Paper ID: 55067
oral
student

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: Mr. Scott Millwood
Germany, scott.millwood@gmx.de

WHAT SPACE MISSIONS CAN LEARN FROM CYBER-SECURITY BREACHES AND COUNTER-MEASURES IN THE TELECOMMUNICATIONS INDUSTRY

Abstract

As the internet evolved from a network of routers, Telecommunication companies became providers of our global infrastructure backbone. They also became the number one target of cyber-security attacks, attracting double the annual Distributed Denial of Service (DdoS) attacks of the number two target,financial institutions. The author leverages two decades of experience working with Telcommunications infrastructure across the EU and APAC regions, to undertake original research with the Chief Security Officers (CSOs) of the world's leading Telcos. In interviews with CSO's of ATT, China Telecom, Megafon, Deutsche Telekom, Telstra Corporation,Telia Company, Orange and British Telecom, the author investigates the circumstances in which cybersecurity breaches have penetrated core telecommunications infrastructure during the last decade and the counter-measures Telcos have taken in response to increasingly sophisticated attacks. This qualitative research forms the basis of a presentation of "insider insights" from the Telco industry made applicable to space. It highlights the technical vulnerabilities created by the rise of connectivity, cloud-based Infrastructure-as-a-Service (such as SaaS, StaaS, BaaS, BPOaaS) and IoT. It highlights the role of cost-cutting outsourcing which has seen major infrastructure build, management and support functions contracted to third parties who in turn sub-contract further, creating multiple layers of thirdparties. The CSOs highlight the tendency of security breaches to occur in the supply-chain indicating the vulnerabilities that have arisen where Telcos lose line-of-sight and control over their own networks. For all the sophistication of the network, human error remains a major vulnerability in our systems. The space industry faces convergence on a number of Levels: between infrastructure supported by national space agencies and private players; between military and civil purposes; between space-based and terrestrial infrastructure. This paper represents an opportunity to share "lessons learned" in the Telco sector with the space industry. The author proposes legal and technological solutions to mitigate risks of cyber-security attack, while outlining counter-measures the Telco industry has found successful. (Note the author is the former Chief Privacy Officer and legal counsel of the Swedish-Finnish Telco Telia Company and former legal counsel at Australia's Telstra Corporation. Currently studying Space Law at the Institute of Air and Space Law, Leiden University. This paper, which was originally scheduled to be presented at IAC2018 in Bremen (but was withdrawn as the Research had taken considerably longer than anticipated), has now progressed to a stage where it can now be presented at IAC2019.