Abstrakt

Tato diplomová práce představuje komparaci strategií kybernetické bezpečnosti Spojených států amerických a Spojeného království. Čím vyspělejší společnost je, tím větší bývá její digitalizace a závislost na kyberprostoru. Vzhledem k této závislosti jsou státy mimořádně náchylné k interním či externím kybernetickým útokům a útokům na jejich informační systémy. Vytváří se tím zcela nová zranitelná místa, jak pro státy jako takové, tak pro celou společnost. Tato práce blíže představuje a komparuje mechanismy institucionálních reakcí obou států v případě kybernetického incidentu. Tyto mechanismy jsou přiblíženy jak na pozadí historického vývoje kybernetických strategií, tak i demonstrovány na vybraných kybernetických incidentech. Jak Spojené státy, tak Spojené království využívají jako hlavní mechanismus zvládání kybernetických hrozeb metodu cyber detterance, která byla použita i při zmíněných útocích. Práce si klade za cíl přiblížit účinnost této strategie a zasadit jí do kontextu strategie kybernetické bezpečnosti. Ukazuje se, že ač by přístup cyber detterance měl být nedílnou součástí strategie kybernetické bezpečnosti každého státu, bylo by vhodné věnovat zvýšenou pozornost i ostatním přístupům a rovněž přípravám i ofensivních kybernetických strategií.