Received: 30. 3. 2017 Accepted: 30. 3. 2017 Published on-line: 15. 6 2017
Available from: www.obranaastrategie.cz doi: 10.3849/1802-7199.17.2017.01.161-163

# STIENNON, Richard. There Will Be Cyberwar: How the Move to Network-Centric War Fighting Has Set the Stage for Cyberwar. Birmingham: IT Harvest Press, 2015. ISBN 987-0-9854607-8-5.

*Tomáš Maďar*[a]

Monografie Richarda Stiennona, jejíž samotný název slibuje naplnění obav o výskytu fenoménu kybernetické války, je jedním z mnoha příspěvků do diskuze na toto téma v posledních letech. Stiennon zaujímá své stanovisko na základě vhledu, který se mu podařilo získat za desetiletí analytické praxe v oblasti kybernetické bezpečnosti. Autor v této knize přetvořil a rozpracoval svou závěrečnou práci, již obhájil v rámci studia magisterského programu „War in the Modern World" na King's College London.

Stiennon v rozsahem velmi omezené publikaci o 138 stranách čistého textu, rozdělené do osmnácti kapitol, předkládá své postřehy nejen k fenoménu kybernetické války, ale i k teoriím souvisejícím s doktrínou Network Centric Warfare (NCW) či s tzv. revolucí ve vojenských záležitostech (revolution in military affairs, RMA).

První kapitola popisuje černý scénář budoucnosti, v němž je po neočekávané krizi a konfliktu s konkurenční Čínou, která využívá zranitelností v počítačových systémech a sítích vojenských systémů, na hlavu poražena nejsilnější současná velmoc, USA. V dalších dvou kapitolách Stiennon vysvětluje, proč si vybral právě nejčernější příklad a proč svou definici kybernetické války vymezuje jako „použití počítačových a síťových útoků na podporu cílů válčících aparátů" (str. 22).

Předkládané vymezení je poměrně problematické, neboť jej autor nijak dále nevymezuje, nedozvíme se tedy, co to vlastně ten válčící aparát je a co je do něj zahrnuto. Jsou to kupř. i zpravodajské služby a další silové složky? Nebo jen ozbrojené síly, jak je ve zbytku práce implikováno? Bohužel už tato neschopnost dopracovat vlastní koncept se ve finále ukazuje jako symptomatická pro celou publikaci.

Čtvrtá kapitola informuje o tom, jak technologie předchází válkám a jak jsou integrovány do ozbrojených složek. V páté kapitole Stiennon popisuje překotný růst internetu na počátku 90. let, v šesté zase přelom, který v doktríně NCW znamenala první válka v Zálivu. Další tři kapitoly popisují to, co autor pravděpodobně implicitně považuje za milníky v integraci informačních technologií do amerických ozbrojených sil – konkrétně v prvopočátku využití e-mailů, postupné budování složek, které se nakonec

[a] Department of Political Science, Faculty of Social Studies, Masaryk University, Brno, Czech Republic. E-mail: t.madar@mail.muni.cz

spojily v U.S. CYBERCOM, a v neposlední řadě schopnosti, které vyvinula hlavní americká zpravodajská agentura zaměřená na signální zpravodajství: National Security Agency.

Desátá kapitola hovoří o problematice bezpečnosti hardwarových dodávek a ověřování softwaru. Jedenáctá kapitola popisuje rozličná historická selhání amerických ozbrojených sil v kybernetické bezpečnosti. Ve dvanácté kapitole Stiennon krátce nakousne problematiku systematického myšlení při zajišťování kybernetické bezpečnosti, ve třinácté pak vedení elektronického boje.

V kapitole čtrnácté autor varuje před možností rušení schopností zásadních pro splnění bojových úkolů skrze prostředky elektronického a kybernetického boje, v kapitole patnácté jsou krátce zmíněna a diskutována možná protiopatření, která Stiennon doplňuje o upozornění, že postupné koncepční investice bývají levnější než snahy vyřešit jednotlivé incidenty ex post. Kapitola patnáctá varuje před obtížnou aplikací konceptu řízení rizik na kybernetickou bezpečnost, jako řešení kapitola šestnáctá uvádí analýzu hrozeb. Plochý dvoustránkový závěr opakuje některé výroky z dřívějších kapitol a zdůrazňuje, že užití kybernetických útoků na taktické a operační úrovni na bojišti při správné integraci s kinetickým komponentem může mít pro strategickou rovnováhu horší důsledky než případné snahy způsobit smrt skrze útoky na kritickou infrastrukturu v zázemí.

Jak už samotný počet stran publikace spolu s nepoměrným počtem kapitol napovídají, Stiennonova kniha je na mnoha místech velmi plochá a téměř bez přidané hodnoty. Několikeru nejkratších kapitol – kupříkladu té o systémovém myšlení a konceptu software assurance, případně těm věnovaným dot-comovému boomu či válce v Zálivu – autor věnuje pouhopouhé tři, respektive čtyři strany. Text je zároveň často nekoherentní a kapitoly na sebe mnohdy přímo nenavazují, ačkoliv je protíná tenké vlákno, kterým jako by se autor snažil dospět k něčemu, co si bohužel sám nikde nestanovuje.

Kvalita jednotlivých kapitol je rovněž velmi nekonzistentní, přičemž mezi silnější stránky knihy jasně patří ty části, v nichž se autor na základě své profesní minulosti evidentně dobře orientuje. Konkrétně se jedná především o kapitoly věnované problematice řízení velkých organizací a koncepčního zavádění a údržbě informačních technologií do ozbrojených sil a jiných velkých podniků, historii adaptace těchto technologií do amerických ozbrojených sil, více technickému popisu současných zranitelností v počítačových systémech a sítích, či určitých doporučení směřovaných na snížení rizik z těchto zranitelností plynoucích. Naopak nezvládnuté kapitoly pak tvoří ty, kde se Stiennon snaží o jakoukoliv bezpečnostní analýzu na strategické úrovni. Autor zde projevuje tendence poměrně slušně představit čtenáři problematiku, a následně bez hlubší diskuze prezentovat své názory na současný budoucí vývoj v oblasti, aniž by se pokoušel svá stanoviska jakkoliv hlouběji prodiskutovat či podložit adekvátními zdroji.
V konečném důsledku je tak kniha protknuta řadou nedostatečně podložených implikací, které čtenáři slouží spíše jako podněty k zamyšlení se než jako koherentní představení konkrétních pozic a názorů. Čtenář se tak například dozví, že v budoucím konfliktu mezi dvěma podobně silnými a technologicky vyspělými soupeři pravděpodobně nastane situace, která bude později označována jako kybernetická revoluce ve vojenských

záležitostech (Cyber Revolution in Military Affairs, CRMA): skrze metody elektronického a kybernetického boje dojde k oslepení schopností budovaných podle v současné době akcentované vojenské doktríny Network Centric Warfare, autor tuto myšlenku však dále nerozvíjí. Především pak Stiennon selhává v jakékoliv sebereflexi limitů konstrukcí scénářů, kdy mluví o výše zmiňovaných možnostech, jak oslepit případného protivníka, aniž by se zamyslel, jak dlouho dopředu by musely konkrétní schopnosti předpřipraveny či jak složité by vše bylo koordinovat, a to především při zahrnutí útoků na izolované systémy oddělené tzv. air-gapem.

Stiennon se navíc dopouští chyb, za něž byli již dříve jeho předchůdci kritizováni. Například jeho varování vzhledem k manifestaci fenoménu kybernetické války v mezinárodním prostoru je v knize založeno pouze na argumentu, že v počítačových systémech a sítích existují zranitelnosti – každý hypotetický soupeř se je tak v případě vojenského konfliktu jistě bude snažit využít. Autor se pravděpodobně neplete, ale odborná publikace by se měla snažit argumentovat lépe. Přestože tak v době, kdy Stiennon na knize pracoval, již došlo k celé řadě událostí a rozličných „prvních vlaštovek“, které proponenti kybernetického konfliktu často skloňují (namátkou autorem zmiňovaný červ Stuxnet, kyberfyzický útok na nejmenovanou německou ocelárnu, či celá řada špionážních kampaní, které by vzhledem k autorově nepříliš vhodné volbě definice kybernetické války také bylo možné do argumentace zařadit), Richard Stiennon bohužel nenapsal publikaci, která by přesvědčivě větší měrou přispěla do debaty o kybernetickém konfliktu.

Knihu je možné doporučit čtenářům, které zajímá adaptace informačních technologií americkými ozbrojenými silami na počátku a v průběhu první poloviny devadesátých let a doktrína Network Centric Warfare, těm se zájmem o historii výstavby amerického CYBERCOMu, případně těm, kteří mají zájem o překážky související s implementací informačních technologií napříč velkými organizacemi. To ovšem jen za předpokladu, že jim nebude vadit omezený rozsah či absence analytické hloubky, které Stiennon jednotlivým tématům věnuje. Mezi povinnou literaturu těch, kteří se profesně či akademicky věnují teorii kybernetické bezpečnosti, však knihu s klidným srdcem zařadit nelze.