48th 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. Deborah Housen-Couriel
Tel Aviv University, Israel

INTERNATIONAL COOPERATION IN RESPONDING TO CYBERSECURITY THREATS TO SPACE MISSIONS: TOWARDS A TYPOLOGY OF COUNTERMEASURES

Abstract

Cybersecurity threats to space missions are a relatively new phenomenon, yet have quickly come to the forefront of concern for the sustainability of missions due to the vulnerabilities that such threats may exploit and negatively impact. These vulnerabilities are liable to be mission-critical, including launch systems, communications, telemetry, tracking and command, and mission completion. These and other aspects of space missions depend on secure, consistent and resilient cyber capabilities. Due to the global nature of both cyberspace activities and cybersecurity, these capabilities rely on international cooperation for setting a baseline of agreed cybersecurity levels with respect to space missions. This concern is relevant during all mission phases, from planning stages to final wrap-up. Under optimal circumstances, the norms and standards of cybersecurity are developed and enforced by both nation-state actors and non-state actors, including companies, which are committed to mission's success. When breaches of cybersecurity do occur in the form of hostile cyber events, international law determines a range of countermeasures (defined as reprisals in response to intentionally illegal acts, and not involving the use of force), as legitimate responses on the part of states. For instance, a hostile disruption to a TT&C communication from earth to a space object may cause a change of course, thereby endangering it and other space objects. This is an especially compelling cybersecurity issue, involving questions around the extent to which a virtual act (such as a false TT&C communication) may be considered a use of force. If so, it may violate the UN Charter's collective security regime, prompting a state's right to self-defense. This presentation proposes an analysis of the countermeasures available under international law in response to hostile acts impinging on space missions' cybersecurity. The typology of these countermeasures ranges from mild to severe, commensurate with the damage inflicted. Three normative regimes influence the types of countermeasures that may be undertaken: space law (governing the launching of objects and their space activities, including damage liability); global telecommunications law (governing transmission of data between earth and space); and the substantive law regarding freedom of information). The proposed typology takes these regimes into account, categorizes the threats to cybersecurity and the possible responses thereto, and provides a framework for effective cooperation under international law in responding to cybersecurity threats to space missions.