Abstrakt

Diplomová práce se zabývá především zmapováním cílů, motivací, nástrojů a důsledků současných kybernetických válek. V prvé řadě se zaměřuje na charakter kybernetických konfliktů, identifikuje a definuje podstatu kybernetického terorismu; jeho principy, příčiny a hrozby. Kromě popisu obecných metod kybernetického boje klade také důraz na podrobnou analýzu konceptu „Information Assurance," který představuje druh strategie, užívané za účelem definice rizik informační bezpečnosti v kyberprostoru. Analytická část práce se věnuje konkrétním případům mezinárodního kyberterorismu a jeho jednotlivým formám v kybernetických střetech mezi lety 2007 a 2010. Z geopolitického hlediska chronologicky analyzuje jednotlivé kybernetické útoky, k nimž došlo v oblasti evropsko-ruské, asijsko-americké a na Středním východě. Z komparace teoretického modelu „Information Assurance" a dílčích analýz jednotlivých příkladů kybernetických válek tak vyplynulo, že nedodržení tohoto modelu v praxi má za následek narušení informační bezpečnosti daného systému, což v uvedených případech výrazně přispělo ke vzniku kybernetických konfliktů, čímž byla potvrzena platnost a použitelnost konceptu „Information Assurance" při zabezepečování informačních systémů.