

61st IISL COLLOQUIUM ON THE LAW OF OUTER SPACE (E7)
Integrated space applications, EO telecoms navigation (3)

Author: Ms. Sandra Cabrera Alvarado
University of Luxembourg, Luxemburg, sadalbaris@yahoo.com

COPERNICUS AND EUROPEAN SPACE SECURITY: LEGAL CHALLENGES WITH OPEN DATA
POLICIES

Abstract

The European Union and accompanying institutions are increasingly interested in investing in space assets because space-based technologies serve as a useful tool in fulfilling public policy mandates such as security policies. For instance, the Copernicus Programme, as a European Earth observation programme assists European environmental and security policies supporting with border security (Frontex) and the European Maritime Security Agency in border surveillance and coastal monitoring. Specifically, the Copernicus open data policy provides access to information in a [potentially] non-restrictive manner with free access to registered users worldwide. This accessibility to information could present a major concern to Member States who may consider such information and remote sensing data access to information as a possible threat to their national assets and interests. While the Copernicus Regulation stipulates a full Chapter on data and security policies to reassure Member States, the fact remains that open data practices here present inescapable risks, particularly in regards to disruption of data, security in management of processed data, storage, service and/or software disruption. This last case was already seen in the GPS software bug detected on GPS satellite SVN-23 in 2016, which was at the end of life. It triggered only a small delay on the rest of the constellation once the satellite was turned off, yet still causing some collateral damage on Earth. Consequently, even though EO and GNSS are different space technologies, both inevitably remain vulnerable and subject to disruptions. In regard to Copernicus, ESA maintains an obligation to exercise best efforts to ensure a resilient space segment, including a resilient data management service to guarantee the security of Copernicus services and its data. This paper will highlight the pertinent and potential legal challenges to open data policies and practices with specific focus on the security interests of EU Member States and the participants of Copernicus.