MINISTERSTVO OBRANY SLOVENSKEJ REPUBLIKY
Operačný program Efektívna verejná správa
Európska únia
Európsky sociálny fond

//AÚ// Analytický útvar

Článok 5/2019
OKTÓBER

Ministerstvo obrany SR
https://www.mod.gov.sk/analyticky-utvar-mo-sr/

Dominik Štepanovič

Hybridné hrozby

Slabiny Slovenskej republiky ako ciele hybridných aktivít

Výzvy spojené s hybridnými hrozbami sú v súčasnosti čoraz častejšie používaným nástrojom dosahovania požadovaných cieľov štátnych aj neštátnych aktérov. V hybridnej vojne sú aplikované rozličné nástroje využívajúce zraniteľnosť a slabiny dotknutých subjektov. Predkladaný článok sa bude primárne venovať dvom z nich, ktoré sa v poslednom období výraznejšie prejavujú v podmienkach Slovenskej republiky. Po prvé, kybernetické útoky a po druhé, informačná vojna. Slovenská republika musí byť pripravená reagovať na oba typy hrozieb a efektívne im čeliť.

Hybridné hrozby nemožno jednoznačne definovať vzhľadom na ich premenlivosť a nestálosť.

Definície hybridných hrozieb sú rôzne a musia zostať flexibilné, aby mohli reagovať na premenlivú povahu týchto hrozieb a aby vystihli súbor rôznych nátlakových a podvratných činností a konvenčných či nekonvenčných metód (diplomatických, vojenských, ekonomických a technologických), ktoré môžu rôzne štátne aj neštátne subjekty koordinovaným spôsobom využívať na to, aby dosiahli konkrétne ciele bez formálneho vyhlásenia vojny. Ich definičným znakom je zneužívanie zraniteľnosti cieľa a vytváranie neprehľadných situácií s cieľom narušiť rozhodovacie procesy. Nástrojom hybridných hrozieb môžu byť masívne dezinformačné kampane, ako aj využívanie sociálnych médií na propagandu alebo radikalizáciu, nábor a priame ovládanie svojich priaznivcov. (Spoločný rámec..., 2016)

Hybridný útok predstavuje synchronizované využitie viacerých mocenských nástrojov prispôsobených špecifickým slabinám v celom spektre spoločenských funkcií, s cieľom dosiahnuť synergický efekt. Výhodou hybridného útoku je to, že v úvodných fázach je veľmi ťažké posúdiť, či dochádza k aplikácii hybridných nástrojov. Tie môžu byť aplikované dlhodobejšie, pričom škody sa začínajú prejavovať až oneskorene, keď je už schopnosť cieľa účinne sa brániť dôsledkom týchto útokov značne narušená. (Cullen, 2017)

Priebeh hybridného útoku

Spoločným znakom hybridných hrozieb je útok na kritické body systému – slabiny subjektu.

Hybridné útoky sú mierené na tzv. slabiny štátu. Tie predstavujú kritické body systému (štátu) a ich zneužitie môže viesť k narušeniu fungovania štruktúry celku, alebo jeho jednotlivých častí. Pre zjednodušenie problematiky sa príspevok zaoberá danými slabinami v čase mieru. Vo vojnovom stave, alebo v stave, v ktorom dochádza k eskalácii konfliktu, môžu mať útoky podobný charakter, sú však ďaleko rozsiahlejšie a ich intenzita je vyššia. Hybridné hrozby a ich dopad je náročné pochopiť bez priamej referencie na tieto slabiny, ktoré formujú predstavu o probléme.

Hlavným cieľom hybridných útokov je zmeniť podstatu subjektu. V praxi to znamená, že pôvodca útokov sa snaží narušiť spoločenskú súdržnosť štátu, politický systém, bezpečnostné štruktúry, či celkové fungovanie štátu v medzinárodnom prostredí. Útoky

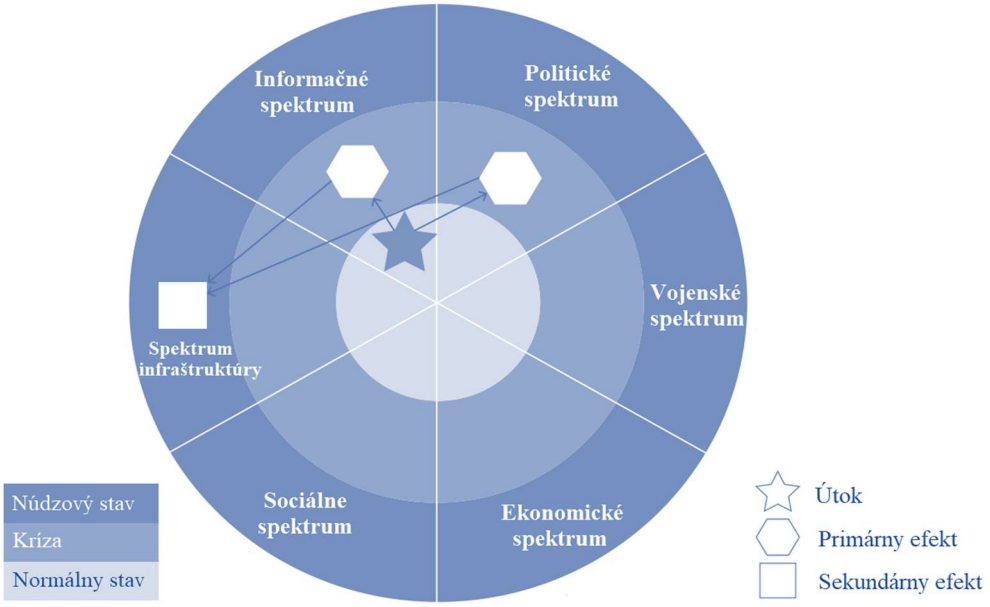
Národný projekt: Budovanie a posilnenie analytických kapacít v rezorte obrany a zavedenie kľúčových znalostných systémov rezortu. Tento projekt je podporený z Európskeho sociálneho fondu.

sú vždy prispôsobované tak, aby do čo najväčšej miery využili slabiny a špecifiká cieľového systému. Hlavnou výhodou takejto stratégie je nemožnosť identifikácie, rozsahu pôsobenia a efektov útoku a predovšetkým konkrétneho spúšťacieho prvku. Ten je totiž kombináciou priamych útokov a existujúcich problémov, takže je náročné identifikovať kauzálny vzťah medzi príčinami a dôsledkami.

Rizikom je pre útočníka fakt, že hybridný útok môže vyvolať sekundárne efekty v protiklade k jeho pôvodným cieľom.

Je dôležité poznamenať, že zvolená stratégia A nemusí nevyhnutne viesť k očakávanému výsledku B. Výsledky zvolených stratégií sú ovplyvňované kontextom krajiny, v ktorej je daná stratégia použitá. (Cullen, 2017) Tento jav predstavuje dvojsečnú zbraň, keďže útočník nedokáže dostatočne predikovať, či jeho akcia vyvolá požadovaný efekt, prípadne nevyvolá sekundárne a terciárne efekty, ktoré budú kontraproduktívne cieľu. Napríklad útoky s cieľom rozdeliť spoločnosť v súvislosti s dlhodobým neriešením problémov národnostnej menšiny môžu mať dvojaký efekt. Buď následkom takýchto útokov zosilnie nacionalizmus a bude ohrozená spoločenská súdržnosť, alebo dôjde k pozitívnym efektom. V napadnutej krajine sa začnú vytvárať inštitúcie, ktoré problematické body dostatočne obhája pred rizikovou časťou populácie a miera slabiny a jej potenciálne využitie sa výrazne oslabí. Nedôjde k požadovanému rozkolu, ale naopak k zosilneniu štruktúry.

Obrázok 1 Vizualizácia hybridného útoku



ZDROJ: Cullen, 2017

V prípade obrázku 1 došlo k útoku na slabinu informačného spektra v normálnom stave. Jeho efekty sa primárne prejavili v informačnom a politickom spektre a vyvolali zmenu stavu slabiny, a to na stav krízy. Následne sa efekty preliali a prejavili ako sekundárny efekt v infraštruktúre, kde vyvolali núdzový stav slabiny. V prípade hybridného útoku by pravdepodobne došlo k simultánnym útokom na viac slabín naraz, čo by situáciu a identifikáciu priamej príčiny výrazne sťažilo. Významným produktom hybridného útoku je miera prelievania či už je úmyselná, alebo pôsobí ako vedľajší produkt aktivity.

Slabiny a ich využitie proti Slovenskej republike

Podľa správ slovenských spravodajských služieb (Vojenské spravodajstvo, Slovenská informačná služba) v súčasnosti nedochádza k výraznému, masívnemu využívaniu hybridných nástrojov voči Slovenskej republiky. Dochádza ale k menším útokom hybridného charakteru, no nie k aplikácii cielenej sofistikovanej stratégie v takom rozsahu, ktorý je zvyčajne badateľný pri masívnych hybridných útokoch.

Podľa správy VS (2018) na Slovensku došlo k nárastu rizika kybernetických útokov zo strany síl cudzej moci.

Výročná správa Slovenskej informačnej služby uvádza, že „*...SR doteraz nebola predmetom intenzívnejšej, špecificky zameranej hybridnej kampane niektorého zo štátnych alebo neštátnych aktérov a nebolo proti nej zaznamenané ani použitie agresívnejších prostriedkov ako sú rozsiahle kybernetické útoky zamerané na znefunkčnenie infraštruktúry, priama podpora extrémistov, či masívna snaha získavať citlivé informácie (napr. mailovú komunikáciu politicky činných osôb), ktoré môžu byť manipulované a využiteľné pri diskreditácii a oslabení politických síl, ktoré nevyhovujú záujmom útočníkov.*“ (SIS, 2019) V priestore Slovenskej republike sa aplikácia hybridných aktivít sústreďuje najmä na oblasť propagandy a dezinformácií, ktorých efekty sa následne prelievajú do iných oblastí. Koncom roka 2018 došlo tiež ku kybernetickému útoku na Ministerstvo zahraničných vecí a európskych záležitostí SR. Informácie o iných kybernetický útokoch na štátne inštitúcie neboli medializované.

Vojenské spravodajstvo vo svojej správe uvádza, že došlo k zvýšeniu rizika pravdepodobnosti kybernetických útokov síl cudzej moci, ktoré spadajú pod hybridný spôsob vedenia bojových činností. Uvádza, *že „...boli získané viaceré informácie, ktoré indikovali útoky na informačné, alebo komunikačné systémy verejnej a štátnej správy s použitím škodlivého kódu vykazujúcim znaky pokročilých pretrvávajúcich hrozieb - APT. V prípade hackerských skupín boli získavané poznatky o ich štruktúre, zameraní činnosti, možnej podpore zo strany štátnych/neštátnych aktérov a prebiehajúce kybernetické kampane, na ktorých participujú. V súvislosti s taktikou, metodikou a postupmi, využívanými pri kybernetických operáciách, boli monitorované aj nové formy aktivít a spôsobilosti, ktoré využívajú rôzne druhy zraniteľností. V hodnotenom období boli vyhodnocované indikátory prepojenia takýchto zoskupení s problematikou pôsobenia cudzích spravodajských služieb a aktivít cudzej moci v rámci hybridného spôsobu vedenia bojových operácií.* (VS, 2019)

V prípade útoku na MZVaEZ SR nebol špecifikovaný pôvodca útoku a ani jeho štátna príslušnosť. Premiér Peter Pellegrini uviedol, že „*...kybernetický útok bol aktivovaný zo zahraničia. Ide o nadnárodnú sofistikovanú špionážnu organizáciu, ktorá je schopná prenikať do informačných systémov štátov.*“ (Ministerstvo zahraničných vecí..., 2018) Cieľom útoku bol zisk osobných dát, nie utajovaných materiálov. Kybernetické útoky ako prostriedok aplikácie hybridných aktivít sú veľmi účinné z niekoľkých dôvodov. Takýto útok je uskutočniteľný pri relatívne nízkych nákladoch pre útočníka. Náklady, ktoré musí cieľ útoku vynaložiť na obranu, sú niekoľkonásobne vyššie, čo útočníka stavia do výhodnej pozície. Rovnako je veľmi náročné vystopovať pôvodcu kybernetických útokov. V prípade profesionálnych hackerov je to so súčasnými technológiami takmer nemožné, pokiaľ samotný útočník nespraví zásadnú chybu. Na bližšiu identifikáciu útočníka sa používa aj preskúmanie štýlu útoku, ktorý je pri niektorých útokoch rovnaký, pozostáva z podobnej taktiky, obsahuje podobne napísaný škodlivý kód.

Keďže útok nie je vo veľa prípadoch možné prisúdiť páchateľom, otázka potrestania vinníkov je ďalším problémovým bodom. Kybernetický útok nemá rovnakú právnu rovinu ako konvenčný útok, napriek tomu, že jeho dôsledky môžu byť ďalekosiahle. Dokonca aj v zriedkavých situáciách, kedy sú identifikovaní páchatelia kybernetického útoku, nie je postup v riešení vždy dostatočne razantný.

V októbri 2018 napríklad Holandsko zadržalo príslušníkov ruskej vojenskej rozviedky pri pokuse o hackerský útok na Organizáciu pre zákaz chemických zbraní. Reakciou na útok bolo ich vyhostenie. Politická reakcia pozostávala z verejného odsúdenia útokov. (Holandsko prekazilo ruský..., 2018) Diametrálne odlišnú reakciu mal Izrael počas kybernetického útoku na jeho strategickú infraštruktúru. Izrael identifikoval budovu, z ktorej prebiehal kybernetický útok a zbombardoval ju. Ide o prvý príklad využitia vojenskej sily proti kybernetickému útoku. (Doffman, 2019) Táto reakcia je kontroverzná, ale predstavuje efektívnu odpoveď na hybridný útok a môže sa stať precedensom. Zvažuje sa, že v prípade útoku na jednu doménu (napr. kybernetický útok), by malo dôjsť k odpovedi na inú doménu (limitovaná vojenská akcia na infraštruktúru útočníka). V prípade, že by sa takýto typ odpovede zlegitimizoval, útočník by nevedel, v akej oblasti jeho útok vyvolá odpoveď, čo môže byť dostatočným odstrašujúcim mechanizmom. (MCDC, 2019)

V Slovenskej republike sa aplikácia hybridných aktivít sústreďuje najmä na oblasť propagandy a dezinformácií.

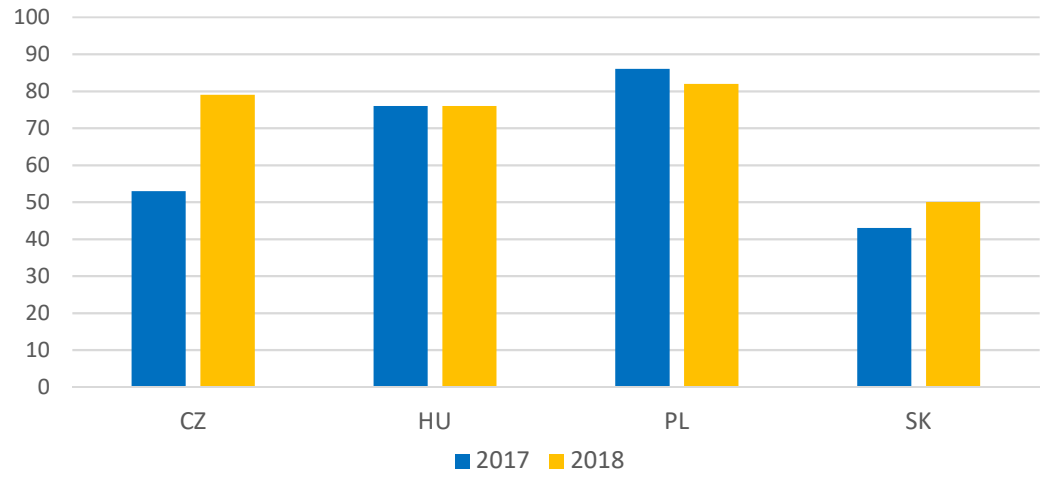
Zdá sa, že najväčším problémom v kontexte aplikácie hybridných hrozieb na slabiny na Slovensku je vplyv dezinformácií a propagandy. Tá je efektívna najmä preto, že nepôsobí iba na jednu slabinu, ale na celé spektrum. Jedným z ich efektov je znižovanie dôvery verejnosti voči mainstreamovým médiám a erózia naratívov. Častokrát nie je cieľom jednoznačne spochybniť oficiálny výklad udalostí, ale poskytnúť alternatívne vysvetlenie a spochybniť dôveryhodnosť zdroja. V tomto priestore neexistuje základ, na ktorom je možné stavať a z neho prisudzovať zmysel udalostiam, ale vytvára neistotu v celospoločenských otázkach. Znižovanie miery dôvery verejnosti k mainstreamovým médiám sa odráža na podpore tzv. alternatívnych médií, ktoré, ako sa prezentujú, ponúkajú pohľad na problematiku z inej strany. Táto alternatíva však vo väčšine prípadov neodzrkadľuje inú optiku, ale vyhradzuje sa voči mainstreamu a šíri dezinformácie a falošné správy.

Výročná správa Vojenského spravodajstva uvádza, že „...v *súvislosti s negatívnymi účinkami propagandy na strategickej úrovni je dlhodobo zaznamenávané systematické a cielené šírenie špecifických naratívov. Nejde len o naratívy, ktorých predpokladaným cieľom je narušenie kohézie EÚ a NATO, alebo také, ktoré sú založené najmä na spomienkovom optimizme tzv. „slovanskej histórie“. Zaznamenávané sú vo veľkej miere najmä naratívy, ktoré sú ideovo založené resp. využívajú spoločenské deliace línie, ktoré obsahujú potenciál pre vznik konfliktov. Najväčšou výzvou vo vzťahu k strategickej propagande aj naďalej zostáva presné systémové zadefinovanie varovných problémov a zostavenie sústavy spoľahlivých indikátorov nevyhnutných pre objektívne vyhodnocovanie tejto hrozby. Dôvodom potreby takéhoto rámcovania je, že je veľmi problematické spoľahlivo a objektívne rozlíšiť, ktoré naratívy sú výsledkom cielených škodlivých aktivít externých bezpečnostných aktérov a ktoré sú napríklad v polarizovanej spoločnosti prirodzeným výsledkom legitímnych spoločenských, alebo vnútropolitických procesov, či len prirodzeným výsledkom videnia sveta jednotlivcami, alebo sociálno - spoločenskými zoskupeniami. Bez takéhoto rámcovania nie je možné nastaviť strategickú komunikáciu ani prijímať ďalšie efektívne protiopatrenia.*“ (VS, 2019)

Jedným z dôsledkov týchto aktivít je aj existencia vysokej miery občanov, ktorí veria konšpiračným teóriám a nedôverujú v západnú orientáciu Slovenskej republiky a jej integráciu do západných štruktúr. Mimovládna organizácia Globsec vykonala v tejto oblasti niekoľko výskumov. Graf 1 a 2 zobrazujú, že Slovensko má spomedzi krajín V4 vysokú mieru inklinácie veriť v konšpirácie a že jeho orientácia smerom do štruktúr NATO je vo vysokej miere nepodporovaná.

SR v roku 2018 vykazovala najnižšiu mieru inklinácie k zotrvaniu v NATO v rámci štátov V4.

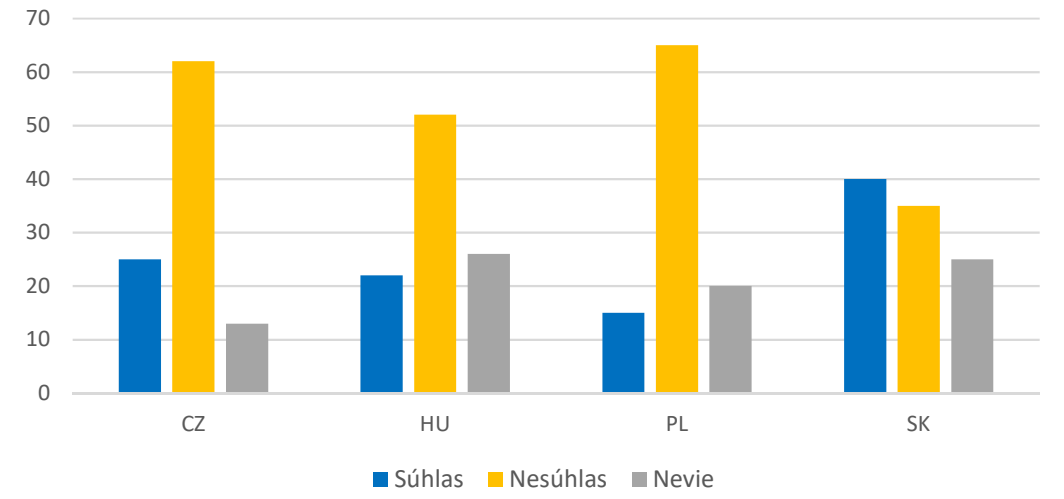
Graf 1 Percento respondentov z krajín V4, ktorí by chceli, aby ich štát zotrval v NATO v prípade, že by sa u nich najbližší víkend konalo referendum o členstve v NATO



ZDROJ: Globsec, 2018

Obyvatelia SR majú podľa prieskumov vyššiu tendenciu veriť konšpiračným teóriám, než občania zvyšných troch štátov V4.

Graf 2 Odpovede respondentov z V4 krajín na otázku: „Do akej miery súhlasíte alebo nesúhlasíte s nasledovným tvrdením – NATO a koalícia vedená USA podporuje teroristov v Sýrii?“



ZDROJ: Globsec, 2018

Záver

Slovenská republika má niekoľko slabín, ktoré môžu byť potenciálne využité voči jej záujmom v rámci hybridného spôsobu vedenia boja. Sú nimi najmä zneužiteľnosť kybernetického priestoru a využitie dezinformácií na ovplyvňovanie verejnej mienky. Niektoré z nich využívané nie sú, niektoré čiastočne, a na niektoré je vyvíjaný mierny tlak. Predpokladá sa, že hybridné útoky budú v konfliktoch budúcnosti tvoriť významnú časť spôsobu vedenia boja. Veľmi dôležitú úlohu tu preto budú mať spravodajské služby, ktorých fungovanie je pre bezpečnosť štátu kritické. Slovenská republika sa v súčasnosti nenachádza v hlavnom ciele záujmov útočníkov, situácia by však nemala byť podceňovaná minimálne kvôli konfliktu na Ukrajine, v ktorom hybridné útoky tvoria významnú časť vojenskej taktiky. Tým, že z politickej a geopolitickej pozície sme schopní dostatočne sledovať udalosti a ich vývin, mali by sme k danej problematike pristupovať preventívne a zodpovedne. Hybridné slabiny by mali byť mitigované, aby ich v prípade zmeny situácie bolo náročnejšie zneužiť. Vo všeobecnosti by mali byť dobre odkomunikované problémové spoločenské témy a mala by sa zintenzívniť snaha o ich riešenie. Je potrebné dbať na úroveň komunikácie medzi štátmi a verejnosťou. Dbať na transparentnosť a otvorenosť v rámci zákona. Mala by existovať jednota v medzinárodnej orientácii politických špičiek. Tie by mali nasledovať snahu o limitovanie dezinformácií a propagandy, ktoré nesmú byť využívané v rámci politického boja. V oblasti kybernetickej bezpečnosti je potrebné zvýšiť schopnosť štátu brániť sa tak, aby sa kybernetický útok stal pre pôvodcu rizikovou a nákladnou operáciou, či už z finančného hľadiska alebo z pohľadu možnej retribúcie.

Článok vyšiel v zborníku príspevkov z konferencie „Národná a medzinárodná bezpečnosť 2019“, AOS LM

Materiál prezentuje názory autora a Analytického útvaru MO SR, ktoré nemusia nevyhnutne odzrkadľovať oficiálne názory a politiky Ministerstva obrany SR. Cieľom výstupov AÚ je podnecovať a zlepšovať odbornú a verejnú diskusiu na aktuálne témy v oblasti obrannej a bezpečnostnej politiky štátu. Práca neprešla jazykovou úpravou.

Referencie

Cullen, P. (2017), *Understanding Hybrid Warfare,* Multinational Capability Development Campaign, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf (cit. 2019-09-13).

Doffman, Z. (2019), *Israel Responds to Cyber Attack With Air Strike On Cyber Attackers in World First,* Forbes, https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first (cit. 2019-09-11).

Globsec, (2018), *Globsec Trends 2018 Central Europe: One Region, Different Perspectives*, https://disinfoportal.org/wp-content/uploads/ReportPDF/GLOBSEC-Trends-2018.pdf (cit. 2019-09-13).

Holandsko prekazilo ruský útok hackerov na Organizáciu pre zákaz chemických zbraní (2018), sme.sk, https://svet.sme.sk/c/20929395/holandsko-prekazilo-rusky-utok-hackerov-na-na-organizaciu-pre-zakaz-chemickych-zbrani.html (cit. 2019-09-05).

MCDC, 2019, *The State of Current Counter-Hybrid Warfare Policy*, Multinational Capability Development Campaign https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/803970/20190519-MCDC_CHW_Info_note_10-State_of_current_policy.pdf (cit. 2019-09-05).

Ministerstvo zahraničných vecí napadli hackeri. Podľa analytika prišiel útok zrejme z Ruska (2018), noviny.sk, https://www.noviny.sk/krimi/379592-ministerstvo-zahranicnych-veci-napadli-hackeri-podla-analytika-prisiel-utok-zrejme-z-ruska (cit. 2019-09-12).

SIS (2019), *Správa o činnosti SIS za rok 2018,* Slovenská informačná služba, http://www.sis.gov.sk/pre-vas/sprava-o-cinnosti.html (cit. 2019-09-13).

Spoločný rámec EÚ pre boj proti hybridným hrozbám (2016), Eur-lex, https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX%3A52016JC0018 (cit. 2019-09-12).

VS (2019), *Správa o činnosti Vojenského spravodajstva za rok 2018*, Vojenské spravodajstvo, http://vs.mosr.sk/sprava-o-cinnosti-vs-2018.html (cit. 2019-09-05).