Paper ID: 84931
oral
student

IAF SYMPOSIUM ON SECURITY, STABILITY AND SUSTAINABILITY OF SPACE ACTIVITIES (E9)
Interactive Presentations - IAF SYMPOSIUM ON SECURITY, STABILITY AND SUSTAINABILITY OF SPACE ACTIVITIES (IPB)

Author: Mr. Vinicius Guedes Gonçalves de Oliveira
Flinders University, Australia

SCRUTINIZING CYBERATTACKS IN THE FINAL FRONTIER: EVALUATING AUSTRALIA'S LEGAL AND POLICY READINESS IN SAFEGUARDING THE SPACE SECTOR

Abstract

The paper delves into the critical intersection of cybersecurity measures and the safeguarding of the Australian space sector. While the media often portrays Anti-Satellite (ASAT) attacks as the primary space threat, the paper contends that cyberattacks pose a clear and present danger. The vulnerability of space technology to cyber threats is exacerbated as advanced information technologies become integral to space assets. This vulnerability is particularly pronounced for nations heavily reliant on external Commercial off-the-shelf (COTS) components, as is the case with Australia. Against this background, firstly the paper demonstrates the main reasons that make cyberattacks such a dangerous attack vector for the space sector, by investigating its main advantages for attackers. By doing so, it analyzes the cost dynamics of cyberattacks, emphasizing their accessibility to a broad spectrum of actors. The discussion extends to the responsible use of counterspace weapons, considering the polluting consequences of other attack vectors to the space environment and highlighting the potential suitability of cyberattacks as a more controlled approach to space operations. Moreover, it explores the advantages of cyberattacks in terms of stealth and plausible deniability. The paper underscores the challenges of attribution in cyberattacks and discusses the reversible nature of cyberattacks, allowing attackers to remain under the threshold of open conflicts. Furthermore, the paper delves into the governance challenges posed by the argued global commons nature of both space and cyberspace, considering the limitations of domestic law in addressing issues that transcend national jurisdictions. Divergent perspectives on cybersecurity, particularly between Western and Sino-Russian blocs, that hinder the development of a cohesive international approach are also examined. Against this background, the final section evaluates the cybersecurity landscape within the Australian space sector. The paper highlights the rising cyber threats in Australia and the country's increasing dependence on space across various sectors. It examines Australia's existing cybersecurity legal and policy frameworks and their application to the space sector, emphasizing the need for a more mature intersection between space and cybersecurity governance. In conclusion, the paper underscores the imperative for Australia to develop a coherent governance structure that efficiently counteracts cyber threats. It advocates for a clear policy and legal framework catered for the cybersecurity of the space infrastructure, emphasizing the need for collaboration and international alliances to establish common principles and standards for securing space infrastructure against cyberattacks.