

## **Abstract**

### **Application of international humanitarian law on cyber military engagement**

The subject of interest of this master thesis with the name *Application of international humanitarian law on cyber military engagement* is a critical assessment of possible applicability of the contemporary norms of international humanitarian law in cyber space. War-like activities in cyber space are unfortunately nowadays reality, therefore it is more than desirable to subject this thesis about the applicability of the international humanitarian law, which is hold by the majority of the international community, to the real analysis. The research question is not only whether international humanitarian law is applicable on cyber military engagement but also into what extent.

The master thesis consists, except for introduction and conclusion, of four chapters. The first chapter is focused on fundamental characterization of international humanitarian law and brief development with a special focus on the development of warfare as a prerequisite to the militarization of cyber space. The following chapter defines concepts connected with cyber space in order to be further used in accordance with those definitions. The main part of this master thesis is the analysis of the applicability of the fundamental principles of international humanitarian law on cyber military engagement and the notice concerning selected problematic aspects of the transfer of existing norms of international humanitarian law into cyber space. The fundamental principles, which are applied on cyber operations, are the principle of necessity, humanity, distinction, proportionality and prohibition of unnecessary suffering. It appeared that principles of distinction and prohibition of unnecessary suffering are in today's state of technologies translated into cyber space with great difficulties. The last chapter focuses on selected problematic issues of applicability of international humanitarian law which is the vocation of authorship of cyber operation, territorial limitation of these operations, increased participation of civilians and its contribution to cyber operations and last but not least the possible decrease of protective possibilities of international humanitarian law in cyber space especially in relation to health-care providers.

Past cyber operations serve as examples, such as DDoS attack against Estonia in 2007, cyber operation against Georgia in 2008 or attack of ransomware WannaCry in 2017. Although international humanitarian law was not as of now applied in practice on cyber operations it is without doubts that such activities are the reality of today's world.