Tomáš Karásek (oponent)

POSUDEK MAGISTERSKÉ PRÁCE

Jan Starý:
Potenciál kybernetických hrozeb v oblasti kritické energetické infrastruktury

Kybernetická bezpečnost, resp. kybernetické hrozby jsou v současnosti akademickou i politickou praxí považovány za klíčové téma v úvahách o vývoji, případně transformaci bezpečnostního prostředí. Stále intenzivnější využívání kybernetického prostoru jako doplňku, náhražky či nově koncipovaného nástroje pro společenské interakce nejrůznější povahy se zdá potvrzovat tuto tezi jako empiricky silně zakotvenou. Autor se ve své práci zaměřuje na propojení kybernetické bezpečnosti a kritické energetické infrastruktury, čímž kombinuje dvě významná (nebo přinejmenším módní) témata současné bezpečnostní debaty.

Práce si klade za cíl objasnit parametry zranitelnosti energetické infrastruktury kybernetickými hrozbami za pomoci teorie sítí v konkrétním pojetí Alberta Barabásiho. Text je rozdělen do tří základních částí, z nichž první definuje klíčové pojmy, druhá analyticky zkoumá daný problém a třetí vztahuje provedený výzkum k mezinárodním vztahům. Jádrem práce je jednoznačně druhá zmíněná část, která rozkládá zkoumaný problém do tří dimenzí – vnitřního prostředí, vnějšího prostředí a externích faktorů.

Autora je v každém případě třeba pochválit za snahu o neotřelé uchopení tématu a za odvahu při překračování disciplinárních hranic oboru bezpečnostní studia. Nepochybná je i jeho schopnost strukturování rozsáhlé matérie na úrovni celé práce i jednotlivých částí a kapitol. Autor také prokázal schopnost kreativní a akademicky vhodné práce se širokou škálou zdrojů.

Práce však trpí řadou nedostatků, z nichž některé považuji za zcela zásadní. V prvé řadě jsem přesvědčen, že použitý teoretický rámec a hlavní část provedené analýzy vůbec nespadají nejen do kontextu politologického, ale ani obecněji společenskovědního výzkumu. Barabásiho teorii sítí by patrně bylo možné aplikovat i na sociální, případně politické vztahy, autor to však nečiní. Provedená analýza se soustředí prakticky výhradně na technické parametry kybernetického prostoru a energetické infrastruktury, nikoliv na jejich sociální a politické, potažmo mezinárodní souvislosti (s výjimkou poslední části práce, k níž ale viz níže). Je to škoda, protože i primárně technicky zakotvenou problematiku lze nepochybně zkoumat společenskovědním instrumentáriem.

Toto základní selhání se projevuje až překvapivým ignorováním politické dimenze problémů, o nichž autor pojednává. Jedním z příkladů může být konceptualizace pojmu hrozba, kterou autor provádí prostým odkazem na učebnicový text, aniž by projevil jakoukoliv snahu o její zasazení do obecnějšího kontextu bezpečnostních studií, v nichž například v uplynulých dvaceti letech silně rezonovalo nikoliv objektivní chápání hrozby, ale její intersubjektivní konstrukce. Na několika místech textu (např. s. 48, 1. odstavec) autor poukazuje na sociální kontext zkoumaného problému, aniž by se však o něj hlouběji zajímal. Obecně lze práci charakterizovat jako velmi sofistikovaný vhled do technických aspektů problému a minimální, případně velmi bazální reflexi jeho politických souvislostí. To podtrhuje příznačně eklektická a neuspořádaná 3. část práce, která navíc trpí nepřesnostmi v používání zmiňovaných konceptů (např. vadná aplikace Waltovy teorie rovnováhy hrozeb na s. 72). Shrnu-li, autor analyzuje technické téma z úhlu pohledu, který je opět výrazně technicistní a nemá prakticky žádnou ambici včlenit provedenou analýzu do společenskovědního kontextu.

Za druhé, s předchozí připomínkou souvisí další námitka, která směřuje k jednomu z klíčových předpokladů provedené analýzy, podle něhož je centralizovaná síť nejzranitelnější variantou. To

patrně platí na úrovni automatizovaných systémů, ale ne nutně v širším sociálním a politickém kontextu. Lze totiž přinejmenším namítnout, že právě vědomí zvýšené zranitelnosti může stimulovat snahy o zabezpečení kritického místa sítě (tedy jejího centrálního uzlu). Přitom by v rámci centralizovaného systému mohla být tato opatření provedena efektivněji a úsporněji než v decentralizovaném systému.

Třetí námitka směřuje proti autorově konstrukci hlavní hypotézy a subhypotéz (s. 14). Ve skutečnosti totiž hypotézy 2-4 nepředstavují rozvinutí nebo specifikaci hlavní hypotézy (jak lze jednoduše ukázat prostým srovnáním hypotézy 1 a hypotézy 2), ale spíše samostatné vedlejší hypotézy. Nejde o pouhé slovíčkaření: Východisko v podobě hlavní hypotézy a jejích subhypotéz by odkazovalo k propracovanému, jednotnému analytickému rámci, zatímco zvolené řešení vyvolává otázky o výzkumné potřebnosti a vhodnosti jednotlivých vedlejších hypotéz.

Za čtvrté, ačkoliv (přesněji řečeno právě proto, že) se text zabývá výrazně technicistní problematikou, bylo by záhodno vyvarovat se pádu do žargonu daného odvětví – což se však autoru nepodařilo (první věta na s. 40 budiž snad nejkřiklavějším, ale rozhodně ne výjimečným příkladem). Stejně tak musím práci vytknout nedbalé nebo nesprávné používání přebíraných termínů (Proč jsou anglické – a někde i české – termíny nesmyslně psány s velkým počátečním písmenem? Proč je název kapitoly 2.1.2.1 kompletně v angličtině? Atd.). Nejde o maličkost: Absolvent magisterského studia by měl mimo jiné disponovat určitou kulturou vyjadřování.

Celkově tak práci hodnotím jako sympatický pokus o neotřelý pohled na téma, které v oboru v současnosti silně rezonuje, jenž nicméně nerespektuje základní parametry, východiska a možnosti oboru, v němž práce vznikla. Jen proto, že je z práce zjevné velké úsilí a nepochybná kvalifikovanost, kterou do ní autor vložil, hodnotím ji jako ***dobrou*** a ***doporučuji ji k obhajobě*** s tím, že autor by se měl během ní vyjádřit k zakotvení své práce v oboru bezpečnostních studií.

V Praze dne 20. 1. 2015