ABSTRAKT

Internetová a počítačová kriminalita je součástí kybernetické kriminality, což je značně široká a poměrně nestejnorodá skupina trestných činů. Diplomová práce se zaměřuje na trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů. Tyto kybernetické útoky mohou ohrozit kybernetickou bezpečnost na úrovni státu a způsobit nedozírné škody. V současné době je v České republice připravován zákon o kybernetické bezpečnosti, jehož cílem je reagovat na tyto útoky. Diplomová práce zkoumá zejména trestněprávní aspekty tohoto zákona. Velký prostor je v práci dále věnován nedávno ratifikované Úmluvě o počítačové kriminalitě.

Kromě zmíněných dvou právních norem diplomová práce vychází z právních předpisů a rozhodovací praxe české i zahraniční, k čemuž využívá odborné literatury dostupné v českém, anglickém či německém jazyce. S ohledem na zvolené téma bylo nutné využít též značné množství neprávní literatury.

Celá práce je rozdělena do šesti kapitol. První kapitola předkládá krátký úvod do tématu a též stručné vysvětlení základních pojmů. Kapitola druhá klade otázky ohledně oprávněnosti a užitečnosti státní regulace v kyberprostoru, které jsou částečně filosofické povahy. Tato část též popisuje specifika v kyberprostoru, která je třeba vzít v úvahu při posuzování kybernetické kriminality, stejně jako před prováděním zákonné regulace kyberprostoru. Třetí kapitola se zaměřuje na způsoby provedení trestných činů v kyberprostoru. Čtvrtá kapitola shrnuje zásadní evropské a mezinárodní právní instrumenty pro boj s útoky proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů. Kapitola pátá se zabývá trestnými činy relevantními k tomuto tématu v českém trestním zákoníku. Závěrečná kapitola zhodnocuje trestněprávní důsledky vyplývajícími z budoucího zákona o kybernetické bezpečnosti.