Challenges in Cybersecurity for Long-Duration Robotics and Human Exploration of the Moon and Mars

John Kwok and Alex Cervantes

As the prospects of long-duration robotics and human exploration of celestial bodies such as the Moon and Mars become increasingly plausible, the significance of robust cybersecurity measures cannot be overstated. This abstract delves into the unique challenges that arise in the realm of cybersecurity, particularly concerning uplink and downlink operations, and presents potential roles for public governments/nations versus the private sector in addressing these challenges.

Exploring the Moon and Mars requires the establishment of complex communication networks between Earth-based control centers and remote mission locations. The constant flow of critical data via uplink and downlink channels exposes these missions to various cybersecurity threats. One primary challenge is the vulnerability of these communication links to interception, unauthorized access, and data tampering. Protecting the confidentiality, integrity, and availability of mission-critical information becomes imperative to prevent potential sabotage, unauthorized control, or espionage by malicious actors.

Furthermore, the long duration of these missions amplifies the challenges of maintaining cybersecurity over extended periods. The evolving threat landscape demands continuous monitoring, threat intelligence updates, and adaptive security measures to safeguard mission operations. The inherent limitations of space-based systems, including constrained resources, limited computing power, and high latency, present additional obstacles to implementing comprehensive cybersecurity measures.

In addressing these challenges, a collaborative approach between public governments/nations and the private sector becomes essential. Public governments/nations can play a vital role in providing overarching cybersecurity frameworks, regulations, and standards that ensure the security of space missions. They can establish international agreements to foster cooperation, information sharing, and joint efforts in combating cyber threats in space exploration.

Simultaneously, the private sector can contribute expertise and innovation to develop cutting-edge cybersecurity technologies tailored for long-duration missions. Private entities specializing in cybersecurity can partner with space agencies to develop secure communication protocols, encryption techniques, intrusion detection systems, and anomaly detection algorithms. These collaborations can foster the integration of best practices from both sectors and promote the resilience of space missions against emerging cyber threats.

To conclude, the challenges in cybersecurity for long-duration robotics and human exploration of the Moon and Mars demand comprehensive measures to protect critical mission operations. Uplink and downlink operations require secure communication channels to prevent unauthorized access and data tampering. Public governments/nations should establish regulatory frameworks, while the private sector can contribute expertise and innovation. Collaboration between these stakeholders is crucial to mitigating cyber threats and ensuring the succes

John Kwok and Alex Cervantes are with the Jet Propulsion Laboratory, California Institute of Technology, 4800 Oak Grove Drive, Pasadena, CA 91109, USA