BUCERIUS LAW SCHOOL
HOCHSCHULE FÜR RECHTSWISSENSCHAFT

Active Cyber Defense under International Law

Yasir Gökce

Contact: gokceyasir@gmail.com

Supervised by: Prof. Dr. Mehrdad Payandeh, LL.M., Chair of Public Law II - International Law, European Law and Public Law

Abstract

The internet, the connectedness that it brings and the increasing use of information technologies expose assets to new threats, risks and challenges and generate new vulnerabilities against asset owners. An increasing number of States has begun to explore ways to exploit or leverage these vulnerabilities in ways that maximize their respective interests. This relatively new phenomenon has allowed the conduction of the traditional rivalry/hostility characterizing today's reelpolitik in cyber space.

In response to the threats and challenges emerging from cyber domain, States have begun adopting measures to improve their national cyber defenses and reviewed their cyber policies and programs accordingly. States have thereby incorporated active elements in their cyber defense strategies which envisage engaging with the adversary through limited offensive capabilities such as preventive and preemptive strikes or hack backs. Taking into account the ever-increasing use of Active Cyber Defenses (ACDs) by States and/or incorporation thereof in national strategy documents, this study has addressed the legal issues arising from the adoption and employment of ACDs under international law. It has enquired the applicability of the traditional concepts of international law, such as the right to self-defense, the non-intervention principle or the use of force, to cyber space. It has revealed the aspects of the use of cyber operations in general and ACDs in particular, which appear to be problematic under international law and thereupon focused on the ways in which ACDs can be devised and employed in consistent with international law. All in all, the study has demonstrated that, just like in land, sea and air, cyber space is a domain where international law stands valid and that cyber operations in general and ACDs in particular can be designed and used by States in accordance with international law.

In this study, countermeasures taken in response to internationally wrongful acts were identified as a ground precluding the wrongfulness of ACDs if employed in line with the restrictions envisaged by the law governing countermeasures. It has been furthermore concluded that a State is entitled to invoke ACDs amounting to the use of force within the framework of self-defense if it becomes the target of an armed attack. Disruptive and destructive ACDs have been identified as the ones which might be employed, in terms of their 'scale and effects', as potentially forcible cyber operations in response to an armed attack, whether

cyber in nature or not. Besides, anticipatory self-defense has been highlighted as a potential legal ground which would preclude the wrongfulness of an ACD that meets the threshold of the use of force. Finally, the study has established that international human rights law can be implicated by ACDs. More precisely, ACDs which constitute interference with human rights might still be in consistent with international human rights law, provided that they are in line with certain limitations that are necessary to achieve a legitimate purpose, nondiscriminatory, proportionality and authorized by law.