

52nd IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE  
ACTIVITIES (D5)

Cyber-security threats to space missions and countermeasures to address them (4)

Author: Dr. Joel Scanlan  
University of Tasmania, Australia

Mr. Jarrod Styles  
Australia

Mr. David Lyneham  
Australia

Prof. Margareta Holtensdotter Lützhöft  
Norway

NEW INTERNET SATELLITE CONSTELLATIONS TO INCREASE CYBER RISK IN ILL  
PREPARED INDUSTRIES

**Abstract**

The deployment of the Starlink, OneWeb and LeoSat satellite constellations will have a transformative impact on the availability of the internet globally. The existing satellite delivered Internet access from providers are operated from geostationary orbit resulting in high latency connections, with limited bandwidth. The recently completed the Iridium Next constellation is comprised of 66 satellites in LEO and provides a maximum speed of 1.5Mbit/s bandwidth. This bandwidth is a fraction of the 100s Mbit/s and Gbit/s speeds within the proposed constellations of OneWeb and SpaceX, each containing hundreds, up to thousands, of satellites. These offerings promise global access, with low latency and high bandwidth. These platforms will be transformative in their impact on global access to internet, with many unforeseeable positive and negative outcomes.

This paper will discuss what it suggests is a likely increase in cyber-attacks on ill-prepared industries due to the rapid adoption of highspeed Internet delivered through these proposed constellations. The industries we suggest are most at risk are those which are geographically dispersed and unable to currently attain reliable and fast Internet access and have existing legacy software systems with poor security. This will be explored within the context of the maritime and offshore industries as a case study, since they currently make use of the existing limited satellite connections for non-mission critical tasks but are looking to transition to shore-based control and increased automation of shipboard systems. The industry has not formerly been at great risk from cyber-attack due to geographic isolation and limited connectivity to the systems. However, the satellite constellations will enable them to have fast, high bandwidth connections, nearly anywhere on the globe. There are a range of industries, or at least segments within industries, that are ideally suited to utilise these new platforms that formerly did not need to be responding to cyber-attacks, and as such do not have a strong security design culture. These will be contrasted to the much better-prepared networks, such as stock exchanges, that have been spoken of by providers as being an ideal use case.

This risk is not the responsibility of the Internet providers, who in this case are the companies building these expansive constellations. However, it may be in their best interest to work to raise awareness among prospective clients in non-traditionally connected industries.