ABSTRAKT

Tato dizertace studuje, jak se z kybernetické bezpečnosti stala agenda národní bezpečnosti a diskutuje implikace těchto procesů na mezinárodní bezpečnost. Práce je rozdělena do tří částí. První část rozebírá teoretický a metodologický přístup. Druhá část rozebírá tři různé diskurzy spojené s kybernetickou bezpečností, diskurz technologických nadšenců (techno-geek), diskurz kybernetické kriminality a špionáže a diskurz kybernetické národní obrany za pomocí metody známé z díla Michela Foucaulta Archeologie vědění. Třetí část následně diskutuje implikace zjištěné v empirické části za pomocí několika teoretických přístupů. Konkrétně z pohledu disciplíny studující vědu a technologii z perspektivy společenských věd (Science and Technology Studies – STS), z pohledu teorie ANT (actor-network theory) a síťových asambláží. Kritická část výzkumu se orientuje na různé pohledy konstitutivních funkcí jednotlivých diskurzů. Zatímco technologičtí nadšenci jsou vnímáni jako zdroj použitého jazyka tvořícího významové znaky (semiosis), následně kryptoanarchistickou ideologii ovlivněnou kyberpunkovou subkulturou, diskurz kriminality a špionáže je studován jako zdroj empirické evidence dovedností technologických nadšenců (geeks). Když jsou tyto dva světy zkombinovány, vzniká přehnaná imaginace na straně národních států, které primárně vnímají snahy technologických nadšenců se vyhnout zákonu vývojem tzv. osvobozujících technologií (liberating technologies), které jsou též používány k organizaci globálních kriminálních gangů. Důsledek těchto procesů je vznik přehnaných imaginací budoucnosti národní bezpečnosti bez ohledu na nedostatek empirických dat potvrzujících realizovatelnost katastrofických scénářů. Kybernetická bezpečnost jako národně bezpečnostní agenda byla schopna vytvořit oblast znalostí, které nejsou dokladem možnosti naplnění katastrofických scénářů, nýbrž součástí sociální konstrukce celé imaginace potenciální katastrofické budoucnosti. Expertíza, která vzniká na politický popud, daleko spíše odpovídá na tuto potenciální imaginaci namísto toho, aby doložila naplnění hrozeb vyplývající z technologických možností komunikačních technologií. Práce argumentuje tím, že nedůsledné oddělování imaginací stojících na kulturním základě namísto základu technicistně faktickým, způsobuje vznik nereálných scénářů vývoje národní bezpečnosti implikující žádost vzniku národní obrany kybernetické bezpečnosti. Nicméně důsledky jsou dalekosáhlejší v tom, že samotná iniciativa na straně států implikuje další iniciativu na straně technologických nadšenců (geeks), kteří vyvíjí další osvobozující technologie, jenž národní státy nejsou schopny efektivně regulovat. V důsledku toho vzniká organizovaná rezistence, kterou národní státy začínají vnímat jako potenciální líheň kybernetického terorismu čistě z důvodu jejich dovedností, ale bez ohledu na jejich zájmy. Nicméně tyto katastrofické zájmy pro národní státy jsou vidět v zájmech krypto-anarchistických hnutí. Následující vývoj má však zásadní dopady na vnímání charakteru liberálně demokratického státu západního typu. A to především po událostech, kdy globální sledování všech dostupných lidí v kyberprostoru tyto hodnoty přímo popírá, neboť nejen, že tyto operace přispívají ke vzniku utopického panoptikonu, ale též proto, že národní státy ztratily možnost tyto operace efektivně řídit. V případě, že státy nebudou schopny reagovat a regulovat vznik nových technologií efektivně a s respektem ze strany vzdorujících technologických nadšenců, je pravděpodobné, že svět se bude ubírat směrem hybridního vládnutí, do světa vlády tzv. oligoptikonu, ve kterém státy nebudou hrát roli suverénního globálního aktéra.