

Abstrakt

Aplikace mezinárodního práva na kybernetické vedení boje

Předmětem zájmu této diplomové práce s názvem *Aplikace mezinárodního humanitárního práva na kybernetické vedení boje* je kritické posouzení možností aplikovatelnosti současných norem mezinárodního humanitárního práva v kybernetickém prostoru. Válečné aktivity v kybernetickém prostoru jsou bohužel realitou dnešní doby, tudíž je více než žádoucí podrobit tezi o aplikovatelnosti mezinárodního humanitárního práva, kterou zastává většina mezinárodního společenství, reálnému rozboru. Výzkumnou otázkou tedy není pouze, zda je mezinárodní humanitární právo aplikovatelné na kybernetické vedení boje, ale také do jaké míry.

Diplomová práce se kromě úvodu a závěru skládá ze čtyř kapitol. První kapitola se věnuje základní charakteristice mezinárodního humanitárního práva a stručnému vývoji, se zaměřením na vývoj válečnictví jako předpokladu pro militarizace kybernetického prostoru. Následující kapitola definuje pojmy spojené s kybernetickým prostorem, aby byly dále v souladu s těmito definicemi používány. Stěžejní část diplomové práce tvoří rozbor aplikovatelnosti základních principů mezinárodního humanitárního práva na kybernetické vedení boje a upozornění na vybrané problematické aspekty přenosu existujících norem mezinárodního humanitárního práva do kybernetického prostoru. Základními zásadami, jež jsou aplikovány na kybernetické operace, jsou zásada vojenské nutnosti, humanity, rozlišování, přiměřenosti a zákazu zbytečných útrap. Ukázalo se, že zásady rozlišování a zákazu zbytečných útrap jsou do kybernetického prostoru za současného stavu technologií jen těžko přenositelné. Poslední kapitola se zaměřuje na vybrané problematické okruhy aplikovatelnosti mezinárodního humanitárního práva, a to určení autorství kybernetické operace, teritoriální limitace těchto operací, zvýšení účasti civilistů a jejich podílu na kybernetických operacích a v neposlední řadě možné zmenšení ochranných možností mezinárodního humanitárního práva v kybernetickém prostoru, především ve vztahu k nemocničním zařízením.

Jako příklady jsou užívány proběhnuvší kybernetické operace, jako například DDoS útok na Estonsko v roce 2007, kybernetická operace vůči Gruzii z roku 2008 či útok ransomware WannaCry v roce 2017. Přestože dosud nebylo mezinárodní humanitární právo na kybernetické operace aplikováno, je nepochybné, že takové aktivity jsou realitou dnešního světa.