Paper ID: 44043
oral

61st IISL COLLOQUIUM ON THE LAW OF OUTER SPACE (E7)
The relationship between space law and cyberlaw, and other recent developments in space law (5)

Author: Dr. Roy Balleste
St. Thomas University School of Law, United States, rballeste@stu.edu

RECONSIDERING RULES OF ENGAGEMENT IN OUTER SPACE

Abstract

Similar to human existence, those tackling the challenges associated with cyberattacks in outer space have reached a crossroads. If cyberspace is going to be considered another theater of combat, then all humanity shares a challenge and a duty as a sentient species to at least mitigate any collateral damage. The goal of this presentation and paper will be motivated by the law governing space activities, and the relationship between space law and cyberspace law. The paper will be concerned with the expansion of human conflicts into outer space, while focusing on the dangers of anti-satellite weapons, and in one weapon in particular: cyberspace. Large-scale cybersecurity threats overshadow the space activities of governments and corporations. Cyber threats and attacks are launched with high sophistication causing great damage. Acts of aggression in cyberspace are elusive and so far have escaped the classification that would label them 'actions within the domain of war.' Whether it involves the use of malicious code or involves State-sponsored activities, these cyberattacks threaten the vulnerabilities found in the supervisory control systems, and also threaten to disrupt satellite transmissions, while inflicting terrible damage on adversaries. Given the nature of cyberspace, questions remains about what should be the limit and consequences of State-sponsored activities that may threaten the peaceful utilization of outer space. In this context, the presentation/paper will be divided into a three part methodology. Part One will introduce the cyber landscape of outer space, the methodology, and historical considerations. Part Two will discuss the policy and sources of law associated with the crossroads of cyber and space. Finally, Part Three will survey anti-satellite weapons, defines them, appraises their use in light of present space activities, and center on the utilization of cyberspace in relation to those activities. The basic criterion by which stakeholders must be guided is the recognition that for a profitable and secure management of satellite technologies and space exploration, there needs to be a definition for outer space cybersecurity risks. The end result of the analysis is one that assumes that the inhabitants of planet Earth will survive their "technological adolescence" and will not destroy themselves. The final result presents two suggested rules of engagement applicable to cyber operations related to space activities. An overriding preference must certainly be that rules should be made for the protection of the peaceful enjoyment of outer space—activities that are now in danger of suffering the effects of cyberattacks.