Paper ID: 53171
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: Ms. Maria Lucas-Rhimbassen
Université de Toulouse 1 Capitole, France

Dr. Cristiana Santos
Université de Toulouse 1 Capitole, France
Prof. Lucien RAPP
University of Toulouse I (UT1), France

BREAKING THE GOLDEN CHAIN OF TRANSPARENCY: CROSSLINKS BETWEEN CYBER THREAT AND BLOCKCHAIN WITHIN SPACE AND GOLD INDUSTRIES

Abstract

Currently, the supply chain in the space industry is under pressure (e.g. COTS). The economic situation results in an exacerbated pressure on outsourcing and subcontracting, whereby the supply chain could lose control (The Big Hack, Bloomberg, October 2018). The international scene is being shaken by trade war, and economies are turning towards gold in an era of slowbalisation. In this paper, we address the escalation of cyber threat in the space industry by studying other industries' deterrence efforts. We will particularly regard the lessons drawn from the gold market. We posit that transparency capabilities derived from blockchain technology can be modeled within this scenario. Herewith, our proposal includes blockchain, especially when cyber gold transactions will increase at high trading speed via satellites. Firstly, we will assess the impact of the gold industry and convey its effects on the space industry. Our recommendations will be of strategic essence, based on new competition policy shifts. We will then regard the effect of the twofold blockchain forces: democratisation vs cartelisation. For this reason, we will look into several supply chain cases and business models, assessing cyber vulnerability cases and analyse how blockchain will prove (or not) as a transparent solution in the competitive and strategic space supply chain industry. From our analysis, we anticipate that pros include transparent monitoring of the supply chain. Cons include technological vulnerabilities to hacking in chain reaction (e.g. smart contracts.), quantum computing. We further state blockchain can also trigger legal debate surrounding collusion and cartelisation, since sharing data on blockchain in different public/private channels might lead to cartelisation. Conversely, the 2018 OECD report qualifies the blockchain as a solution to antitrust, which today remains unpredictable and "obsolete" (e.g. Alstom/Siemens case in Europe), but yet crucial to space accelerations (e.g. launchers race), and leaves the supply chain at the mercy of trade war. In our discussion, we set forth that blockchain could disrupt the space industry. In this juncture, we devise a link between the three major States involved in cyber threat, and the three major gold producers, namely China, Russia and the US, which incidentally are leading spacefaring nations. The paper acknowledges that converging these countries on a new dialogue, based on blockchain transparency, might contribute with the following: disrupt forces of multilateral and intensified competition; reshape supply chain dynamics; and scale down the threat of cyber warfare, all in space and time, block by block.