Abstract

Cyber attacks can target any nodes of the space infrastructure, and while these attacks are called non-violent, there is a credible capability to use cyber attacks to cause direct or indirect physical damage, injury or death. However, the vulnerability of satellites and other space assets to cyber attack is often overlooked, which is a significant failing given society's substantial and ever increasing reliance on satellite technologies. Through a policy analysis, this dissertation assess the set of political provisions provided by the European Union to address the cyber security issue of the space infrastructure.

Such study aims at exploring the geopolitical consequences linked to space cyber security risks, and at assessing the political preparedness of the European Union to address these challenges. The perspective of transatlantic cooperation to further support both American and European effort to tackle this security risk is also addressed. The overarching value of the study is to contribute to future European cyber security for space and transatlantic debates by providing useful perspectives and key takeaways on these two domains.

Ultimately, he existing set of policies are not sufficient to address the cyber security issue in Outer Space, a unified approach by the European Union and the United States could improve information-sharing and the capacity to respond quickly attacks, strengthening cybersecurity across Europe, and throughout the international scene.

Keywords: space security, cyber attacks, European Union, United States, transatlantic, policy analysis, NIS Directive, Cyber Diplomatic Toolbox, NIST Cybersecurity Framework, human security.