POLITICKÉ VEDY / POLITICAL SCIENCES

Časopis pre politológiu, najnovšie dejiny, medzinárodné vzťahy, bezpečnostné štúdiá / Journal for Political Sciences, Modern History, International Relations, security studies

URL of the journal / URL časopisu: http://www.politickevedy.fpvmv.umb.sk

Author(s) / Autor(i):	**Radoslav Ivančík**
Article / Článok:	**Informačná vojna – jeden z multidisciplinárnych fenoménov súčasnej ľudskej spoločnosti**
Publisher / Vydavateľ:	**Fakulta politických vied a medzinárodných vzťahov – UMB Banská Bystrica / Faculty of Political Sciences and International Relations – UMB Banská Bystrica**
DOI:	**https://doi.org/10.24040/politickevedy.2021.24.1.135-152**

Recommended form for quotation of the article / Odporúčaná forma citácie článku:

Radoslav Ivančík. 2021. Informačná vojna – jeden z multidisciplinárnych fenoménov súčasnej ľudskej spoločnosti. In *Politické Vedy*. [online]. Vol. 24, No. 1, 2021. ISSN 1335 – 2741, pp. 135-152. Available at: DOI: https://doi.org/10.24040/politickevedy.2021.24.1.135-152

INFORMAČNÁ VOJNA – JEDEN Z MULTIDISCIPLINÁRNYCH FENOMÉNOV SÚČASNEJ ĽUDSKEJ SPOLOČNOSTI

INFORMATION WAR – ONE OF THE MULTIDISCIPLINARY PHENOMENNES OF CURRENT HUMAN SOCIETY

Radoslav Ivančík*

ABSTRACT
Contemporary human civilization is gradually still more and more tied to the use of communication and information technologies and is continually becoming dependent on it. The use of these technologies brings many new phenomena – in addition to the many positives and benefits manifesting itself in all spheres of society's life, there are also completely new security risks and threats to the human society on the other side. One of these phenomena, which is the subject of our investigation, is the information war, which by its multidisciplinary nature is one of the fundamental threats to what we now call information society. The aim of this study is, with the use the relevant methods of scientific research, especially in the field of military and security science, as well as political sciences, to point out that the information war has long gone beyond the traditional military understanding of the term and not only extends to civilian spheres of human society, but through the information and communication technologies which is closely linked to, gradually wipes out the boundaries between military and civilian sector.

Key words: information warfare, information and communication technologies, security risks and threats

„*Dosiahnutie sto víťazstiev v sto bitkách nie je vrcholom dokonalosti, ale podmanenie si nepriateľskej armády bez boja, to je skutočný vrchol dokonalosti*."
Sun Tzu

* plk. gšt. v zál., Ing. Radoslav Ivančík, PhD. et PhD. pôsobí ako odborný asistent na Katedre informatiky a manažmentu Akadémie Policajného zboru v Bratislave, Sklabinská 1, 835 17 Bratislava, Slovenská republika, e-mail: radoslav.ivancik@akademiapz.sk.

DOI: https://doi.org/10.24040/politickevedy.2021.24.1.135-152

Úvod

Informačné a komunikačné technológie (ďalej len „IKT“) už v minulosti výrazne ovplyvnili niektoré sektory našej spoločnosti, avšak v súčasnosti zásadným spôsobom ovplyvňujú všetky aspekty života ľudskej civilizácie. História samotného pojmu informačno-komunikačných technológií siaha do roku 1980. Podľa **Burgerovej** (2006) to bol **Alvin Toffler**, kto sa ako jeden z prvých ľudí zaoberal týmto pojmom a použil ho vo svojich prácach. Informačno-komunikačným technológiám sa venoval najmä vo svojom knižnom diele *Tretia vlna*, v ktorom opísal analýzu vývoja ľudskej spoločnosti. V nasledujúcom období postupne vychádzali ďalšie publikácie, v ktorých sa ich jednotliví autori zaoberali problematikou IKT. Kým niektorí autori považovali informačné technológie len za techniku, ktorá spracováva informácie, iní zasa informačné technológie označujú ako systém metód, pomocou ktorého sa realizuje maximálne využitie zdrojov (blízkych aj vzdialených) na komunikáciu v počítačových sieťach. (Kolenička, 1998)

Zo širšieho uhla pohľadu *„IKT sú technológie, ktoré nám umožňujú elektronicky zaznamenávať, uchovávať, vyhľadávať, spracovávať, prenášať a šíriť informácie, pričom predstavujú kombináciu informačných technológií (a techniky) a komunikačných technológií (a techniky)“* (Riley, 2015). V súčasnosti sú absolútne nepostrádateľné, pretože sú využívané už vo všetkých sférach a odboroch ľudskej činnosti a verejných či súkromných organizáciách a inštitúciách. Bez ich pomoci by dnes už len ťažko mohli fungovať úrady, obchody, banky, poisťovne, zdravotníctvo, doprava, priemyselná výroba, vedecké inštitúcie, médiá, zábavný priemysel, kultúrne inštitúcie, polícia, armáda, atď. Jednoducho v dnešnej modernej dobe sú neoddeliteľnou súčasťou našich životov. (Marolla, 2018)

Hoci vyššie uvedené tvrdenie o zásadnom vplyve IKT na všetky aspekty života ľudskej civilizácie je možné v dnešnej dobe a na tomto stupni vývoja spoločnosti považovať z istého uhla pohľadu trochu už aj za klišé, napriek tomu len málo ľudí si naozaj reálne uvedomuje, aký enormný dosah majú IKT na všetky sféry spoločenskej existencie. Jednou z oblastí, do ktorej zasiahli naozaj výrazne, je oblasť vojenstva, v rámci ktorého, v úzkej súvislosti so spôsobom konvenčného vedenia vojny, vznikol jeden z novodobých fenoménov – informačná vojna.

Informačná vojna je tak v súčasnosti, zvlášť po prepuknutí konfliktu na Ukrajine, fenomén, ktorý svojím multidisciplinárnym charakterom patrí medzi

zásadné potenciálne hrozby pre to, čo dnes nazývame informačnou spoločnosťou. Samotné slovné spojenie informačná spoločnosť je dnes už natoľko rozšírené a tak často diskutované, že by sa mohlo zdať zbytočné ho nejakým spôsobom znovu vysvetľovať, avšak v kontexte tejto štúdie a popisu prostriedkov informačnej vojny ako potenciálnej hrozby pre súčasnú ľudskú spoločnosť, sa charakterizovanie tohto termínu javí ako úplne nevyhnutné. Vďaka značnému zvýšeniu frekvencie jeho používania medzi vedeckou i laickou komunitou v poslednej dobe totiž dochádza k tomu, že pojem informačná spoločnosť je často vysvetľovaný rôznymi spôsobmi. Podobne ako pri mnohých iných pojmoch, jednotnú či univerzálne uznávanú a používanú definíciu tohto pojmu však prakticky nie je možné nájsť. Z uvedeného dôvodu predstavíme aspoň niektoré z definícií, ktoré sa pokúšajú tento fenomén postihnúť.

Napríklad **Krištofovičová a kol.** (1999) definujú informačnú spoločnosť ako *„spoločnosť založenú na integrácii IKT do všetkých oblastí spoločenského života v takej miere, že zásadne menia spoločenské vzťahy a procesy“*. **Schement** (2002, s. 11) zasa hovorí, že: *„Informačná spoločnosť je spoločnosť, v ktorej IKT ovplyvňujú každodenný život väčšiny jej členov. Za pomoci rozvoja internetu a kultúry "zosieťovania" sú IKT používané k širokému spektru osobných, sociálnych, výukových a obchodných aktivít a tiež k rýchlemu vysielaniu, prijímaniu a výmene dát medzi veľmi vzdialenými miestami. V informačnej spoločnosti sú informácie rovnako mocným zdrojom, akým bol v predchádzajúcich obdobiach výrobný a poľnohospodársky priemysel.“* (Schement, 2002, s. 11)

Ďalšia s definícií charakterizuje informačnú spoločnosť ako *„spoločnosť, v ktorej informatika, počítače a mikroelektronika určujú a premieňajú celý spoločenský systém, vystupujú ako prostriedok vytvorenia nových spoločenských, nadtriednych a nadnárodných štruktúr a zásadným spôsobom menia mechanizmy spoločenského vývoja. Jej vznik, rozdelenie, použitie, integrácia a manipulácia s informáciami, je významnou ekonomickou, politickou a kultúrnou činnosťou. Jedným z cieľov informačnej spoločnosti je získať konkurenčnú výhodu v medzinárodnom meradle práve vďaka používaniu IKT kreatívnym a produktívnym spôsobom.“* (Danessi, 2013, s. 190)

Čo sa týka primárneho predmetu nášho skúmania, tak samotný pojem informačná vojna býva najčastejšie používaný v oblasti vojenstva na označenie konfliktu, ktorý vedie útočiaca strana s cieľom narušiť, eliminovať či ochromiť informačné aktivity protivníka a zároveň ochrániť svoje vlastné. Prostriedky a metódy informačného boja však nepredstavujú reálne riziko len počas vojny,

ale aj v čase mieru, čo obzvlášť platí pre dnešnú spoločnosť, v ktorej zohrávajú v čím ďalej tým väčšej miere úlohu už spomínané IKT.

IKT síce na jednej strane prinášajú spoločnosti množstvo pozitív, napríklad v podobe rapídneho zrýchlenia komunikácie a výmeny informácií, zároveň však ide o dvojsečnú zbraň. Závislosť modernej spoločnosti na nich totiž neustále stúpa, a preto bude v budúcnosti potrebné venovať veľkú pozornosť nebezpečenstvám a rizikám, ktoré so sebou už zmienená závislosť spoločnosti na nich prináša. IKT totižto skutočne zásadným spôsobom ovplyvňujú všetky aspekty života našej spoločnosti a majú enormný dosah na všetky sféry spoločenskej existencie.

Aj z toho dôvodu je cieľom tejto štúdie, s využitím relevantných metód vedeckého výskumu, najmä z oblasti vojenskej a bezpečnostnej vedy, ale aj politických vied, poukázať na to, že slovné spojenie informačná vojna už dávno presahuje pôvodne tradičné vojenské chápanie tohto pojmu a nielenže v čoraz väčšej miere zasahuje do civilných sfér života spoločnosti, ale prostredníctvom IKT, na ktoré je úzko naviazaná, postupne stiera hranice medzi vojenským a civilným sektorom.

1. Informačná vojna

V prípade používania pojmu informačná vojna sa mnohým ľuďom spravidla vybaví neistý obrys akéhosi moderného typu konfliktu, ktorý však podľa nich ešte nenastal, takže je pomerne ťažké tomuto obrysu dať nejakú konkrétnu náplň. Čo presne tento termín znamená, ako a z čoho sa definícia informačnej vojny vyvinula, aké sú jej ciele a predovšetkým akú úlohu hrá v súvislosti s touto novou formou vedenia bojovej činnosti dnešná informačná spoločnosť, to všetko sú otázky, a aj mnohé ďalšie, ktoré boli súčasťou realizovaného výskumu a na ktoré sa snaží zodpovedať predložená štúdia.

V súvislosti s vojnou, klasik **Herbert G. Wells** v roku 1914 napísal: *„Nič nemohlo byť ľuďom zrejmejšie, ako to, s akou rýchlosťou sa vojna stávala nemožnou. Bohužiaľ, takto zrejmé to už nebolo miliónom tých, ktorí umierali v zákopoch prvej svetovej vojny – vojny, ktorá ukončí všetky ďalšie vojny."* (Mleziva, 2004, s. 106) **Wellsove** slová svedčia o tom, že ľudstvo bolo v minulosti už viackrát presvedčené (a presviedčané), že ďalšie vojny už nebudú, že tá posledná vojna, ktorá priniesla také strašné obete a škody, bude tentoraz už naozaj dostatočným mementom pre všetkých, ktorí by sa opovážili ešte raz prísť s myšlienkou akéhokoľvek ďalšieho násilného riešenia sporov. Z histórie sa však

môžeme poučiť, že to tak, žiaľ, do dnešných dní nikdy nebolo. Vojny, nanešťastie, vždy boli a stále sú jedným z nástrojov, ako riešiť politické či iné nezhody, a ľudstvo k nim až príliš často pristupovalo z pohľadu toho, akú vojny prinášajú fyzickú i psychickú devastáciu. Aj preto je vysoko nepravdepodobné, že by sa naša budúcnosť zaobišla bez ďalších vojnových konfliktov, obetí a násilností. Čo sa však oproti minulosti istotne zmení, je spôsob, akým budú konflikty v budúcnosti vedené.

Voľba prostriedkov, akými bola vojna vedená, sa podľa **Ušiaka** a **Görnera** (2017) vždy riadila predovšetkým podľa typu cieľov, ktoré mala za úlohu zničiť, aby bolo dosiahnuté víťazstvo. Ak bolo možné víťazstvo vo vojne zaručiť prostredníctvom zničenia živej sily protivníka, ako tomu bolo napríklad v staroveku, používali sa zbrane, ktoré boli určené špeciálne na tento účel. Neskôr vo vojnách industriálnej éry sa používali zbrane, ktoré boli schopné zaistiť víťazstvo pomocou zničenia nielen živej vojenskej sily, ale aj rozsiahlej fyzickej infraštruktúry znepriateleného štátu.

V dnešnej dobe – dobe globalizácie[1] a masívneho využívania IKT a globálnej siete internetu začínajú oba tieto segmenty postupne v čoraz väčšej miere zastávať úlohu, ktorú v minulosti predstavovali dva vyššie spomenuté typy terčov – teda najprv bojovníci (živá sila) v poli a potom kľúčové fyzické štruktúry. Podľa viacerých názorov[2] však nastáva doba, keď víťazstvo vo vojne zaručí oveľa skôr zničenie alebo narušenie on-line objektov či služieb (napríklad napadnutie armádnych počítačov a veliacej komunikačnej siete a ich vyradenie z prevádzky), alebo fyzických štruktúr, ktoré je možné napadnúť prostredníctvom siete (napríklad vypustenie priehrady, prerušenie dodávok elektrickej energie, nabúranie sa do informačných systémov bánk, poisťovní, nemocníc a pod.).

[1] Globalizácia predstavuje v súčasnosti vysoko dynamický a mnohostranný proces, v ktorom sa prelínajú a navzájom ovplyvňujú politické, ekonomické, sociálne, vojensko-strategické, technologické, ekologické a ďalšie faktory. (Šikula, 2005) Zároveň predstavuje celý rad fenoménov, ktoré generujú tlaky, ktoré štáty výrazne pociťujú. (Ondria, Kollár, 2011) a ktoré ovplyvňujú, okrem iného, aj ich obranu a bezpečnosť. V dôsledku globalizácie tak dochádza nielen ku zmenám stability a bezpečnosti, ale zároveň aj k vyššej zraniteľnosti a závislosti štátov. (Baričičová, 2017) Súčasný globalizujúci svet a pohyby spoločenských skupín naprieč štátmi prinášajú nové vnímanie bezpečnostného ohrozenia štátov, pričom vznikajú nové potenciálne druhy hrozieb, na ktoré štáty musia reflektovať a vytvárať nástroje proti týmto hrozbám (Nečas, Ušiak, 2011), vrátane nástrojov vojenských. To je aj jeden z dôvodov, prečo štáty cítia potrebu reagovať spoločne, vyvíjať integrované úsilie, kolektívne čeliť novým hrozbám a prispôsobiť medzinárodné organizácie, ktorých sú členmi (v prípade európskych krajín najmä EÚ a NATO), novým úlohám (Marek, 2017) v oblasti zaistenia vlastnej, individuálnej i kolektívnej bezpečnosti a obrany.

[2] Bližšie pozri napr.: Kazanský, 2015; Koblen – Szabo – Bučka, 2011 alebo Kramer, 2014.

Fyzické, ale aj virtuálne objekty, prístupné prostredníctvom siete sa tak stávajú čím ďalej tým výhodnejšími cieľmi potenciálneho konfliktu – informačnej vojny.

2. Teoretické východiská a charakteristika informačnej vojny

Informačná vojna je v podstate všeobecný pojem zahŕňajúci niekoľko typov vedenia bojovej činnosti, ktoré majú určité spoločné vlastnosti. Zrejme najpodstatnejšiu z týchto vlastností predstavuje (ako už vyplýva z názvu) dôraz kladený na informácie, ktoré sú v tomto type konfliktu brané ako kľúčový element nutný k dosiahnutiu víťazstva. Rôzni autori vysvetľujú pojem informačná vojna rôznymi spôsobmi, a preto podobne ako pri iných pojmoch, aj v prípade informačnej vojny je možné nájsť v odbornej literatúre množstvo rôznych, viac či menej výstižných definícií. Neexistuje však žiadna jednotná, univerzálna, unifikovaná a všeobecne akceptovaná a používaná definícia termínu informačná vojna.

Najvšeobecnejšia a zrejme aj najjednoduchšia a zároveň najčastejšie používaná definícia označuje informačnú vojnu ako *„boj o kontrolu nad informačnými aktivitami protivníka a snahu uchrániť svoje vlastné."* (Bayer, 2006) Iná, komplexnejšia definícia hovorí, že: *„Informačná vojna predstavuje široké spektrum aktivít, ktorých nástrojom alebo cieľom sú informácie a informačné technológie. Medzi tieto aktivity patrí napríklad šírenie dezinformácií, psychologické operácie a kybernetické útoky – narušovanie komunikačných sietí a prieniky do nich za účelom získania strategických informácií. Tieto aktivity môžu prebiehať aj v čase mieru bez toho, aby museli vôbec nejakému konfliktu predchádzať. Hlavným cieľom informačnej vojny nie je protivníka oslabiť zvonku, ale oslabiť, dezorientovať a destabilizovať ho zvnútra."* (Halpin a kol., 2006, s. 79)

Čo sa týka histórie termínu informačná vojna (angl. *Information War*, resp. *Information Warfare*), tá siaha do doby studenej vojny, t. j. do čias ešte pred obdobím masívneho nástupu IKT. **Jírovský** (2007) uvádza, že tento termín sa prvýkrát objavil v roku 1976 v štúdii s názvom *Weapons Systems and Information War*, spracovanej **Thomasom P. Ronom**. V tejto štúdii bola informačná vojna opísaná ako boj rozhodovacích systémov, čo však vystihuje iba jeden z možných pohľadov na tento typ konfliktu.

Na vyššom stupni abstrakcie je informačná vojna ponímaná ako ideologické ovplyvňovanie protivníka, pričom sa na tento účel využíva široké spektrum nástrojov, ako napríklad dezinformovanie, propaganda, ale aj diplomacia či vojenský nátlak a pod. Niekde medzi týmito dvoma rovinami potom leží tretia

definícia informačnej vojny, ktorá ju charakterizuje ako *„koncepciu pomáhajúcu (umožňujúcu) konvenčným vojenským silám, transformovateľným v rámci tzv. "Revolution in Military Affairs"* (ďalej len RMA)[3]*, dosiahnuť informačnú prevahu na bojisku.“* (Halpin a kol., 2006, s. 81) V materiáloch súvisiacich s transformáciou americkej armády a aplikáciou konceptu RMA sa definícia informačného boja objavuje ako širšie či užšie vymedzenie boja o získanie informačnej dominancie (prevahy). Informačná vojna je teda chápaná ako konflikt o získanie informačnej dominancie (prevahy). Informačná dominancia je pritom definovaná ako *„schopnosť zhromažďovať, spracovávať a šíriť informácie, zatiaľ čo sa využívajú alebo potláčajú snahy protivníka robiť to isté.“* (US DoD, 2000, s. 8)

Jedným z najvýznamnejších materiálov, ktorý operuje s termínom informačná prevaha a považuje jej získanie za kľúčový predpoklad úspešného vedenia bojových operácií, je dokument amerického ministerstva obrany *Joint Vision 2020*. Ide o súhrnný materiál popisujúci transformáciu amerických ozbrojených síl, pričom práve informačné operácie budú podľa tohto dokumentu hrať v rámci budúcich konfliktov veľmi dôležitú úlohu. Joint Vision 2020 opisuje informačné operácie v tomto kontexte:

- sú kľúčové pre získanie tzv. celospektrálnej dominancie;
- majú uľahčiť a ochrániť rozhodovacie procesy amerických ozbrojených síl a znemožniť to isté protivníkovi;
- zahŕňajú nielen ochranu vlastných počítačových sietí, ale aj psychologické operácie a pod.;
- neustály rozvoj komunikačných a informačných technológií a globálneho informačného prostredia (internetu, atď.) má za následok, že informačné operácie nadobúdajú v súčasnosti rovnaký význam ako operácie na súši, na mori či vo vzduchu;
- pomocou informačných operácií sa má získať informačné prevaha;
- informačná prevaha sama o sebe dáva bojovým jednotkám výhodu iba vtedy, ak je správne využitá;
- informačná prevaha má byť využitá na dosiahnutie maximálnej efektivity všetkých operácií na potenciálnym bojisku budúcnosti (manévru, presných úderov, cielenej logistiky i ochrany vlastných vojsk a pod.). (US DoD, 2000, s. 9 - 10)

[3] Bližšie pozri: *RMA Debate*. Dostupné na internete: <http://www.comw.org/rma/>

3. Informačná vojna verzus klasický konvenčný konflikt

Ako vidieť, informačná vojna je chápaná z rôznych uhlov pohľadu, pričom nájsť jednotný výklad tohto termínu je veľmi ťažké. Celkovo však informačnú vojnu napriek tomu charakterizuje niekoľko výrazných rysov, ktoré ju vymedzujú oproti klasickému konvenčnému typu bojovej činnosti. Rozdielom medzi klasickým konvenčným konfliktom a informačnou vojnou sa venujú viaceré odborné analýzy, materiály a teoretické práce,[4] týkajúce sa budúcnosti amerických ozbrojených síl.

Podľa týchto analýz budú Spojené štáty americké (ďalej len USA) v budúcnosti čeliť zvýšenému riziku napadnutia prostredníctvom tzv. asymetrických útokov, teda útokov, ktoré budú vedené nekonvenčnými cestami, napríklad prostredníctvom sietí. Väčšina z týchto prác operuje s myšlienkou, že prípadný budúci konflikt povedú USA proti nepriateľovi, ktorý bude čo do konvenčných zbraní oveľa slabší, takže sa bude chcieť vyhnúť priamemu stretu a snažiť sa napadnúť Spojené štáty iným spôsobom s využitím niektorých ich slabín. Medzi tieto slabiny patrí okrem iného najmä vzrastajúca závislosť USA na IKT, pričom vyložene nepriaznivo pôsobí najmä fakt, že aj ozbrojené sily (čo však neplatí iba pre americké ozbrojené sily) využívajú v pomerne veľkej miere komerčne dostupné softvérové vybavenie, ktorého slabiny sú dobre známe a ktoré sú teda relatívne ľahko napadnuteľné.

Asymetrickosť prípadného konfliktu a pomerne vysoká závislosť vojenských informačných a komunikačných štruktúr na civilných však nie sú jedinými aspektmi informačnej vojny. Ďalším významným atribútom, ktorý s týmto priamo súvisí, je relatívne ľahká dostupnosť prostriedkov informačnej vojny (*infoware*). Vďaka svojej nízkej obstarávacej cene (napríklad oproti klasickým zbraniam) sú dostupné nielen štátnym aktérom, ale aj rôznym sub-nacionálnym skupinám a bez väčších problémov aj jednotlivým osobám, pričom vďaka relatívne veľmi jednoduchej šíriteľnosti týchto prostriedkov nie je ich výsledný efekt oproti konvenčným zbraniam v podstate takmer nijako limitovaný počtom útočníkov či veľkosťou organizácie, ktorá takýto útok vedie. Jednoducho povedané, v prípade použitia klasických konvenčných zbraní jednotlivec prakticky nemá šancu zasadiť štátu ochromujúci úder alebo mu spôsobiť vážne škody, ktoré by ho paralyzovali.

V prípade informačnej vojny to však už až taký veľký problém byť nemusí, pretože v takomto konflikte má teoreticky aj jednotlivec k dispozícii prostriedky, ktoré toto dokážu. Napríklad vývoj počítačových vírusov a ich kopírovanie nie je

[4] Bližšie pozri napr.: Gelsson, 2012.

ani zďaleka také problematické ako masová výroba strelných zbraní. Celkovo sa dá preto povedať, že potenciálny útočník je v informačnej vojne oproti napadnutej strane vždy v značnej výhode, pretože náklady na vývoj, prípravu a použitie infoware bývajú spravidla oproti potenciálnym škodám, ktoré je takáto zbraň (napríklad počítačový vírus) schopná napáchať, vždy neporovnateľne nižšie. Navyše je v tomto prípade nutné vziať do úvahy fakt, že značné zdroje je nutné investovať do preventívnej ochrany počítačových sietí a informačných a komunikačných zariadení pred takýmto útokom, pričom náklady na dlhodobo udržiavanú ochranu sa môžu vyšplhať relatívne vysoko, a to bez toho, aby k nejakému útoku na ne vôbec niekedy došlo. Samotná hrozba takéhoto útoku je však natoľko odstrašujúca, že si automaticky vyžaduje neustále investície do preventívnych ochranných protiopatrení.

Jednou z ďalších špecifických vlastností prostriedkov informačnej vojny je ich neobmedzený dosah. Potenciálnym terčom informačnej vojny sa stáva v podstate akékoľvek miesto, ktoré je pripojené k inžinierskym sieťam, čo znamená, že sa prakticky úplne stiera rozdiel medzi ,,frontom“ a ,,tylom“, pretože v prípade informačného konfliktu sú všetky miesta v relatívne rovnakom ohrození. Znamená to, že keby napríklad USA viedli klasický konvenčný konflikt, ktorý by však bol sprevádzaný použitím prostriedkov informačnej vojny, ich kľúčové zariadenia na domácej pôde a aj obyvatelia, ktorí sú na nich závislí, by sa mohli ocitnúť vo väčšom ohrození, než ich vojenské jednotky priamo na frontovej línii, vzdialené tisíce kilometrov. Tým pádom sa zároveň tiež stierajú rozdiely medzi civilnými a vojenskými cieľmi, pričom civilná infraštruktúra býva spravidla menej chránená, a teda aj ľahšie zraniteľná, než prvky vojenskej (obrannej) infraštruktúry.

Ďalšou vlastnosťou, ktorou sa informačná vojna líši od klasického ozbrojeného konfliktu, je veľmi obťažná rozpoznateľnosť útoku samotného. Napríklad v prípade kybernetického útoku je často veľmi zložité rozoznať, či vôbec ide o cielený útok, alebo ide iba o náhodu či poruchu. Dôležitú úlohu hrá aj otázka kompetencií. Takýto útok totiž býva z dôvodu zakrytia stôp spravidla vedený cez množstvo serverov nachádzajúcich sa v rôznych štátoch, takže nie je jednoduché určiť, kto je oprávnený vzniknutú situáciu riešiť.

Ďalšou otázkou, ktorá s týmto úzko súvisí, je charakter prípadného útoku. V prípade kybernetického úderu je totiž veľmi zložité posúdiť, či ide o kriminálny alebo vojnový akt, pretože použité zbrane sú v podstate totožné s tými, ktoré sú využívané pri páchaní počítačovej kriminality, takže vyvstáva otázka, čo je vlastne na takýto útok adekvátnou odozvou. Situáciu príliš neuľahčuje ani fakt,

že v prípade rozsiahlejšieho útoku voľba prípadných prvotných terčov nemusí vždy nutne napovedať, čo je skutočným cieľom útočníkov. (Warren, Streeter, 2013)

Informačná vojna dáva oproti klasickému konvenčnému konfliktu tiež oveľa väčší priestor k manipulácii s percepciou obyvateľov. Vzhľadom na to, že prevažná časť aktivít v rámci informačnej vojny sa týka samotnej manipulácie s informáciami, vzniká riziko masívnych kampaní zameraných na ovplyvňovanie obyvateľstva pomocou šírenia skreslených informácií, dezinformácií (napríklad prostredníctvom internetu, ale aj klasických masmédií) a účelového pretvárania faktov pomocou najrôznejších na to určených techník, napríklad digitálne upravovaných fotografií, filmov a pod. (Stein, 2016)

Z vyššie popísaných vlastností je na prvý pohľad zrejmé, že informačnú vojnu ako samostatný fenomén je možné od klasického konvenčného konfliktu veľmi jasne odlíšiť. V tejto súvislosti si je však nutné uvedomiť, že informačná vojna v niektorých svojich formách preberá vlastnosti klasického konvenčného stretu a napríklad vo väčšine súdobých materiálov americkej armády je s ňou počítané len ako s jedným z doplnkov klasického konfliktu, nie ako samostatným typom boja, pomocou alebo prostredníctvom ktorého by bolo možné dosiahnuť celkové víťazstvo.

V niektorých materiáloch[5] je, v nadväznosti na vyššie uvedené, informačná vojna prirovnávaná napríklad ku strategickému bombardovaniu. To je síce samostatným sub-typom vedenia bojovej činnosti a samo o sebe aj pomerne účinným odstrašujúcim nástrojom, avšak jeho (hoci sebe efektívnejšia) aplikácia na bojisku sa ešte zďaleka nerovná jasnému víťazstvu. V prípade informačnej vojny, v porovnaní so strategickým bombardovaním, rozdielom môže byť fakt, že v budúcnosti môže byť naša spoločnosť na IKT závislá do takej miery, že s pomocou nástrojov informačnej vojny bude skutočne možné dosiahnuť celkové víťazstvo. Otázkou, ktorá v tejto súvislosti vyvstáva, je, či sa v budúcnosti nestanú klasické konvenčné metódy boja naopak iba doplnkom informačnej vojny. V takom prípade by sa potom pomocou jednotiek pozemných a vzdušných síl len dovŕšilo ovládnutie priestoru, ktorý by už predtým prakticky kapituloval pod útokom *infoware*.

[5] Bližšie pozri napríklad: Amistead, 2011.

4. Ciele informačnej vojny

V súčasnej spoločnosti, využívajúcej IKT v čím ďalej tým väčšom meradle, neustále pribúdajú potenciálne terče pre prostriedky informačnej vojny. Dá sa povedať, že v súčasnej dobe je už naša spoločnosť na týchto technológiách závislá do tej miery, že zničenie či narušenie funkčnosti týchto systémov by veľmi pravdepodobne viedlo k závažnému ohrozeniu chodu celej spoločnosti či aspoň niektorých jej oblastí, ako napríklad záchranného systému, systému obrany štátu, bankovníctva, rozvodných sietí a pod. Ako najpravdepodobnejšie ciele informačnej vojny sa preto v súčasnosti javia tzv. kritické infraštruktúry (ďalej len KI) a predovšetkým jeden z ich komponentov – kritické informačné infraštruktúry (ďalej len KII).

4.1 Kritické infraštruktúry

Čo sa týka kritickej infraštruktúry, všeobecne možno povedať, že ide o systémy, ktoré sú svojou funkciou absolútne kľúčové pre chod spoločnosti a ich poškodenie alebo prerušenie či narušenie ich fungovania by mohlo mať zásadný negatívny vplyv na chod spoločnosti alebo na životy jeho obyvateľov. Zoznam jednotlivých systémov, ktoré sú považované za kritické, sa líši štát od štátu, avšak zoznam týchto systémov sa v jednotlivých štátoch do značnej miery prekrýva. Postup ich identifikácie je možné definovať na základe prierezových a sektorovo špecifických kritérií, ktoré sú založené na:

a) stratách na životoch (posudzované v zmysle možného počtu mŕtvych alebo zranených osôb),
b) hospodárskom vplyve (posudzované v zmysle závažnosti hospodárskych strát a/alebo zhoršenia výrobkov alebo služieb a zahŕňajúce vplyv na životné prostredie),
c) vplyve na verejnosť (posudzované v zmysle vplyvu na dôveru obyvateľstva, fyzického utrpenia a narušenia každodenného života). (Andrassy, Jasenovec, 2009)

V Slovenskej republike sa KI člení na sektory a prvky. **Sektorom KI** je tá časť KI, do ktorej sa zaraďujú prvky, pričom sektor môže obsahovať jeden alebo viac podsektorov. Prvkom KI sú najmä inžinierske stavby, služby vo verejnom záujme a informačné systémy v sektore KI, ktorých narušenie alebo zničenie by malo podľa sektorových kritérií a prierezových kritérií závažné nepriaznivé dôsledky na uskutočňovanie hospodárskej a sociálnej funkcie štátu, a tým na kvalitu života

obyvateľov z hľadiska ochrany ich života, zdravia, bezpečnosti, majetku, ako aj životného prostredia. (MH SR, 2017)

Z hľadiska obranno-bezpečnostného pohľadu na KI ako na súčasť národnej infra-štruktúry štátu je možné KI definovať ako *„časť národnej infraštruktúry, zahŕňajúcu vybrané organizácie, inštitúcie, objekty, sústavy, zariadenia, služby a systémy, ktorej zničenie alebo znefunkčnenie v dôsledku pôsobenia rizikového faktora spôsobí ohrozenie alebo narušenie politického a hospodárskeho chodu štátu alebo ohrozenie životov a zdravia obyvateľstva. Neoddeliteľnou súčasťou KI sú aj objekty a zariadenia obrannej infraštruktúry. Sektor KI predstavuje taký sektor národnej infraštruktúry, u ktorého zlyhanie niektorej z jeho dôležitých funkcií alebo niektorého jeho prvku spôsobí ohrozenie alebo narušenie niektorej z oblastí bezpečnosti štátu, napríklad politického chodu štátu, vrátane fungovania verejnej správy, obrany a hospodárstva štátu, života, zdravia a majetku jeho obyvateľov, dopravy, komunikačných a informačných systémov, životného prostredia. Prvok KI je zasa taký prvok národnej infraštruktúry, ktorého zničenia alebo narušenie môže mať negatívny vplyv na niektorú z oblastí bezpečnosti štátu.“* (Vláda SR, 2011)

V USA je KI definovaná ako *„systémy a aktíva, či už fyzické alebo virtuálne, natoľko životne dôležité pre Spojené štáty, že zneschopnenie či zničenie týchto systémov a aktív by malo oslabujúci vplyv na národnú ekonomickú bezpečnosť, národné verejné zdravie a celkovú bezpečnosť alebo akúkoľvek kombináciu spomínaného.“* (Moteff, Parfomak, 2004)Výpočet jednotlivých oblastí a štruktúr, ktoré sú chápané ako kritické pre chod americkej spoločnosti, sa v USA v priebehu uplynulých desaťročí priebežne menil, pričom na začiatku nového milénia patrili medzi ne aj národné symboly alebo historické pamiatky. Zaradenie týchto (na prvý pohľad rýdzo symbolických) aktív bolo odôvodnené tým, že ich zničenie by mohlo vážne narušiť morálku obyvateľov Spojených štátov. Neskoršie definície však už tieto symboly neuvádzajú. V súčasnej dobe sú teda v USA medzi kritické infraštruktúry počítané tieto oblasti: vláda, poľnohospodárstvo, potravinárstvo, vodohospodárstvo, zdravotníctvo, pohotovostné zložky, obranný priemysel, informácie a telekomunikácie, energetika, doprava, bankovníctvo a financie, chemický priemysel, poštové služby a lodná preprava. (Moteff, Parfomak, 2004)

V prípade porovnania zoznamov kritickej infraštruktúry aj v iných krajinách sa dá zistiť, že vo všetkých zoznamoch figurujú ako kritická infraštruktúra aj informačné a komunikačné systémy. Z tohto je zrejmé, že táto oblasť je v súčasnej dobe už chápaná ako prvok, bez ktorého by bolo fungovania každého

štátu vážne ohrozené, v podstate nemožné. Význam týchto systémov totiž v súčasnosti vzrástol do takej miery, že je nevyhnutné im venovať minimálne rovnakú pozornosť ako fyzickým štruktúram a službám. Naviac je nutné brať do úvahy fakt, že IKT sú vo väčšej či menšej miere zároveň integrované do všetkých ostatných oblastí, vymenovaných ako kritické infraštruktúry. Tento fakt z nich vytvára zložku úplne primárneho významu. Na rozdiel od všetkých ostatných menovaných oblastí, KI sú oblasťou, ktorá zasahuje do všetkých segmentov ľudskej činnosti. Ich poškodenie či zničenie by teda viedlo k ochromeniu mnohých ďalších kľúčových odvetví.

4.2 Kritické informačné infraštruktúry

Termín kritické informačné infraštruktúry (ďalej len KII) sa v odbornej literatúre nevyskytuje tak často ako kritické infraštruktúry, pretože v tomto prípade ide o oveľa špecifickejšiu oblasť. Z hľadiska definovania: *„Kritická informačná infraštruktúra štátu slúži k informačnému zabezpečeniu riadnej funkčnosti kritickej infraštruktúry štátu, pričom zahŕňa komplex komunikačných a informačných systémov a ich služieb. Zároveň obsahuje súčasti, akými sú telekomunikácie, počítačové systémy a ich programové vybavenie, internet, prenosové siete, poskytované služby, atď."* (Říha, 2007, s. 46)

Z tejto definície okrem iného vyplýva aj fakt, ktorý bol naznačený už vyššie, a teda že KI sú na KII plne závislé a nie sú schopné bez nich správne fungovať. Práve informačná infraštruktúra je v dnešnej informačnej spoločnosti oným kľúčovým komponentom. Dokazuje to napríklad aj portál Európskej únie venovaný Informačnej spoločnosti, kde sa uvádza: *„Elektronické komunikačné služby a siete vytvárajú chrbticu európskeho hospodárstva a sú životne dôležité pre jej občanov, obchodné subjekty a vlády. Bývajú označované ako kritická informačná infraštruktúra. Informačné infraštruktúry ako telefónne linky, optické vlákna a počítačové siete ovládajú životy občanov Únie, a preto musia byť zabezpečené. Závisí na tom značná časť ekonomiky Európskej únie. Množstvo služieb a procesov začalo byť v čím ďalej tým väčšej miere závislých na fungovaní IKT, komunikačno-informačných systémov, prostriedkov a sieťach. S narastajúcou decentralizáciou, vzájomnou prepojenosťou a závislosťou týchto sietí hrozí riziko, že prípadné zlyhanie týchto infraštruktúr môže spôsobiť reťazovú reakciu, prekračujúce štátne hranice."* (EÚ, 2019)

KII na základe toho predstavujú zložku, na ktorej je chod dnešnej informačnej spoločnosti priamo závislý. Narušenie ich funkčnosti či úplné vyradenie týchto systémov z prevádzky by mohlo znamenať ďalekosiahle dôsledky nielen pre

národné hospodárstvo, ale aj pre väčšinu obyvateľov. Ochrana KII je preto v súčasnej dobe jedným z prioritných cieľov všetkých vyspelých štátov. Aké následky by malo reálne napadnutie týchto systémov a ich následné vyradenie z prevádzky možno len veľmi ťažko odhadnúť, avšak potenciál pre vážne narušenie chodu štátu je v prípade vyradenia týchto systémov úplne evidentný. Samozrejme, záleží tiež do značnej miery na tom, ktoré prvky kritickej infraštruktúry by boli takto postihnuté, pretože nie všetky prvky majú rovnaký vplyv na chod štátu a životy jeho obyvateľov.

Záver

Informačné a komunikačné technológie priniesli ľudskej civilizácii ohromný pokrok. Bez akýchkoľvek pochybností ide o technológie prináležiace k tým najvýznamnejším, aké kedy uzreli svetlo sveta. Tieto pokrokové technológie posunuli ľudstvo do úplne nového veku, charakterizovaného celkovou zmenou našej spoločnosti, ktorá sa prejavuje vo všetkých oblastiach – od spôsobu komunikácie, cez výrobu, obchod, kultúru a vzdelávanie, až po životný štýl a trávenie voľného času každého z nás. IKT dnes tvoria neoddeliteľnú súčasť nášho sveta a zasahujú do všetkých oblastí ľudského konania. Vďaka výrazným zmenám v spoločnosti, v nadväznosti na masívne využívanie IKT, však zároveň došlo aj k zmenám v charaktere hrozieb, ktoré ohrozujú bezpečnosť dnešného sveta.

V spôsobe vedenia ozbrojeného zápasu sa vždy odrážal spôsob fungovania súdobej spoločnosti, nakoľko tieto prvky sú spolu pevne späté. V prípade vedenia informačnej vojny boli ako potenciálna Achillova päta nového typu spoločnosti – informačnej spoločnosti –identifikované kritické infraštruktúry, a predovšetkým kritické informačné infraštruktúry, ktoré tvoria v prenesenom slova zmysle "chrbticu" týchto systémov. Ukázalo sa, že hrozba odstavenia týchto systémov z prevádzky pomocou cieleného vonkajšieho zásahu je (hoci k niečomu podobnému zatiaľ v masovom meradle nedošlo) úplne reálna, pričom dôsledky vzniknuté z tejto situácie by boli schopné vážnym spôsobom ohroziť nielen chod napadnutého štátu, ale aj životy jeho obyvateľov.

Využívanie praktík informačnej vojny však nie je iba otázkou vojny samotnej, ale (ako už bolo uvedené vyššie) týka sa aj nášho každodenného života a bežného fungovania spoločnosti, v ktorej dnes žijeme. V tejto súvislosti si však je nutné uvedomiť, že v prípade informačnej vojny nejde len o problém technický či technologický, ale aj o problém spoločenský, bezpečnostný, politický,

legislatívny, atď. Tento fenomén sa neustále a veľmi rýchlo vyvíja, takže prezentované definície častokrát ani nestíhajú obsiahnuť všetky nové atribúty, ktoré v tomto smere vystávajú. Komplikácie pri skúmaní informačnej vojny predstavuje aj jej multidisciplinárnosť a taktiež skutočnosť, že informačná vojna už vo svojej podstate zahŕňa skryté stratégie a taktiky, aby ani samotní účastníci nevedeli, že sa stali jej aktérmi.

Ďalším dôležitým aspektom, ktorý výrazným spôsobom ovplyvňuje skúmanie fenoménu informačnej vojny je fakt, že informačná vojna už dávno prekročila hranice samotného vojenstva. A ešte znepokojivejším je fakt, že tieto hranice postupne, aj pod vplyvom prudkého vývoja nových technológií, zmazáva. Tradičné chápanie vojny tak už v ponímaní informačnej vojny nie je dostačujúce a na základe výsledkov výskumu možno tvrdiť, že tak spoločnosť, ako aj jednotlivci sú už dnes súčasťou informačnej vojny (i keď v drvivej väčšine nevedomky). Fyzické bojiská sa v čoraz väčšej miere presúvajú do virtuálneho priestoru, pričom cieľom už nie je zničiť reálnu fyzickú infraštruktúru nepriateľa, ale zasiahnuť, zničiť, vyradiť alebo aspoň narušiť prevádzku a funkčnosť jeho informačných a komunikačných systémov a sietí, a tým narušiť chod celej jeho spoločnosti.

Literatúra:

AMISTEAD, L. 2011. *Information Operations: Warfare and the Hard Reality of Soft Power*. Washington : Potomac, Inc., 2011. 296 s. ISBN 978-1-59797-355-7.

ANDRASSY, V. – JASENOVEC, J. 2009. Využitie simulačných technológií v ochrane prvkov kritickej infraštruktúry. In *Riešenie krízových situácií v špecifickom prostredí* : *zborník príspevkov zo 14. medzinárodnej vedeckej konferencie*. Žilina : Fakulta špeciálneho inžinierstva Žilinskej univerzity, 2009. ISBN 978-80-554-0014-3.

BARIČIČOVÁ, Ľ. – PAJPACHOVÁ, M. 2016. Policajná organizácia ako garant vnútornej bezpečnosti. In *Právní a bezpečnostní prostředí Evropské unie v teritoriální optice vybraných zemí středoevropského prostoru.* České Budějovice: Vysoká škola evropských a regionálních studií, 2016. ISBN 978-80-7556-005-6, s. 18-26.

BAYER, M. 2006. *Strategic Information Warfare: An introduction.*. Dostupné na internete: <https://link.martin.bayer/book/1057/9780230625839#toc> https://doi.org/10.1057/9780230625839_3

BEARDH, A. J. 2014. *Just War Theory and Information War*. Dostupné na internete: <http://www.iacap.org/proceedings_IACAP13/paper_44.pdf>

BURGEROVÁ, J. 2006. E-learning v dištančnom vzdelávaní na Pedagogickej fakulte PU. In *Dištančné vzdelávanie v aplikovanej informatike DIVAI 2006*, Nitra : Univerzita Konštantína Filozofa, 2006. ISBN 80-8050-975-1.

DANESSI, M. 2013. *Encyclopedia of Media and Communication*. Toronto : University of Toronto, 2013. 752 s. ISBN 978-1-4426-1169-6.

EÚ. 2019. Európska únia: *Information Society*. Dostupné na internete: <https://eur-lex.europa.eu/summary/chapter/information_society.html?root_default=SUM_1_CODED%3D31&locale=en> [cit. 2019-04-30]

GELSSON, W. D. 2012. *War in the Past versus War in the Future*. Trentwood : Arena Publishing, 2012. 228 s. ISBN 978-0-54678-321-0.

GRUBLER, A. 2013. *Technology and Global Change*. Cambridge : Cambridge University Press, 2013. 464 s. ISBN 978-0-5215-4332-3.

HALPIN, E. – TREVORROW, P. –WEBB, D. – WRIGHT, S. 2006. *Cyberwar, Netwar and the Revolution in Military Affairs*. London : Palgrave McMillan, 2006. 253 s. ISBN 978-1-349-54123-2.

IVANČÍK, R. 2011. Fenomén zvaný globalizácia. In *Vojenské reflexie*, 2011, roč. 6, č. 1. ISSN 1336-9202, s. 32 - 49.

JIROVSKÝ, V. 2007. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a tro-jských koních bez tajemství.* Praha: Grada Publishing, 2007. 284 s. ISBN 978-80-247-1561-2.

KAZANSKÝ, R. 2015. *The Theory of Conflicts*. Banská Bystrica : Belianum – vydavateľstvo UMB, 2015. 186 s. ISBN 978-80-557-0970-3.

KOBLEN, I. – SZABO, S. – BUČKA, P. 2011. *Obranné spôsobilosti, výskum, vyzbrojovanie a obranný priemysel v kontexte Európskej spolupráce*. Liptovský Mikuláš : Akadémia ozbrojených síl generála M. R. Štefánika, 2011. 380 s. ISBN 978-80-8040-432-1.

KOLENIČKA, J. 1998. Veda a informačné technológie. In *Zborník z konferencie DIDINFO 98*. Banská Bystrica : Fakulta prírodných vied Univerzity Mateja Bela, 1998. ISBN 978-80-9047-745-5, s. 215 - 225.

KRAMER, F. D. 2014. *NATO's Framework Nations: Capabilities for an Unpredictable World*. In *Atlantic Council*, 2014. Dostupné na internete: <https://www.atlanticcouncil.org/images/publications/NATOs_Framework_Nations.pdf>

KRIŠTOFOVIČOVÁ, E. – JURČACKOVÁ, Z. – ONDRIŠOVÁ, M. 1999. *Terminologický slovník z knižnej a informačnej vedy*. Bratislava : Stimul, 1999. 1 CD-ROM. ISBN 978-80-88982-12-X.

MAREK, J. 2017. Globalizácia ako aktér medzinárodnej bezpečnosti 21. storočia. In *Národná a medzinárodná bezpečnosť – zborník z 8. medzinárodnej vedeckej konferencie*. Liptovský Mikuláš : Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 2017. ISBN 978-80-8040-551-9, s. 297-303.

MAROLLA, C. 2018. *Information and Communication Technology for Sustainable Development*. Boca Raton : CRC Press, 2018. 243 s. ISBN 978-1-35104-522-3.

MH SR. 2017. Ministerstvo hospodárstva Slovenskej republiky: *Definície v oblasti kritickej infraštruktúry*. Dostupné na internete: <https://www.mhsr.sk/ministerstvo/bezpecnost-a-krizove-riadenie/ki-kriticka-infrastruktura/definicie-v-oblasti-ki>

MLEZIVA, E. 2004. *Diktatura informací: jak s námi informace manipulují.* Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, 2004. 133 s. ISBN 80-86898-12-1.

MOTEFF, J. – PARFOMAK, P. 2004. *Critical Infrastructure and Key Assets: Definition and Identification*. [online]. Dostupné na: <http://www.fas.org/sgp/crs/RL32631.pdf>

MURDZA, K. 2006. *Sociológia : Úvod do všeobecnej sociológie a sociologického výskumu*. Bratislava : Akadémia Policajného zboru, 2006. 110 s. ISBN 80-8054-381-X.

NEČAS, P. – UŠIAK, J. 2011. *Nový prístup k bezpečnosti štátu na začiatku 21. storočia*. Liptovský Mikuláš : Akadémia ozbrojených síl generála M. R. Štefánika, 2011. 166 s. ISBN 978-80-8040-401-7.

ONDRIA, P. – KOLLÁR, D. 2011. Vplyv globalizácie na národnú bezpečnosť. In *Bezpečnostné fórum 2011 – zborník vedeckých prác z medzinárodnej vedeckej konferencie*. Banská Bystrica : Fakulta politických vied a medzinárodných vzťahov Univerzity Mateja Bela, 2011. ISBN 978-80-557-0136-3, s. 18 - 22.

RILEY, J. 2015. *What is ICT?* Dostupné na internete: <https://www.tutor2u.net/business/ reference/what-is-ict>

ŘÍHA, J. 2007. Kritická infrastruktura a riziko mimořádné události. In *Urbanismus a územní rozvoj*, 2007, roč. 10, č. 4. ISSN 1212-0855, s. 44 - 51. Dostupné aj na internete: <https://www. uur.cz/images/5-publikacni-cinnost-a-knihovna/casopis/2007/2007-04/08_kriticka.pdf>

SCHEMENT, J. R. 2002. *Encyclopedia of Communication and Information*. New York : McMillan Reference, 2002. 1161 s. ISBN 978-0-02865-383-9.

STEIN, I. 2016. *The Media as an Instrument of Information Warfare*. Dostupné na internete: <https://www.grin.com/document/337247>

SUN TZU. cca 500 rokov p. n. l. *Umenie vojny*. Bratislava : Citadella Publishing, 2013. 85 s. ISBN 978-80-89628-10-0.

ŠIKULA, M. 2005. K metodologickým východiskám ponímania fenoménu globalizácie. In *Ekonomický časopis*, 2005, roč. 53, č. 7. ISSN 0013-3035, s. 663 - 679.

US DoD. 2000. United States Department of Defense: *Joint Vision 2020*. Washington : United States Government Printing Office, 2000. Dostupné na internete: <https://www.hsdl.org/? abstract&did=446826>

UŠIAK, J. – GÖRNER, E. 2017. Economic Theories of Military Regrutation. In *18th International Scientific Conference on International Relations - Current Issues of World Economy and Politics*. Bratislava : Ekonóm, 2017. ISBN 978-80-225-4488-7, s. 1023 - 1033.

Vláda SR. 2011. *Koncepcia kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany*. Uznesenie vlády Slovenskej republiky č. 120 zo 14. februára 2007, č. m. 2489/2007. Dostupné na internete: <https://www.mhsr.sk/uploads/files/1VryBxtU.pdf>

WARREN, P. – STREETER, M. 2013. *Cyber Crime & Warfare: All That Matters*. London : Hachette UK, 2013. 160 s. ISBN 978-1-44419-000-7.