IAF SYMPOSIUM ON SPACE SECURITY (E9)
Cyber-based security threats to space missions: establishing the legal, institutional and collaborative framework to counteract them (2)

Author: Ms. Laetitia Zarkan Cesari
University of Luxembourg, Luxembourg , laezar@protonmail.ch

Dr. Nebile Pelin Mantı
Space Generation Advisory Council (SGAC), Türkiye, np_manti@yahoo.com
Mr. Antonio Carlo
Tallinn University of Technology, Estonia, ancarl@taltech.ee
Mrs. Lucille Roux
Belgium, rouxlucille7@gmail.com
Ms. Rania Toukebri
DSI Aerospace Technologie GmbH, Germany, rania.toukebri@spacegeneration.org

SPACE AS NATO'S OPERATIONAL DOMAIN: THE CASE OF THE CYBERTHREATS AGAINST GNSS

Abstract

In the last decades, modern society has become growingly dependent on new technological and digital domains. In this view, the North Atlantic Treaty Organization (NATO) identified and defined two areas, first cyber and subsequently space, as operational domains alongside land, sea and air.

Such development reflects the threat landscape that stems from a society more dependent on technological solutions, where space and cyber may have a prominent role in future conflicts. Currently NATO is developing rules on engagement for cyber attacks and attacks against space assets. At the same time, NATO explores the potential of space capabilities during a conflict and prepares for preventing adversaries from doing the same, which is critical to the success of military operations. A hostile act carried out against a satellite system could have widespread consequences. If there is a 'strike' in cyberspace, it would be most likely against a strategic system providing an important service used during conflicts. In this paper, Global Navigation Satellite System (GNSS) is identified as the most critical space system that could be subject to a cyber threat.

NATO does not have its own space capabilities and relies on the members of the alliance to provide access and information. Given the growing importance of space technology and of its protection against cyber risks, NATO's role with regard to national divergent interest shall be analysed. Within its framework, there is still more to be done in terms of coordinating efforts and designing resilience strategies against future threats. Against this background, NATO's response to cyber threats against space systems will be examined using as a reference NATO's conduct in other operational domains.

The paper will examine what legal and policy repercussions could follow from the loss of GNSS signal, whether for a limited time or prolonged period. It will conclude that the recognition of space and cyber as operational domains is a step toward preparing NATO for threats and possible competitors. It will also suggest strategies for building defences for the intersection of these domains, taking into account the provisions of the North Atlantic Treaty and other relevant instruments of the Organization.

Please note that the present abstract is submitted under the auspices of the Space Generation Advisory Council, as part of the activities of the Space and Cybersecurity Project Group.