Prof. Ing. Ladislav BUŘITA, CSc.
Univerzita obrany, Fakulta vojenských technologií, Katedra informatiky a kybernetických operací

Oponentní posudek habilitační práce

Ing. Július BARÁTH, Ph.D.: „Model vyspelosti a sieťovej infraštruktúry pre NATO NEC C2"

Posuzovaná habilitační práce (dále jen HP nebo práce) o rozsahu 117 stran obsahuje 2 hlavní části: Model vyspělostí NATO NEC C2 (35 stran) a Síťová infrastruktura NATO NEC C2 (42 stran). K obvyklé struktuře HP chybí části: Stav oboru, Cíle a metody.

A) Aktuálnost tématu HP

Koncept NATO NEC je stále platný, ale byl již rozšířen projektem FMN (Federated Mission Networking). Stále aktuální je však základní myšlenka v účinném propojení senzorů-míst velení-efektorů (zbraňových systémů). Práce se v daném konceptu orientuje na oblast C2 (Command and Control – Velení a řízení) a rozšiřuje ho. Zejména zaměření na hodnocení stavů vyspělosti NATO NEC C2 je aktuální, protože umožňuje posoudit stav konkrétní jednotky, úkolového uskupení či armády pro zapojení do mise a dává návod na zlepšení stavu.

B) Splnění stanoveného cíle a použité metody

Cíl HP není explicitně stanovený, ale z textu práce vyplývá, že je orientovaný na rozvoj modelu vyspělostí NATO NEC C2 a návrh síťové infrastruktury NATO NEC C2. Absence explicitně vyjádřeného cíle práce neumožňuje posoudit jeho splnění.

Použité metody nejsou uvedeny; aplikované byly metody analýzy a syntézy, modelování, etapizace a experimentování. Metody byly použity v řešené tématice adekvátně.

C) Výsledky práce a nové poznatky

Práce začíná vymezením základních pojmů. Je popsána historie C2, rozebrán pojem síťová způsobilost, schopnost vedení operace, konceptuální model, model vyspělosti NATO NET C2 a jeho jednotlivé složky. Tuto pasáž lze částečně považovat za hodnocení stavu oboru zájmu HP.

V kapitole 2 (K2) je rozebrán Model vyspělostí NATO NEC C2. Jedná se o analytickou část s rozborem jednotlivých složek modelu a určení parametrů k posouzení stavu vyspělosti. Pro kvalifikovaný návrh modelu je třeba, aby zpracovatel měl odpovídající zkušenosti ve velení na operačním a strategickém stupni armády, či byl zapojen ve strukturách NATO. Jinak se jedná o akademický pokus s malým teoretickým a praktickým přínosem. K novým poznatkům lze označit právě metodický postup rozpracování modelu a návrh parametrů pro hodnocení stavu vyspělosti. K pozitivnímu přínosu v této části lze ještě zařadit proceduru přechodu mezi úrovněmi vyspělosti C2 s odpovídajícím seznamem úloh.

Nedostatky v K2 jsou v použití některých pojmů a v hodnocení parametrů vyspělosti. Označení nejvyššího stupně vyspělosti NATO NEC C2 je uvedeno jako „Edge / Koherentní / Transformované". Právě „edge" (okraj) je použito nejčetněji, ale evokuje technologické téma „edge computing". Za nejlepší označení lze považovat „koherentní", což je i v souladu se Studií proveditelnosti NATO NEC.

V textu K2 jsou označeny subjekty zájmu pro posouzení jako entity a jejich sady jako „kolektiv"; což by mohlo být nahrazeno vhodnějším vojenským pojmem „úkolové uskupení". Hodnocení proměnných v tabulkách na obr. 16–18 je vágní a nejasné. Obsahuje stavy: minimální, úzký, omezený, výrazně omezený, bez omezení, mírný, široký, výrazný, bohatý, úplný, hluboký. Správně by bylo předem stanovit škálu hodnocení a tu pak používat!

V K3 je analyzována síťová infrastruktura pro NATO NEC C2, jsou navrženy její prvky, se kterými jsou pak uskutečněny experimenty. Tato kapitola je rozhodně z hlediska zaměření, výsledků výzkumu a přínosnosti zdařilejší než předchozí kapitola, je to dáno samozřejmě odborným zájmem Ing. Barátha. Síťově orientovaná způsobilost by měla zajistit „bezešvé" propojení senzorů-míst velení a zbraňových systémů. K tomu směřují, jak výsledky uskutečněného výzkumu, tak i výsledná doporučení. Je charakterizovaná globální informační mřížka v kybernetickém prostoru,

jsou definované C2 proměnné a jsou rozebrané otázky kybernetické bezpečnosti. Cílené zaměření na kybernetickou bezpečnost síťového prostředí je významným přínosem práce.

Jsou vyjmenované (podle ISO/IEC 27002) požadavky na monitorování sítě k zajištění její bezpečnosti (celkem 15 požadavků, s. 70) a řada z nich je následně experimentálně ověřována. Pro jejich zvládnutí jsou specifikována opatření, jako automatizované zpracování provozních záznamů pomocí nástrojů SIEM (Security Information Event Management), budování specializovaných pracovišť SOC, CERT/CIRT, CSIRT. Klíčový význam zde hrají operační systémy.

Následuje monitorování lokální sítě, které přesvědčivě dokumentuje schopnost habilitanta zvládnout tento složitý problém. Přínosným tématem je optimalizace provozních záznamů pro detekci incidentů v síti. Je uveden přehled vhodných nástrojů a jsou popsána nastavení parametrů jednotlivých kategorií operačního systému MS Windows 10 a MS Windows Server 2016.

Experiment s použitím SIEM na monitorování síťové komunikace, spojen s analýzou získaných dat, zpracovaný v tab. 7 až 9, dává přesvědčivé výsledky. Přínosná je aplikace dataminig v analýze metodou rozhodovacích stromů a shlukovací analýzou. Zhodnocení dosažených výsledků je realistické.

Poslední část K3 tvoří zjišťování a vyhodnocování bezpečnostních incidentů pomocí SIEM. Je vytvořen aktivní kanál pro zobrazení a analýzu událostí, jsou vytvořeny filtry podle sledované oblasti, výsledky jsou zpracovány a dokumentovány podle typu událostí. Tato část patří mezi kvalitní a přesvědčivé výsledky HP.

D) Význam pro další rozvoj vědy, společenskou praxi a vzdělávání

Za teoretické přínosy lze uvést:

- Metodický přístup k modelování vyspělosti NATO NEC C2.
- Metodika návrhu a ověření síťové infrastruktury.
- Zajištění kybernetické bezpečnosti síťové infrastruktury.
- Optimalizace monitorování provozních parametrů sítě.

Za přínosy pro společenskou praxi lze uvést:

- Postupy monitorování v síti, odvození typu operačního systému.
- Vyhodnocení bezpečnostních incidentů, zejména s aplikací metod dataminig.

Za přínosy pro vzdělávání lze uvést:

- Uplatnění všech teoretických a praktických přínosů HP ve výuce na AOS LM.

E) Formální úprava práce a její jazyková úroveň

HP je napsána srozumitelným jazykem a neobsahuje formální nedostatky. Má odpovídající formální a grafickou úroveň.

F) Závěr

V závěru konstatuji, že HP Ing. Júlia BARÁTHA, Ph.D. má charakter habilitační práce a splňuje a podmínky kladené na úroveň HP. Žádám, aby Ing. Baráth při obhajobě zaujal stanovisko na výtky v posudku, zejména:

- Struktura HP a její chybějící části.
- Použití pojmů edge, entity a kolektiv.
- Způsob hodnocení parametrů vyspělosti.

V Brně dne 21. května 2021