

IAF SYMPOSIUM ON SECURITY, STABILITY AND SUSTAINABILITY OF SPACE ACTIVITIES
(E9)Interactive Presentations - IAF SYMPOSIUM ON SECURITY, STABILITY AND SUSTAINABILITY
OF SPACE ACTIVITIES (IPB)

Author: Ms. Denitza Petrounova
University of Vienna, Austria, a00867828@unet.univie.ac.at

CYBER ATTACKS AGAINST SPACE ASSETS: THE RIGHT TO SELF-DEFENCE

Abstract

Cyber attacks against military, civilian or dual-use space assets – primarily satellites – take place off-planet, and not only in futuristic action films but in our current reality – and also at an uncomfortable and unforeseen intersection of space law, cyber law, the law of armed conflict and general international law.

Critical questions arise and exacerbate daily as the international security situation deteriorates, and at the same time the interdependency of space and cyber systems nears a point of mutual inextricability. These questions range from the most basic premises of what the applicable law is, to general doubts on where the threshold of armed attack lies, to downright dramatic questions of self-defence.

Considering the cyber attack which took place on 24 February 2022 against a satellite telecommunications service provided by a U.S. company in the Ukraine, formally attributed to the Russian Federation by the EU, one can ascertain multiple “victims”: Ukrainian military communications, a U.S. company as the owner, France as the state of registration of the satellite, users in several other countries, and thousands of wind turbines in Germany. Which of these states has the right to self-defence? The surprising answer *de lege lata* appears to be France, and this is also France’s opinion as expressed in its new national manual on the law of military operations. But is this answer adequate?

What of the requirements under which a state may react to an attack against privately owned assets belonging to a company under its jurisdiction? What if a satellite is also critical infrastructure? Who gets to decide on applicability, definitions and reactions?

An attempt to highlight these and related questions at a point of complex interplay of legal regimes, systematise the problems and suggest some solutions shall be made on the basis of existing law, while keeping in mind that at the rapidly evolving technological and scientific frontiers international law is deeply unsettled, and states (or military alliances such as NATO) may be likely to decide on a response before they design their legal justifications and without committing to clear definitions or a single legal approach in a deliberate choice for strategic ambiguity.