Recenze

GEERS, Kenneth (Ed.). *Cyber War in Perspective: Russian Aggression against Ukraine.*

Tallinn: NATO CCD COE Publications, 2015.
ISBN 978-9949-9544-4-5 (print). ISBN 978-9949-9544-2 (pdf).
Dostupné z: https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_full_book.pdf

JUDr. Jakub Harašta,
Mgr. MgA. Jakub Míšek

Recenzovaná kniha se zabývá aktuálními otázkami možnosti vedení kybernetické války a staví je do rámce probíhajícího rusko-ukrajinského konfliktu. S výjimkou úvodní kapitoly z pera editora monografie Kennetha Geerse jsou ostatní kapitoly řazeny do pěti tematicky souvisejících částí. Tato souvislost je systematicky naznačena v seznamu kapitol a dá se vytušit i z organizace textu – v samotném těle knihy je dělení na jednotlivé tematicky související celky však vynecháno. Tematické celky jsou postupně nazvány *Strategic Framework, Tactical Viewpoints, Information Warfare, Policy and Law* a *The Future*.

V průběhu úvodní tematické části jsou předestřeny čtyři kapitoly. V rámci první z nich Keir Giles přehledně shrnuje pozadí rusko-ukrajinského konfliktu a doktrinální rámec kybernetické války. Uvádí tak čtenáře do problematiky jak historicky, tak teoreticky. Tato kapitola se dá použít jako úvodní rámec monografie – úvod editora totiž tuto funkci nenaplňuje a je spíš krátkým shrnutím jednotlivých kapitol. Ve druhé části James Wirtz poskytuje analýzu existence a využití možností kyberprostoru v ruské globální strategii a poskytuje stručné porovnání se strategií NATO. Dle Wirtze se Rusko nepokouší a nebude pokoušet NATO porazit, ale právě využíváním hraničních situací v rámci hybridního konfliktu bude prakticky demonstrovat, že je NATO neakceschopné a nefunkční. Využití diskutabilní povahy kybernetických operací nekinetické (primárně informační) povahy je klíčovou součástí tohoto plánu, protože znemožňuje efektivní zásah – tato výzva statu quo může být dle Wirtze vyřešena pouze diskreditací strategie NATO způsobené eskalací konfliktu nebo přizpůsobením se novému stavu věcí. Ve třetí kapitole James Lewis dochází po analýze známých incidentů k závěru, že ač kybernetické operace umožnily Rusku získat krátkodobou taktickou výhodu, nijak se neprojevily v dlouhodobém strategickém měřítku. V poslední kapitole úvodní části pak Martin Libicki opakuje svůj dobře známý skeptický názor na možnost kybernetické války – uzavírá, že se primárně jednalo o hacktivistické aktivity nebo o kybernetickou špionáž. V případě kybernetické operace s fyzickými následky totiž nemá napadený možnost zjistit, že k útoku došlo. Závady na zařízeních a sítích budou připisovány technickým vadám a lidským chybám. Kybernetická

válka ve smyslu Clausewitzova chápání termínu války tak vlastně nastat ani nemůže, protože chybí manifestované násilí.

Právě šíře záběru, kterou prezentovali autoři první části na prvních zhruba 40 stranách, je symptomatická pro celý zbytek knihy. Jednotlivé závěry se často doplňují na intuitivní úrovni, ale kniha postrádá zásadní jednotící myšlenku a konceptuální vymezení diskutovaného tématu. Jediné vymezení je zasazení do prostředí rusko-ukrajinského konfliktu, což není dle našeho názoru pro diskuzi tak aktuálního a kontroverzního tématu zcela vhodné. Publikace pak totiž namísto ucelené monografie připomíná sborník a komplikuje laickému čtenáři pochopení a celkovou práci s knihou.

V rámci dalších kapitoly (s. 55–58) totiž představuje Nikolay Koval, který v roce 2014 vedl CERT-UA, operační stránku konfliktu na Ukrajině. Zásadním postřehem je navázání počtu kybernetických incidentů na vývoj politické situace, což je závěr, který byl v jiném kontextu již v minulosti prezentován Kennethem Geersem v rámci jeho analytické činnosti pro společnosti FireEye. Politický vývoj se pak odrážel i v rámci skladby nahlašovaných incidentů, kdy se postupně začal objevovat sofistikovaný malware namísto defacementu webových stránek. Koval kritizuje nedostatečné povědomí ukrajinské společnosti o kybernetických hrozbách, což mělo zásadním způsobem omezit schopnost CERT-UA věnovat pozornost kybernetickým incidentům. Namísto toho bylo nutné věnovat se „nouzovému" vzdělávání uživatelů. Tyto závěry jsou přitom v poměrně ostrém rozporu s premisami, ze kterých vychází další kapitoly, např. kapitola 9 (s. 79–86) uvádí, že na Ukrajině je dostatek kvalifikované síly, kterou ale nebyla, na rozdíl od Ruska, schopna vlastenecky mobilizovat v rámci kybernetických operací. Podobně argumentuje i autor kapitoly 13 (nacházející se na stranách 113–122), když uvádí, že na Ukrajině je v důsledku akcentu sovětského vzdělávacího systému na technické obory dostatek vzdělaných odborníků, kterým ale chybí institucionální rámec umožňující jejich zapojení do obrany státu. Tyto názory sice nejsou vzájemně v přímém protikladu, ale do určité míry spolu soupeří, což vyplyne pouze při pozorném čtení – čtenář by mohl legitimně očekávat vzájemné odkazy mezi kapitolami nebo zmínku v úvodu. Ta ale v knize chybí.

Podobný problém je možné zahlédnout i v nekonzistentním používání termínu „válka" napříč publikací. Část publikace vnímá válku v pojetí Clausewitze (již zmíněný Libicki, s. 49–54), čemuž nasvědčují i závěry kapitoly 8 (s. 67–78), kde Jen Weedon konstatuje, že došlo jen k minimálním fyzickým škodám na kritické infrastruktuře a celá válka tak byla spíše informačního charakteru. Část publikace se pak, bez zjevného varování, přiklání k významu, který termínu přisuzuje mezinárodní právo – přebírá tak závěry Tallinnského manuálu o kinetické ekvivalenci (kapitola 14, s. 123–134), které se snaží dále diskutovat (kapitola 15, s. 123–134). Publikace pak plynule přechází někde mezi tyto dva postoje, kdy konstatuje změnu vnímání NATO ve vztahu ke kybernetickým operacím po summitu ve Walesu (kapitola 16, s. 145–152), která ale není v rámci mezinárodního práva bezvýhradně uznávána.

Podobný problém se vyskytuje i ve třetí části Information Warfare, kdy opět není zcela jasně zřejmá cílová skupina textů. Propagandu skrze narativ praxe bývalého Sovětského svazu představuje Margarita Levin Jaitner (kapitola 10, s. 87–94), která ale nakonec zakončuje konstatováním decentralizace jako nového směru propagandistické činnosti – oblast kouře a zrcadel s globálním dosahem, virálním šířením a postupnou obměnou. V rozporu s těmito závěry je pak možné chápat kapitolu 12 (s. 103–112), kde je nám

předloženo shrnutí proruské činnosti na sociálních sítích, které ale tentokrát není chápáno jako nástroj propagandy (a tedy jako informační válka), ale v širším konceptu kybernetické války, který vymezila ruská doktrína. Tento posun je těžké postřehnout a publikace tak předpokládá čtenáře, který je přesně obeznámen s konceptuálním vymezením – tomu ale neodpovídá obsah v podobě krátkých kapitol, které poskytují široký rozhled, ale nediskutují problematiku do hloubky.

Jakým způsobem se tedy k těmto nedostatkům postavit? Kniha je, i přes veškeré výše uvedené výhrady, extrémně informačně bohatá a má co nabídnout širokému okruhu čtenářů. Pro laxnost autorského kolektivu ve vztahu k používání termínů nejenom v rámci jednotlivých tematických částí, ale i jednotlivých, často sousedících kapitol, je však nutné ji číst opatrně. Neměla by sloužit jako studijní materiál, ale může vhodně rozšířit znalosti těch, kteří jsou již obeznámeni s jednotlivými koncepty, a zajímá je, jakým způsobem se projevovaly v rusko-ukrajinském konfliktu.

Náš závěr je takový, že rozsáhlý autorský kolektiv různého odborného zázemí nebyl schopen předložit kvalitní monografii. Jednoznačně ale předložil informačně nabitý sborník s jednotící linkou představovanou rusko-ukrajinským konfliktem a jeho virtuálním a informačním rozměrem.

Autoři: ***JUDr. Jakub Harašta**, narozen 1988. V současnosti působí na Ústavu práva a technologií Právnické fakulty MU. V roce 2015 guest research fellow na Univerzitě v Haifě. Zaměřuje se na kybernetickou bezpečnost, kybernetickou válku a právní informatiku.*

***Mgr. MgA. Jakub Míšek**, narozen 1989. Působí jako interní doktorand na Ústavu práva a technologií Právnické fakulty MU. Zaměřuje se na ochranu soukromí a osobních údajů. Od února 2015 působí na Ministerstvu vnitra jako poradce pro právní aspekty otevřených dat v ČR.*