Paper ID: 28658
oral

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: Mr. Ram Levi
Tel Aviv University, Israel, ramlevi@gmail.com

CYBERATTACK OF SPACE SYSTEMS - INSTRUMENTS OF DENIABLE ACTION

Abstract

IAF 2015 Abstract

Satellites systems are indispensable both for military and civilian uses. As a result, weapons against space systems are a reality and a concrete strategic concern. Strategic threats to satellite systems and computer systems have long been researched as separate subjects. However, the close relationship between them requires an examination of the nature and extent of their influence on each other.

Cyberattacks against satellite systems are computer–based attacks aimed at damaging a satellite system or the service provided by the system. The main argument of the paper is that cyber-attack against a satellite system (rather than on the satellite itself) is possible because the components of the satellite system are depended on computers and thus vulnerable to cyber-attacks. Furthermore, without the possibility of attribution the attacker can achieve devastating effects, not having to pay the strategic price of attacking a satellite. This option is embodied in cyberattacks as they are inherently instruments of deniable actions.

There are many possible ways to attack space systems using cyber-attacks such as: implanting malware during system production, counterfeit chips with embedded software backdoors to allow access to in-orbit satellites, attacks on computers in ground station to gain control over the satellite or denial of services attacks on satellite system architectures. Cyber-attack against a satellite system (rather than on the satellite itself) is possible because the components of the satellite system are depended on computers and thus vulnerable to cyber-attacks. Furthermore, without the possibility of attribution the attacker can achieve devastating effects, not having to pay the strategic price of attacking a satellite.

There are very few incidents of cyber-attacks on satellites such as the alleged cyber-attack against the ROSAT satellite in 1998 and large- scale hostile activities that compromise computer networks in space agencies that have the potential to severely cripple operations. Hence, despite the fact that there is some debate over the depth of the threat to satellite systems from cyberattacks, the threat itself is real.

The paper will review the potential emerging cyber threat against space systems, describe basic attack vectors, explore the differences between information security and cyber security and their contemporary relevance, provide case studies of major attacks against critical infrastructure and command and control systems, highlight the similarities between space and cyberspace, provide knowledge about known attacks against space systems and space agencies computers and discuss measures that need be taken to reduce the potential threat.