions. The globalization of the space supply chain, the proliferation of small satellites using COTS com- ponents and the possibility to operate space mission payloads across networks through public internet connectivity substantially increase the vulnerability of space systems to cyber-attacks. As space assets continue to move towards the integration of more advanced information technologies such as software-defined radios, digital components, increased on-board processing and machine learning, the opportunities for cyber-attacks are inevitably bound to increase. Although cyber threats to space systems are not dissimilar to those faced by other Industries, systems and capabilities that rely on ICT to operate, manufacturers and operators of space infrastructure have not yet reached the level of cyber resilience of their "terrestrial" counterparts. This project is investigating cyber security risk management approaches to protect complex space launch systems and operations, to inform policy makers and inform government legal priorities as the Australian Sovereign space industrial complex grows and matures. This project also considers the economical constraints faced by new start-ups as they enter the field, how Australian industry engages in the broader international field and what ontologies, and standards need to be developed for the securing of space mission systems. On a broader level, the project outcomes will also inform regulatory agencies of other jurisdictions, reinforce cyber education programmes, and potentially training purposes.