Paper ID: 72684
oral

IAF SYMPOSIUM ON SECURITY, STABILITY AND SUSTAINABILITY OF SPACE ACTIVITIES (E9)
Cyber-based security threats to space missions: establishing the legal, institutional and collaborative framework to counteract them (2)

Author: Mr. Scott Schneider
Australia, scott.schneider@community.isunet.edu

INDUSTRY'S MANAGEMENT OF CYBER RISKS DURING LAUNCH ACTIVITIES UNDER LAW IN AUSTRALIA

Abstract

This paper examines the cybersecurity considerations of two Australian launch sites facilitating international space activities. The aim of the paper is to inform states and industry actors of the matters which must be taken into account when cyber security is included in the scope of a state's regulation of space activities. Australia is examined as a case study to demonstrate the concerns from an industry perspective against the known concerns of the state, and how launch site operators can manage both when carrying out their business. The paper discusses the nature of cyber security risks in the context of Australia's recent development of NewSpace launch capability. These observations are then discussed with consideration of Australia's laws governing the launches and return of space objects. As these laws are recent and largely yet to be applied in a consistent manner, the paper discusses how states may regulate particular security risks in a way which allows industry to most effectively manage those risks. The launch industry in Australia comprises of personnel and organisation with extensive experience in cyber security matters, including the prevention, monitoring and mitigation of risks. Upon a review of the nature of commercial launch activity in Australia, the paper discusses how the government may best harness the knowledge and expertise of industry members in ensuring threats are identified and to not eventuate. Examples drawn from previous and current activities in the Australian space launch industry demonstrate how the domestic launch site operators are able to implement secure strategies leading up to and during launch activities on the one hand, and what lessons can be learned for future operations with differing particulars which may be anticipated in Australia, on the other. The upcoming critical infrastructure regulations which Australia is imposing on industry is also discussed in this context. The paper concludes the Australian industry is so far able to effectively manage cybersecurity risks considering the nature of the risks and the expertise of the industry actors. Proposals are suggested for how domestic regulation can best facilitate industry in sustaining effective management of risks as the nature of cyber threats evolve.