NEW IHL FRAMEWORK FOR CYBER WARFARE - ABSTRACT

Regarding the increasing number of revealed cyber-attacks aimed at public facilities including the governmental ones by who seems to be other state actors, this thesis aims to reveal the major importance of cyber warfare, point out the fatal vacuum regarding the IHL framework currently in force and suggests its completion by a new IHL convention, which would regulate cyberwarfare in International Armed Conflicts.

In order to provide a well-structured and pertinent arguments to support its main points, the thesis uses methods of qualitative analysis of the current IHL sources including international treaties, customary law and work of the main institutions of international justice along with work of judicial scholars and cyber experts.

The work contains five main chapters. The first chapter presents the underlining principles of Laws of Wars, including its theory, history and development; and focuses on one of its three main regimes – the International Humanitarian Law.

The second part is dedicated to the topic of cyber warfare, defines its scope as computer network attacks, explains their classification system, analyses their effects and provides examples of such attacks.

The third chapter focuses on the issue of the current legal vacuum in relation to cyber warfare and delivers a critical analysis of the most severe drawbacks to possible solutions of the vacuum.

The fourth part presents the insurmountable differences between the traditional kinetic warfare and cyber warfare and explains why these differences make the current IHL framework truly incompatible with cyber warfare in practice.

The last part of the thesis suggests a solution to the issue of incompatibility of the current IHL provisions and cyber warfare in a form of a new IHL treaty dedicated to cyber warfare and provides a draft of its main points so that future cyber conflicts can be evaluated and judged according to the updated IHL framework, which would correspond to its era.