TEORETICKÉ ASPEKTY INFORMAČNEJ VOJNY V IKT

Erika Vojtová

ABSTRAKT

Príspevok sa zameriava na informačnú vojnu ako na proces získavania prevahy prostredníctvom informačno-komunikačných technológií. Ide o rýchlo sa rozvíjajúci multidisciplinárny fenomén, ktorý zahŕňa množstvo situácií od problémov vo využití informačno-komunikačných technológii vo vojenskej vede až po ich politické či etické dôsledky na spoločnosť i jednotlivca. Článok predstavuje koncepčnú analýzu tohto javu, s cieľom vymedziť teoretickú bázu informačnej vojny. To je potrebné nielen z hľadiska jej pochopenia, ale aj ako predpoklad ďalšieho skúmania danej oblasti. Príspevok sa sústredí predovšetkým na vymedzenie konceptu informačnej vojny, ktorá ešte i dnes nie je jasne definovaná a pochopená a prináša rôzne pohľady na tento jav. Informačná vojna už dávno presahuje tradičné vojenské chápanie tohto pojmu a nielen že zasahuje do civilných sfér, ale prostredníctvom IKT, na ktoré je úzko naviazaná, stiera i hranicu medzi vojenským a civilným.

1 ÚVOD

Informačno-komunikačné technológie (IKT) prudko ovplyvnili všetky aspekty našej spoločnosti. Toto tvrdenie už môžeme v dnešnej dobe považovať za klišé. Avšak len málo ľudí si skutočne uvedomuje, aký naozaj enormný dosah majú IKT na všetky sféry spoločenskej existencie. Významne zasiahli aj do oblasti vojenskej vedy a konvenčného vedenia vojny a dali vzniknúť novodobému fenoménu nazývanému informačná vojna (IV).

Na jednej strane vo svojej podstate koncept informačnej vojny nie je ničím novým. Už čínsky vojenský stratég SunTzu (2009) v 4. storočí pnl. v diele Umenie vojny tvrdil, že lepšie než vyhrať sto bitiek je pokoriť cudzie vojská bez bitky. Poraziť nepriateľa dôvtipom a vynachádzavosťou, bez použitia násilia bolo podľa neho najvyšším stupňom vojenského umenia. Siete špiónov, informátorov a tajných agentov, ktorých úlohou bolo zbierať informácie, propaganda či manipulácia, zastrašenie protivníkov i civilného obyvateľstva – to

všetko bolo súčasťou všetkých dôležitých vojenských (ale i nevojenských) konfliktov takmer od nepamäti. Revolúcia v tomto smere však nastala práve s príchodom masívneho využitia IKT.

Za významný medzník v tomto kontexte môžeme považovať roky 1964 – 1975 a vojnu vo Vietname, ktorá sa v týchto rokoch odohrala. Odborná literatúra tu hovorí o tzv. "vietnamskom syndróme" alebo "vietnamskom ponaučení". Počas konfliktu sa totiž prvýkrát zreteľne demonštroval vplyv médií na reálny výsledok konfliktu. Väčšina vojenských stratégov sa zhoduje, že neobmedzené mediálne pokrytie daného konfliktu ovplyvnilo neúspech celej akcie. (Pfauser 2010)

Azda ešte významnejším konfliktom z pohľadu informačnej vojny je Operácia púštna búrka v Perzskom zálive. Tento konflikt sa nazýva aj ako „prvá vojna v priamom prenose“, na základe obrovského mediálneho záujmu. Práve po púštnej búrke sa začali objavovať úvahy o novom spôsobe vedenia vojny, ktoré uviedol do praxe následný rozmach informačno-komunikačných technológií a informačná revolúcia a objavujú sa aj prvé definície informačnej vojny. (Vojtová 2015)

Informačná revolúcia tak podporila vznik nových spôsobov vedenia vojny, všeobecne prostredníctvom útokov na infraštruktúry, na ktorých sú čoraz viac závislé moderné spoločnosti. Vo vývoji IV neustále sa vyvíjajúce technológie zohrávajú dôležitú úlohu. Nielen, že vďaka nim vznikli nové nekonvenčné formy vedenia vojny, na druhej strane strach z fatálnych dôsledkov ďalšieho globálneho konfliktu núti štáty, ale i jednotlivcov, tieto formy čoraz viac zdokonaľovať. Informačná vojna ponúka aspekty neznáme minulým generáciám a potenciál informácie stať sa zbraňou vyplýva z toho, že aj tradičnými vojenskými cieľmi sa stávajú informácie. Na strane druhej IV už dávno prekročila hranice tradičného chápania konvenčného vojenského konfliktu a techniky a intelektuálne mechanizmy informačných vojen sa stávajú bežnou súčasťou konfliktov nielen na národnej úrovni, ale aj v politickej, ekonomickej, sociálnej či dokonca súkromnej sfére.

2 DEFINÍCIE INFORMAČNEJ VOJNY

Potreba vymedzenia pojmu informačná vojna je dnes, viac než kedykoľvek predtým, potrebná, ba priam naliehavá. Aj keď sa o to pokúšajú mnohí autori, pri hlbšej analýze narážame na početné problémy - nejednotnosť, nejednoznačnosť či vágnosť pri jeho vymedzení. Tieto problémy vystávajú nielen zo samotného problému vymedzenia pojmu

informácia, ale aj z problému vymedzenia pojmu vojna. Význam vojny, ako ju chápu mnohí autori a teoretici vojenskej vedy ešte i dnes sa totiž značne posunul. Rovnako je pojem informačná vojna používaný i v prenesenom význame a stretávame sa s ním často v mediálnych výstupoch bez toho, aby sme si v skutočnosti uvedomovali, čo všetko je v ňom obsiahnuté. (Vojtová, 2015)

Na druhej strane sa tento fenomén neustále a veľmi rýchlo vyvíja, definície často krát nestíhajú obsiahnuť nové aspekty, ktoré v tomto smere vystávajú. Ďalším problematickým hľadiskom pri definovaný konceptu je jeho multidisciplinárnosť a tiež fakt, že informačná vojna už vo svojej podstate zahŕňa skryté a nezrejmé stratégie, jej cieľom často je, aby samotní účastníci nevedeli, že sa stali jej aktérmi a definovanie tohto javu je o to komplikovanejšie.

Na problematiku termínu informačná vojna upozorňuje aj A. Jones (1999) a uvádza, že termín sa používa na opis širokého spektra techník a javov s rôznou mierou presnosti. Značná nekonzistentnosť panujúca v danej problematike vyvoláva veľa diskusií o vhodnosti používania termínu. Vynára sa veľké množstvo otázok, či ide o nový fenomén alebo v podstate len staré techniky, prostredníctvom ktorých sa v cynickom úsilí snažia kompetentní získať finančné prostriedky na znižujúcom sa trhu obrany a obnoviť záujem o počítačovú bezpečnosť. Nepochybne, všetky tieto otázky sú na mieste a poskytnuté odpovede sú založené na pravde, napriek tomu celá oblasť je zle definovaná a pre rôznych ľudí informačná vojna znamená rôzne veci.

Väčšina definícií informačnej vojny, pochopiteľne, pochádza od autorov venujúcich sa vojenskej vede respektíve pôsobiacich v ozbrojených silách. Predovšetkým autori z USA rozpracovávajú koncepciu tohto pojmu, keďže práve Spojené štáty americké tento fenomén podrobne skúmajú i využívajú. Samozrejme, problematikou informačnej vojny sa čoraz častejšie a intenzívnejšie zaoberajú i ostatné technologicky vyspelé štáty, čím tento pojem dostáva status javu vyžadujúceho dôkladný výskum v oblastiach svojho vedenia, dopadov i etických hraníc. (Nižňanský 2003)

Jednu z prvých koncepcií informačnej vojny priniesol Libicki (1995), ktorý tvrdí, že informačná vojna ako samostatná technika vedenia vojny neexistuje. Namiesto toho existuje podľa neho až sedem foriem informačných vojenských konfliktov, ktoré zahŕňajú ochranu, manipuláciu, degradáciu a odmietanie informácií, pričom rozlišuje elektronickú vojnu (rádioelektronické alebo kryptografické techniky), psychologickú vojnu (v ktorej sa

informácie používajú na zmenu myšlienok), "hackerské" vojny (v ktorých sú napadnuté počítačové systémy), boj proti hospodárskym informáciám (blokovanie informácií alebo ich usmerňovanie s cieľom dosiahnuť hospodárske dominantné postavenie) a kybernetické útoky, pričom všetky tieto formy sú si viac či menej príbuzné.

Slovník vojenských a súvisiacich termínov ministerstva obrany USA definuje informačnú vojnu ako opatrenia prijaté na dosiahnutie informačnej prevahy ovplyvnením protivníkovej informácie, informačných procesov, informačných systémov a počítačových systémov a zároveň opatrenia chrániace naše vlastné informácie, informačné procesy, informačné systémy a počítačové siete. (U.S. Department of defense 2010)

Definícia od Denninga (1998) z Georgetownskej univerzity z knihy Informačná vojna a bezpečnosť hovorí, že informačná vojna pozostáva z ofenzívnych a defenzívnych operácií proti informačným zdrojom. Prebieha preto, lebo informačné zdroje majú istú hodnotu. Útočné operácie majú za cieľ zvýšiť túto hodnotu pre protivníka, obranné operácie sa snažia čeliť potenciálnym stratám hodnoty.

John Arquilla (1999) sa zameriava na etické aspekty informačnej vojny a definuje ju ako nový spôsob vojny, ktorý je primárne rušivý, nie deštruktívny a jej nízke vstupné náklady umožňujú aj jednotlivcom a skupinám (nielen národným štátom) ľahko získať veľmi vážne vojenské schopnosti. Informačná vojna je sama o sebe viacrozmerným konceptom, ktorý sa pohybuje od pojmov využívania kybernetického priestoru ako základne, z ktorej sa vykonávajú útoky za účelom poškodzovať komunikačné uzly a infraštruktúry až po myšlienku využívania masmédií na psychologické ovplyvňovanie. Informačná vojna teda môže slúžiť ako forma podpory pre vojenské sily počas aktívnych operácií na jednej strane, ale môže sa použiť aj v strategických kampaniach, ktorých cieľom je priamo zasiahnuť do vôle a logistickej podpory súpera na strane druhej.

Ruský pohľad na IV poskytujú autori Grau a Thomas (2007) vo Vestníku slovanských vojenských štúdií, pričom IV je podľa nich spôsob, ako vyriešiť konflikt medzi protichodnými stranami. Cieľom je, aby jedna strana získala a udržala informačnú výhodu nad druhou. Toto sa dosiahne vyvíjaním špecifického informačného, psychologického a technologického vplyvu na národný rozhodovací systém, na národ a jeho štruktúry informačných zdrojov, ako aj na porážanie kontrolného systému nepriateľa a jeho zdrojových informačných štruktúr s pomocou dodatočných prostriedkov.

Čínsky pohľad na informačnú vojnu z Centra vojenského strategického výskumu IV charakterizuje ako transformáciu z mechanizovanej vojny priemyselného veku na vojnu rozhodovania a kontroly, vojnu vedomostí a vojny intelektu.

Aj z predkladaných definícií je jasné, že koncept informačnej vojny je naozaj problematický. Väčšina opisov ju skôr charakterizuje, než sa ju snaží definovať a v mnohých definíciách pokrýva široké spektrum rôznych javov vrátane integrovaného využívania všetkých vojenských spôsobilostí, psychologických operácií (PSYOPS), elektronického boja a fyzického ničenia, podporovaného všetkými zdrojmi spravodajských, komunikačných a informačných systémov.

3 CIVILNÝ ASPEKT INFORMAČNEJ VOJNY V IKT

Z množstva vedeckých publikácií, ktoré sa zaoberajú touto tematikou by sme veľmi zjednodušene mohli tvrdiť, že za informačnú vojnu môžeme považovať vlastne čokoľvek. Keďže väčšina dostupných zdrojov pochádza od príslušníkov ozbrojených síl, v dôsledku toho je na celú situáciu nahliadané z vojenského hľadiska (oveľa častejšie než z politického, sociologického, filozofického, etického atď.). V tejto kapitole však predstavíme problém, ktorý z hľadiska informačnej vojny v IKT považujeme za kľúčový, a síce takzvaný civilný aspekt informačnej vojny. Aj keď sa informačnou vojnou zaoberajú rôzne odvetvia ozbrojených síl, už zo svojej podstaty má v informačnom veku potenciálne omnoho širšie dôsledky pre spoločnosť ako celok, či už z hľadiska vojenského alebo civilného, kolektívneho alebo individualistického, systematického alebo neúmyselného.

Koncepciu informačnej vojny z civilného hľadiska vo svojej štúdií podrobne rozpracovávajú Cronin a Crwford (1999). Tí tvrdia, že informačná vojna sa v rámci sveta Pentagonu a jeho satelitných spoločenstiev vykryštalizovala ako radikálne nová koncepcia postindustriálneho boja, ktorá je určená na zabezpečenie pokračujúcej americkej vojenskej dominancie v ére po studenej vojne. Prevládajúci jazyk, obrazy a metafory majú klasickú militaristickú povahu. To často rozmazáva skutočnosť, že mnohé zo základných princípov a predpokladov informačnej vojny majú uplatnenie, ktoré ďaleko presahuje konvenčné vojenské kontexty. Koncepcie informačnej vojny si zaslúžia byť oslobodené od svojich vojenských združení a zavedené do iných diskusných komunít zaoberajúcich sa pochopením sociálnych dôsledkov všadeprítomných informačno-komunikačných technológií. Zásady a praktiky informačnej vojny sa ukazujú vo viacerých civilných kontextoch (od počítačových podvodov až po

počítačovú kriminalitu) a existuje viac než len predpoklad, že tento trend sa zintenzívni a spôsobí potenciálne vážne sociálne problémy.

Civilný aspekt informačnej vojny v definíciách zohľadňujú aj iní autori, medzi ktorých patrí aj Reto Haeni. Haeni (1997) vidí hlavnú príčinu v problematike definovania termínu informačná vojna predovšetkým v jeho mnohoznačnosti. Na jednej strane je totiž informačná vojna vojenským aspektom, na strane druhej je takto označovaná aj vojna (v prenesenom význame) na internete či v médiách, je preto náležité nájsť takú jej definíciu, ktorá by rovnako dobre zachytávala potreby armády i civilných strán.

Takmer identicky nahliada na koncept informačnej vojny i Megann Burnsová (1999) a charakterizuje ju ako komplex nástrojov na zber, ochranu, manipuláciu, narúšanie a degradáciu informácií zabezpečujúcich výhodu nad protivníkom. Hoci sa sústredí najmä na zvyčajné militaristické predstavy o informačnej vojne, túto definíciu je podľa nej možné uplatniť v akejkoľvek konkurenčnej situácii, či už verejnej, súkromnej, vojenskej alebo civilnej.

Nad aspektmi informačnej vojny prekračujúce hranice vojenskej vedy sa zamýšľa aj český autor Josef Nastoupil (1999), pričom podľa jeho mienky pod informačnou vojnou v najširšom zmysle slova rozumieme získavanie, spracovanie a využívanie informácii a tiež aj ovplyvňovanie ľudí, strojov a ich rozhodovania. Rovnako ako Haeni a Burnsová pripúšťa, že určité podoby informačnej vojny majú civilnú povahu a existujú hlboko pod prahom dosiaľ označovaným ako vojna. Je očividné, že v blízkej budúcnosti bude rozhranie medzi mierom a vojnou čoraz menej zreteľné a v každom prípade bude doteraz platný výklad vojny ako ozbrojeného konfliktu medzi štátmi vyžadovať novú definíciu.

Slovenský autor Nižňanský (2003, s. 6) tiež informačnú vojnu v najširšom význame definuje ako „*súčasť štátnej politiky, ktorá sa usiluje o dosiahnutie národných záujmov s minimálnym použitím tradičnej vojenskej sily. Zdôrazňuje sa, že informačná vojna predstavuje v tomto zmysle politickú vojnu, v ktorej použité zbrane nie sú síce viditeľné a zrejmé, zato sú však veľmi konkrétne vo svojich účinkoch.*"

John Petersen (1997) opisuje dve generácie informačnej vojny, pričom prvú generáciu charakterizuje ako technickú, využívajúcu počítačové vírusy či napádanie informačných systémov. Druhá generácia sa v období, keď svoju koncepciu popísal iba rozvíjala a jej vzostup očakával v ďalších desaťročiach, pričom jej hlavným znakom malo byť masívne

využitie manipulácie ľudského vedomia, názorov a postojov prostredníctvom využitia masmédií, dezinformačných kampaní či virtuálnej reality.

Túto koncepciu ďalej rozpracovávajú Harutyunyan , Grinyaev a Arzumanyan (2016), keď vo svojom článku hovoria o informačnej vojne tretej generácie, pričom jej cieľom je ovplyvňovať protivníkov prostredníctvom špeciálnych operácií takým spôsobom, ktorý zmení ich správanie smerom k viac žiaducemu pre ovplyvňujúceho. Fyzická deštrukcia protivníka je len jednou z metód a nástrojov dosahovania cieľov vojny v rámci širšie vykonávanej politiky donútenia protivníka sledovať určitú líniu správania. Z tohto hľadiska informačná vojna presahuje rozsah vojenskej vedy a moderná vojna podľa nich vo svojej podstate ani neumožňuje diferenciáciu medzi vojenským a civilným obyvateľstvom.

Ruský autor Rastogurev (1998) prirovnáva informačnú vojnu k informačnej infekcii a analyzuje ju na základe biologickej, počítačovej a sociálnej infekcie. Na základe tejto analógie sa informačná vojna podľa neho sústredí rovnako ako iné typy vírusov na slabé prvky organizmu, v tomto prípade slabé miesta vedomia jednotlivca i spoločnosti. Za kritické prvky informačnej ochrany v spoločnosti pokladá jej dezintegráciu, rôzne historické traumy a slabé zložky daného štátu ako médiá, vzdelávací systém a podobne. V rovnakom smere rozpracoval koncepciu informačnej vojny aj litovský autor Maliukevičius (2007), ktorý poukazuje na to, že informačná vojna má za cieľ šíriť také informácie, ktoré sú v nesúlade s existujúcimi hodnotami, a tým podporuje nestabilitu spoločnosti v duchovnej, politickej i ekonomickej sfére. Preto primárnymi cieľmi informačnej vojny je podľa neho systém kultúrnych a hodnotových noriem.

Je zaujímavé, že pohľad ruských a čínskych autorov a ozbrojených síl je značne odlišný od toho amerického. V čínskej doktríne "Troch vojen“ je informačná vojna spomenutá ako stratégia zameriavajúca sa na podkopávanie medzinárodných inštitúcií, zmenu hraníc a podvrátenie globálnych médií prostredníctvom psychologických a mediálnych operácií s cieľom dosiahnuť záujmy štátu inak ako tradičnou vojenskou silou. Informačná vojna má za cieľ meniť tradičné morálne hodnoty občanov a manipulovať vedomie sociálnych skupín zavedením takzvanej demokratickej transformácie, pričom informačné zbrane poskytujú (nielen) štátom metódu získavania výhod bez vyhlásenia vojny. V Rusku a Číne je informačná vojna vnímaná ako stála aktivita, ktorá sa má vykonávať bez ohľadu na absenciu okamžitých konfliktov, otvorená a široko uplatniteľná. (Pomerantsev 2015)

Cronin a Crawford (1999) tiež predkladajú štyri hlavné sféry činnosti, v ktorých sa môže veľmi rýchlo stať informačná vojna relatívne bežná: vojenská, podniková (ekonomická), sociálna a osobná. Niektoré koncepcie, stratégie a aplikácie IV sú spoločné pre všetky štyri prostredia, aj keď môžu existovať interpretačné rozdiely, ako aj rozdiely v vnímanej zákonnosti, etike a sociálnej vhodnosti výsledkov, ktoré sledujú rôzni aktéri za rôznych podmienok.

4 ZÁVER

Charakter informačnej vojny posilňuje kompetencie jednotlivcov alebo skupín nízkymi vstupnými nákladmi a možnosťou vyhnúť sa odhaleniu a súčasne im umožňuje spôsobiť významné škody nielen iným jednotlivcom či skupinám, ale aj celým štátom. Informačná vojna tak nepredstavuje len vojenskú výzvu, ale aj výzvu kultúrnu, sociálnu a v neposlednom rade etickú.

Ako uvádza Jones (1999), ktorý sa problematikou informačnej vojny zaoberá aj mimo vojenskú vedu, súčasné pochopenie techník a vplyvov IV je nezrelé a pravdepodobne také aj dlho zostane, pretože technológie a závislosti na nich sa naďalej rýchlo menia. Okolo IV existuje značný rozruch a samotný pojem je často vykladaný takým spôsobom, ktorý sa aktuálne hodí autorovi.

Aj keď jednoznačná definícia IV, ako sme už niekoľkokrát uviedli, je značne komplikovaná, je viac než zrejmé, že informačno-komunikačné technológie aj v tomto smere spôsobili nevídanú revolúciu. Tá sa týka nielen faktu, že informačná vojna dávno prekročila hranice samotnej vojenskej vedy. Tým najznepokojivejším je fakt, že tieto hranice dokonca zmazáva.

Tradičné chápanie vojny už totiž v ponímaní IV nie je dostačujúce a môžeme tvrdiť, že ako spoločnosť, tak i jednotlivci sú súčasťou informačnej vojny (v drvivej väčšine nevedomky), takmer neustále. Fyzické bojiská sa presúvajú v čoraz väčšej miere do virtuálneho priestoru, cieľom už nie je zničiť reálnu infraštruktúru nepriateľa, ale zasiahnuť jeho informačné systémy, pričom v tom najširšom chápaní môže byť informačným systémom i samotná spoločnosť, človek.

Vďaka IKT i jednotlivci či malé skupiny majú potenciálne v rukách moc ako celé armády. Zbrane konvenčnej vojny sú totiž väčšinou nákladné a neprístupné, avšak zbraňou informačnej vojny je informácia. A informácia, jej šírenie a manipulácia, je aktuálne prostredníctvom IKT prístupná takmer komukoľvek. IV tak „prebieha každý deň aj na civilnej

úrovni, v masmédiách, na internete, na sociálnych sieťach, medzi politikmi, záujmovými skupinami, známymi osobnosťami či mediálnymi magnátmi. Je to vojna, v ktorej sa súperí o mysle ľudí a postoje verejnosti.“ (Vojtová 2015, s. 10) Nič nie je tak lacné a zároveň také cenné ako informácia. (Pocheptsov 1998)

Aj na základe vypovedaného považujeme za dôležité, aby sa téme informačných vojen v IKT aj naďalej venoval záujem nielen v kontexte jej jasného teoretického vymedzenia, ale i možnosti defenzívnych mechanizmov a etických rovín.

ZOZNAM LITERATÚRY

ARQUILLA, J., 1999. *Ethics of Information Warfare.* In: Strategic Appraisal: The Changing Role of Information in Warfare [online], 1999. Santa Monica: RAND Corporation, 1999. [cit. 2018-18-09]. Dosupné na: https://www.rand.org/pubs/monograph_reports/MR1016.html

BURNS, M., 1999. *Information Warfare: What and How?* [online]. Pittsburg: Carne-gie Mellon University, 1999, [cit. 2018-18-09]. Dostupné na: http://www.cs.cmu.edu/~burnsm/InfoWarfare.html

CRONIN, B. a CRAWFORD, H., 1999. Information Warfare: Its Application in Military and Civilian Contexts. In: The Information Society [online], 1999, roč. 15, č. 4, s. 257 263 [cit. 2018-18-09-]. ISSN 1087-6537. Dostupné na: https://doi.org/10.1080/019722499128420

DENNING D., 1998. *Information warfare and security.* Boston: Addison-Wesley, 1998. ISBN 912-02-0143-303-0.

HARUTYUNYAN, G – GRINYAEV, S. – ARZUMANYAN, H., 2016. *Information warfare of the new information*. In: Noravank Scientific Educational Foundation [online]. 26.12.2016 [cit. 2018-18-09]. Dostupné na: http://www.noravank.am/eng/issues/detail.php

HAENI, R., 1997. *Information warfare an introduction* [online]. Washington: The George Washington University, 1997, [cit. 2018-18-09]. Dostupné na: http://www.trinity.edu/rjensen/infowar.pdf

GRAU W. L a THOMAS T. L., 1996. *A Russian View of Future War: Theory and Direction,*. In: Journal of Slavic Military Studies [online], 1996, roč. 9, č. 3, s. 501 – 518 [cit. 2018-18-09]. ISSN 1556-3006. Dostupné na: https://doi.org/10.1080/13518049608430250

JONES, A. 1999. *Information warfare – what is it?* In.: Information Security Technical Report [online], 1999, roč. 4 č. 3, s. 12 – 19, [cit. 2018-18-09]. ISSN 1363 4127. Dostupné na: https://doi.org/10.1016/S1363-4127(99)80075-2

LIBICKI, C. M. 1995. What is information warfare. Washington: United States Government Printing, 1995. ISBN 99 96680 61 4.

MALIUKEVIČIUS, N., 2007. Geopolitics and Information Warfare: Russia's Appro-ach. In: *Lithuanian annual strategic review* [online]. Vilnius: University of Vilnius, 2007, s. 121-146 [cit. 2018-18-09]. ISSN 1648–8024. Dostupné na: http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?lng=en&id=120627

NASTOUPIL, J., 1999. Informační válka: způsoby a průběh jejího vedení. In: *Vojen-ské rozhled*y. 1999, roč. 8, č. 1, s. 129-138. ISSN 1210-3292.

NIŽŇANSKÝ J., 2003. *Informačná vojna v ozbrojených silách.* Bratislava: Ministerstvo obrany SR, 2003. ISBN 80-88842-63-8.

PETERSEN, J., 1999. *Info War: The Next Generation.* In: Proceedings Magazine [online], 1999, roč. 125, č. 1, s. 62-64, [cit. 2018-18-09]. ISSN 0041-798X. Dostupné na: https://www.usni.org/magazines/proceedings/1999-01

PFAUSER, L., 2011. Kontrola informačního prostředí během válek v Perském zálivu a Iráku. In: *Metodický portál RVP* [online]. 20.10.2011 [cit. 2018-18-09]. Dostupné na: http://clanky.rvp.cz/clanek/c/g/13793/kontrola-informacniho-prostredi-behem-valek-v-perskem-zalivu-a-iraku.html/.

POCHEPTSOV, G., 1998. *Kak "pereklyuchayut" narody. Psikhologiche-skie/informatsionnye operatsii kak tekhnologii vozdeistviya na massovoe soznanie v XX veke.* Kyjev: BI, 1998.

POMERANTSEV, P., 2015. *Introduction.* In: Information at War: From China's Three Warfares to NATO's Narratives [online]. 22.09.2015 [cit. 2018-09-20]. Dostupné na: https://www.li.com/activities/publications/information-at-war-from-china-s-three-warfares-to-nato-s-narratives

RASTORGUEV S. P., 1999. *Informatsionnaya voyna*. Moskva: Radio i svyaz, 1999. ISBN 5-256-01399-8.

SUN TZU, 2008. *Umění války.* Brno: B4U Publishing, 2008. ISBN 8090385061.

U.S. DEPARTMENT OF DEFENSE, 2010. *Department of defense dictionary of military and associated terms* [online], 2010 [cit. 2015-18-02]. Dostupné na: http://fas.org/irp/doddir/dod/jp1_02.pdf

VOJTOVÁ, E., 2015. *Využitie stratégií informačných vojen vo vybraných konfliktoch 20. a 21. storočia:* diplomová práca. Žilina: Žilinská univerzita, 2015.