Operačný program
Efektívna
verejná správa

Európska únia
Európsky sociálny fond

MAPOVANIE ZRANITEĽNOSTI SLOVENSKEJ REPUBLIKY V OBLASTI HYBRIDNÝCH HROZIEB

GLOBSEC
IDEAS SHAPING THE WORLD

Tento projekt je podporený z Európskeho sociálneho fondu.

MAPOVANIE ZRANITEĽNOSTI SLOVENSKEJ REPUBLIKY V OBLASTI HYBRIDNÝCH HROZIEB

GLOBSEC je nezávislá mimovládna organizácia aktívna v oblasti domácej, medzinárodnej a európskej politiky a bezpečnosti viac ako 20 rokov. Vďaka medzinárodnému tímu, projektom, podujatiam, ako sú GLOBSEC Bratislava Forum a GLOBSEC Tatra Summit, a spoluprácou s poprednými organizáciami, medzinárodnými expertmi a súkromným sektorom, sa GLOBSEC stal zdrojom expertízy nielen v oblasti bezpečnosti a zahraničnej politiky, ale aj v otázkach týkajúcich sa kybernetickej bezpečnosti a strategickej komunikácie v regióne celej strednej Európy.

HLAVNÝ AUTOR

Daniel Milo

AUTORI KAPITOL

Pavol Draxler

Katarína Klingová

Matúš Mišík

Daniel Milo

Michal Piško

Na príprave publikácie sa podieľali Dominika Hajdu, Iveta Kupková a Tomáš Tabiš.

Informácie v tejto publikácii sú aktuálne k 1. októbru 2018.

METODOLÓGIA

V procese prípravy tejto štúdie jej autori čerpali z výsledkov anonymného dotazníkového zisťovania v prostredí verejnej správy, do ktorého sa zapojilo vyše 190 respondentov, výsledkov hĺbkových rozhovorov s predstaviteľmi verejnej správy na centrálnej, ako i regionálnej úrovni, a z analýzy legislatívy a verejných politík prijatých na úrovni EÚ, NATO a na Slovensku.

GLOBSEC, Bratislava, Október 2018

GLOBSEC
Vajnorská 100/B
831 04 Bratislava

www.globsec.org

Táto publikácia bola vydaná v rámci projektu „Zvyšovanie pripravenosti a kapacít verejnej správy na hybridné hrozby“, ktorý sa realizuje vďaka Operačnému programu Efektívna verejná správa, a podpore z Európskeho sociálneho fondu.

OBSAH

ÚVOD DO PROBLEMATIKY HYBRIDNÝCH HROZIEB

„Hybridné činnosti štátnych a neštátnych aktérov naďalej predstavujú závažnú a akútnu hrozbu pre EÚ a jej členské štáty. Úsilie zamerané na destabilizáciu krajín tým, že sa oslabí dôvera verejnosti vo vládne inštitúcie, a spochybnením základných hodnôt spoločností, sa stáva stále bežnejším. Naše spoločnosti čelia vážnym problémom spôsobeným tými, čo sa snažia škodiť EÚ a jej členským štátom, počnúc kybernetickými útokmi, ktoré narúšajú hospodárstvo a verejné služby, cez cielené dezinformačné kampane až po agresívne vojenské akcie.

Hybridné kampane majú viacrozmerný charakter, kombinujú v sebe donucovacie a podvratné opatrenia, pričom využívajú konvenčné aj nekonvenčné nástroje a taktiky (diplomatické, vojenské, ekonomické a technologické) s cieľom destabilizovať protivníka. Sú navrhnuté tak, aby ich bolo ťažké odhaliť alebo nájsť ich pôvodcu, a môžu ich použiť tak štátne, ako aj neštátne subjekty.“

Spoločné oznámenie Európskemu parlamentu, Európskej rade a Rade: Zvyšovanie odolnosti a posilňovanie spôsobilosti riešiť hybridné hrozby, jún 2018[1].

Všetky štáty sveta používajú na presadzovanie svojich geopolitických, ideologických či politických záujmov rôzne prostriedky: od diplomacie cez ekonomickú a energetickú politiku a tajné služby až po nasadenie ozbrojených síl. Ako možno pozorovať napríklad na vývoji bezpečnostnej situácie v okolí Slovenskej republiky, formy medzištátnych konfliktov sa zmenili a otvorené presadzovanie záujmov vojenskou silou nahradila kombinácia rôznych koordinovane pôsobiacich vplyvov, ktoré sa však vo svojom dopade takmer vyrovnávajú vojenskej okupácii. Takémuto centrálne riadenému, koordinovanému a častokrát skrytému pôsobeniu štátnych aj neštátnych aktérov s cieľom dosahovania konkrétnych politických cieľov sa hovorí hybridné hrozby.

Na pôde Európskej únie (EÚ) a NATO sa problematike hybridných hrozieb venuje značná pozornosť, preto bolo prijatých viacero dokumentov.[2] Taktiež boli vytvorené aj špecializované inštitúcie - The European Centre of Excellence for Countering Hybrid Threats (Európske centrum na boj proti hybridným hrozbám), EU Hybrid Fusion Cell (Integrovaná spravodajská jednotka zameraná proti hybridným hrozbám) v rámci EU INTCEN (Spravodajské a situačné centrum Európskej únie), NATO StratCom CoE (Centrum excelentnosti NATO na strategickú komunikáciu) a NATO Cooperative Cyber Defence Centre of Excellence (Spoločné centrum excelentnosti NATO na kybernetickú obranu).

V podmienkach Slovenskej republiky (SR) sa pojem hybridné hrozby prvýkrát objavil vo verejných politikách v roku 2016 v *Bielej knihe o obrane Slovenskej republiky*[3], následne v rámci procesu tvorby *Bezpečnostnej stratégie SR* a v neposlednom rade sa premietol do nedávno prijatej *Koncepcie pre boj SR proti hybridným hrozbám.*

Cieľom predkladanej východiskovej štúdie je zmapovať problematiku hybridných hrozieb najmä v kontexte SR vo všeobecnej rovine, ako aj v jednotlivých špecifických druhoch ohrození, identifikovať medzery a zraniteľné miesta a navrhnúť rámcové odporúčania na ich odstránenie.

1 Európska komisia, Zvyšovanie odolnosti a posilňovanie spôsobilosti riešiť hybridné hrozby, 2018, https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:52018JC0016&from=SK
2 Európska komisia, Spoločný rámec pre boj proti hybridným hrozbám, 2016, https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:52016JC0018&from=EN; European Parliament, Countering hybrid threats: EU-NATO cooperation, Záznam z briefingu – nadväzuje na Joint Framework, 2017, http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599315/EPRS_BRI(2017)599315_EN.pdf
3 Ministerstvo obrany Slovenskej republiky, Biela kniha o obrane Slovenskej republiky, 28. september 2016, http://www.mod.gov.sk/data/BKO2016_LQ.pdf

HLAVNÉ ZISTENIA A ODPORÚČANIA

„Hybridné hrozby predstavujú súbor rôznych nátlakových a podvratných činností a konvenčných a nekonvenčných metód (napríklad diplomatických, vojenských, ekonomických a technologických), ktoré môžu rôzne štátne aj neštátne subjekty koordinovaným spôsobom využívať na to, aby dosiahli konkrétne ciele bez toho, aby formálne vyhlásili vojnu. Snahou je obyčajne zneužívať zraniteľnosť cieľa a vytvárať neprehľadné situácie s cieľom narušiť rozhodovacie procesy.“[4]

Medzi najčastejšie nástroje využívané v kontexte hybridných hrozieb patria:

1. externý alebo interný politický nátlak na najvyšších štátnych predstaviteľov a štátne inštitúcie;
2. ekonomický alebo energetický nátlak ako rozšírenie politického nátlaku;
3. rozsiahle sabotáže proti kľúčovej infraštruktúre;
4. kybernetické útoky s potenciálom spôsobiť škody veľkého rozsahu;
5. informačné a propagandistické operácie s cieľom podkopať dôveru v štátne inštitúcie, vyvolať spoločenské nepokoje a vážne destabilizovať politickú a bezpečnostnú stabilitu;
6. ovplyvňovanie etnických, náboženských a kultúrnych menšín a ich manipulácia na politické účely;
7. hrozba použitia vojenskej sily;
8. aktivity nepravidelných/polovojenských ozbrojených skupín nelojálnych k štátu;
9. výzvedné a podvratné aktivity tajných služieb;
10. strategická korupcia využívaná s politickými cieľmi a motívmi;
11. ovplyvňovanie volebných procesov cudzou mocou.

Napriek tomu, že kombinácia týchto vplyvov sa začala označovať pojmom hybridné hrozby iba pomerne nedávno, koordinované využívanie rôznych druhov pôsobenia s cieľom dosiahnuť strategické, politické či geopolitické ciele je oveľa staršie. Nájdeme ich ako princípy v Umení vojny od čínskeho filozofa Sun-c‘, ale i v konceptoch aktívnych opatrení, maskirovky a propagandy z čias Sovietskeho zväzu. V súvislosti s hybridnými hrozbami sa v relevantných dokumentoch prijatých na pôde EÚ, NATO a na vnútroštátnej úrovni najviac hovorí o využívaní týchto nástrojov zo strany Ruskej federácie a zo strany neštátnych aktérov ako je ISIS. Najmä Ruská federácia sa po vypuknutí konfliktu na východnej Ukrajine, anexii Krymu a snahách o ovplyvňovanie volieb vo viacerých krajinách sveta pomocou dezinformačných kampaní a hackerských útokov označuje za hlavného nositeľa takýchto snáh[5].

Na pôde EÚ je najdôležitejším dokumentom vo vzťahu k problematike hybridných hrozieb *Spoločný rámec na boj proti hybridným hrozbám* prijatý v roku 2016, ktorý po prvýkrát komplexne identifikoval jednotlivé zraniteľnosti a navrhol konkrétne kroky na ich odstránenie. Na národnej úrovni je takýmto dokumentom *Koncepcia pre boj SR proti hybridným hrozbám*[6] z júla 2018, ktorá jednak definuje hybridné hrozby, a zároveň určuje kompetencie a pôsobnosť jednotlivých orgánov štátnej správy a zložiek bezpečnostného systému pri ich monitorovaní, analýze a riešení.

4 Európska komisia, Spoločný rámec pre boj proti hybridným hrozbám, 2016, str.2, https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:52016JC0018&from=EN

5 Viď napr. Parlamentné zhromaždenie NATO, Výbor pre obranu a bezpečnosť, Countering Russia’s Hybrid Threats: An update, Draft Special Report, 2018, https://www.nato-pa.int/download-file?filename=sites/default/files/2018-04/2018%20-%20COUNTERING%20RUSSIA%27S%20HYBRID%20THREATS%20-%20DRAFT%20SPRING%20REPORT%20JOPLING%20-%20061%20CDS%2018%20E.pdf

6 Koncepcia pre boj SR proti hybridným hrozbám, schválená vládou SR dňa 11. júla 2018 uznesením č. 345/2018, http://www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=27668

Z HĽADISKA EXISTUJÚCICH MEDZIER A ZRANITEĽNOSTÍ SR MOŽNO ZA NAJDÔLEŽITEJŠIE POVAŽOVAŤ NASLEDOVNÉ:

1. Nedostatočné kapacity v oblasti strategickej komunikácie na úrovni ústredných orgánov štátnej správy.
2. Poddimenzované analytické kapacity v oblasti kybernetickej bezpečnosti a absencia dostatočne konkrétnych a merateľných opatrení na zlepšenie súčasného stavu v tejto oblasti.
3. Nedostatočná pozornosť energetickej infraštruktúry v kontexte hybridných hrozieb a dosahu prípadného útoku na túto infraštruktúru nad rámec prerušenia dodávok energií.
4. Absencia právnej úpravy polovojenských/paramilitárnych skupín.
5. Nedostatočné zohľadnenie prvku cudzej moci pri iných typoch ohrození bezpečnosti a stability Slovenskej republiky.
6. Absencia zohľadnenia iných než čisto finančných motívov v anti-korupčnej legislatíve – strategická korupcia s politickými motívmi a zapojením cudzej moci.
7. Súčasné znenie legislatívy súvisiacej s financovaním politických strán a volebných kampaní neobsahuje ustanovenia umožňujúce identifikovať skutočných darcov-prispievateľov, ktorí môžu konať pomocou tretích subjektov.
8. Absencia špecifickej právnej úpravy o vedení volebnej kampane v prostredí internetu a sociálnych sietí.

VZHĽADOM NA VYŠŠIE UVEDENÉ MEDZERY, MEDZI NAJDÔLEŽITEJŠIE ODPORÚČANIA PATRIA:

1. Prijať komplexný prístup v oblasti strategickej komunikácie, zahŕňajúci všetky relevantné zložky verejnej správy.
2. Zriadiť špecializované národné kapacity so zameraním na strategickú komunikáciu vo všetkých relevantných rezortoch.
3. Vytvoriť analytické kapacity v oblasti kybernetickej bezpečnosti, ktoré by sa zaoberali tvorbou verejných politík.
4. Prijať akčný plán v oblasti kybernetickej bezpečnosti s jasnými, merateľnými kritériami.
5. Systematicky riešiť otázku hybridných/kybernetických hrozieb v strategických dokumentoch, ktoré sa venujú energetickej politike, resp. energetickej bezpečnosti.
6. Klásť väčší dôraz na špecifiká energetického sektora, ktorý je odlišný od ostatných oblastí kritickej infraštruktúry, pretože hybridné hrozby v tejto oblasti majú dôsledky nielen pre energetickú bezpečnosť, ale aj pre tzv. “hard security”.
7. Identifikovať hybridné hrozby a riešenia nielen na úrovni verejnej/štátnej správy, ale aj v rámci (polo)súkromného energetického sektora, ktorý hrá dôležitú úlohu pri zabezpečovaní energetickej bezpečnosti.
8. Zahrnúť “smart” technológie do diskusie o možných hybridných hrozbách v oblasti energetickej bezpečnosti.
9. Novelizovať legislatívu v oblasti zbraní a streliva a prijať legislatívu upravujúcu pôsobenie polovojenských skupín a ich podporu zo strany cudzej moci.
10. Vytvoriť ľahko dostupné, nízkoprahové alternatívy pre mládež so záujmom o vojenstvo a históriu, pod dozorom štátu a so zapojením Ozbrojených síl SR.

11. Dôsledne uplatňovať ustanovenia Trestného zákona týkajúce sa účasti na bojovej činnosti organizovanej ozbrojenej skupiny na území iného štátu a jej podpory.

12. Posilňovať medzinárodné, ale aj domáce nástroje na odhaľovanie podozrivých finančných tokov cez schránkové firmy a daňové raje v kontexte strategickej korupcie s politickými cieľmi.

13. Analyzovať nefinančné aspekty korupcie a zakotviť pojem strategická korupcia do verejných politík a legislatívy.

14. Prijať legislatívu, ktorá upraví transparentné financovanie politických strán počas celého volebného obdobia, nielen v čase trvania predvolebnej kampane.

15. Upraviť okruh subjektov oprávnených financovať volebné kampane počas volieb do Národnej rady SR a Európskeho parlamentu podobným spôsobom, ako je to v prípade prezidentských volieb.

16. Zaviesť povinnosť informovania o zadávateľovi online politických reklám aj v čase mimo predvolebnej kampane.

1. DEFINOVANIE HYBRIDNÝCH HROZIEB A SÚVISIACICH POJMOV

Existuje množstvo definícií, ktoré sa snažia zachytiť špecifickú povahu nových druhov hrozieb pre bezpečnosť a stabilitu štátu, ktoré koordinovane a plánovito využívajú rôzni aktéri. V tejto súvislosti sa najčastejšie hovorí o hybridných hrozbách (hybrid threats) a hybridných spôsoboch vedenia vojny (hybrid warfare). Táto východisková štúdia pracuje najmä s konceptom hybridných hrozieb, ale je dôležité uviesť aj širší rámec a ostatné javy, ktoré sa spájajú s týmto konceptom.

HYBRID WARFARE - HYBRIDNÉ SPÔSOBY VEDENIA VOJNY

Pojem, ktorý sa úzko spája s problematikou hybridných hrozieb, je hybrid warfare - hybridná vojna alebo hybridné spôsoby vedenia vojny. Hoci sa do značnej miery prekrýva s pojmom hybridné hrozby, existujú medzi nimi rozdiely.

Hybridná vojna môže byť definovaná ako *„použitie asymetrických taktík na skúmanie a využívanie zraniteľností protivníka prostredníctvom nevojenských prostriedkov (ako sú politické, informačné a hospodárske zastrašovanie či manipulácia), ktoré sú podporované hrozbou konvenčnej a nekonvenčnej armády"*.[7] V kontexte NATO znamená hybridná vojna *„kampaň proti spojencovi alebo Aliancii spôsobom, ktorý nevyvolá aktiváciu článku V. Washingtonskej zmluvy o kolektívnej obrane napadnutého štátu"*.[8]

V kontexte Slovenskej republiky sa tento pojem prvýkrát objavil v roku 2016, a to v *Bielej knihe o obrane Slovenskej republiky*[9] z dielne Ministerstva obrany SR. V bode 56. tohto strategického dokumentu je uvedené:

„Z hľadiska spôsobu vedenia konfliktov v meniacom sa bezpečnostnom prostredí je vážnou bezpečnostnou hrozbou najmä propaganda na strategickej úrovni ako súčasť informačného a psychologického pôsobenia na vybrané cieľové skupiny spoločnosti v rámci tzv. informačnej vojny a špecifické operačné postupy, ktoré sú najlepšie charakterizované pojmom ‚hybridný spôsob vedenia bojových činností'. Propaganda na strategickej úrovni je jedným z pilierov konceptu tzv. permanentnej vojny. Základné myšlienky definované týmto konceptom však môžu byť v budúcnosti na vedenie bojových činností v rôznych typoch konfliktov využité nielen bezpečnostnými zložkami štátov, ale ktorýmkoľvek bezpečnostným aktérom (t. j. aj neštátnym). Cieľom je pri minimálnom nasadení vlastných ozbrojených síl dosiahnuť morálne a psychologické zlomenie protivníkových ozbrojených zložiek a najmä časti civilného obyvateľstva (polarizácia cieľových skupín) tak, aby začali pôsobiť proti chráneným hodnotám na území subjektu, proti ktorému je ‚hybridný spôsob vedenia bojových činností' použitý."

Hoci sa pojem *hybrid warfare* začal vo verejných politikách krajín EÚ a NATO objavovať až pomerne nedávno, koncept samotný je oveľa starší. Už Sun-c', čínsky vojenský stratég a filozof, ktorý žil v 5. storočí p.n.l., tvrdil, že najvyšším stupňom vojenského umenia je víťazstvo založené na dômyselnosti a dosiahnuté bez boja. To je aj cieľom hybridných hrozieb takých, ako ich poznáme dnes. Zároveň tiež definoval šesť princípov vojny, ktoré sú nadčasové a z veľkej časti rovnako vystihujú to, čo dnes označujeme ako hybridné formy vedenia boja/hybridnú vojnu.

7 Parlamentné zhromaždenie NATO, Výbor pre obranu a bezpečnosť, General Report Hybrid Warfare: NATO's New Strategic Challenge?, 2015, https://www.nato-pa.int/document/2015-166-dsc-15-e-bis-hybrid-warfare-calha-report
8 Ibid.
9 Ministerstvo obrany Slovenskej republiky, Biela kniha o obrane Slovenskej republiky, 28. september 2016, http://www.mod.gov.sk/data/BKO2016_LQ.pdf

Princípy sú nasledovné:

- víťazstvo bez boja;
- vyhýbanie sa konfrontácii s hlavnou silou protivníka a využitie jeho slabín;
- oklamanie a spravodajská prevaha;
- ovplyvňovanie akcií protivníka na presadenie vlastných zámerov;
- rýchlosť a flexibilita;
- velenie príkladom.[10]

Čo sa týka relatívne nedávnej minulosti, bol to práve Sovietsky zväz, ktorý vyvinul koncepty *aktívnych opatrení* (operácie subverzného politického vplyvu od mediálnej manipulácie po zameriavanie politických oponentov), *maskirovky* (kamufláž vojenských aktivít za účelom popierania a maskovania; príkladom je krytie útočných zbraní transportovaných na Kubu pred Kubánskou krízou v roku 1962) a *reflexívnej kontroly* (zásobovanie oponenta vybranými informáciami, aby ho donútili vykonávať rozhodnutia, ktoré vyhovujú zámerom ich realizátora).[11] Všetky tieto koncepty dnes taktiež spadajú do toho, čo označujeme ako hybridné spôsoby vedenia vojny.

Prominentný expert na sovietsku *reflexívnu kontrolu* Timothy L. Thomas ako príklad uvádzal aj chválenie sa sovietskych lídrov falošnými raketami a podhadzovanie falošných dokumentov západným spravodajským službám, ktoré ich malo presvedčiť, že sovietska nukleárna sila bola hrozivejšia než v skutočnosti.[12] Ďalší príklad sa odohral v roku 1961, keď počas studenej vojny americký prezident John Kennedy vo svojom prejave pred novinármi opisoval akcie ZSSR voči Západu ako systém kombinujúci vojenské, diplomatické, spravodajské, ekonomické, vedecké a politické operácie používané na rozšírenie sféry vplyvu Sovietskeho zväzu.[13] Aj na týchto príkladoch je možné vidieť, že celý koncept, ktorý je starý viac než 2000 rokov, sa využíval sa ešte predtým, než dostal svoje súčasné pomenovanie.

HYBRIDNÉ HROZBY

Základným prvkom, ktorý odlišuje hybridné spôsoby vedenia vojny od hybridných hrozieb, je využitie vojenských síl a kapacít, ako aj hrozba silou alebo priame použitie ozbrojených síl skrytým či otvoreným spôsobom na dosiahnutie politických cieľov.

V rámci EÚ, a teda aj pre Slovensko, je najrelevantnejšia definícia konceptu hybridných hrozieb obsiahnutá v dokumente *Spoločný rámec EÚ pre boj proti hybridným hrozbám*,[14] ktorý uvádza:

„Definície hybridných hrozieb sú síce rôzne a musia zostať flexibilné, aby mohli reagovať na premenlivú povahu týchto hrozieb, ide však o to, aby sa podarilo vystihnúť ***súbor rôznych nátlakových a podvratných činností a konvenčných a nekonvenčných metód (napríklad diplomatických, vojenských, ekonomických a technologických), ktoré môžu rôzne štátne aj neštátne subjekty koordinovaným spôsobom využívať na to, aby dosiahli konkrétne ciele bez toho, aby formálne vyhlásili vojnu.*** *Snahou je obyčajne* ***zneužívať zraniteľnosť cieľa a vytvárať neprehľadné situácie s cieľom narušiť rozhodovacie procesy.*** *Nástrojom týchto hybridných hrozieb môžu byť* ***masívne dezinformačné kampane a využívanie sociálnych médií na propagandu*** *alebo radikalizáciu, nábor a priame ovládanie priaznivcov."*

Z tejto definície vyplýva, že hybridné hrozby sú súborom viacerých aktivít, ktorých cieľom je oslabiť protivníka. Môžu ich využívať štáty, ale aj neštátni aktéri ako napríklad teroristické skupiny.

10 Sun-c´, Umenie vojny, resp. Galatík, V., Krásný, A., Zetocha, K. (eds.), Vojenská strategie, 2008
11 Parlamentné zhromaždenie NATO, Výbor pre obranu a bezpečnosť, Countering Russia's Hybrid Threats: An update, Draft Special Report, 2018, https://www.nato-pa.int/download-file?filename=sites/default/files/2018-04/2018%20-%20COUNTERING%20RUSSIA%27S%20HYBRID%20THREATS%20-%20DRAFT%20SPRING%20REPORT%20JOPLING%20-%20061%20CDS%2018%20E.pdf
12 Ibid.
13 John F. Kennedy, Address before the American Newspaper Publishers Association, 1961,
14 Európska komisia, Spoločný rámec pre boj proti hybridným hrozbám, 2016, https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:52016JC0018&from=EN

Európske centrum na boj proti hybridným hrozbám (Hybrid CoE) definuje hybridné hrozby podobne:

„Hybridné hrozby sú metódy a aktivity namierené voči zraniteľným miestam oponenta. Zraniteľné miesta môžu byť vytvorené mnohými vecami, vrátane historickej pamäte, legislatívy, starých praktík, geostrategických faktorov, silnej polarizácie spoločnosti, technologickými nevýhodami či ideologickými rozdielmi. Ak záujmy a ciele toho, čo využíva hybridné metódy a aktivity, nie sú dosiahnuté, situácia môže vyústiť do hybridnej vojny, kde značne narastie úloha armády a násilia.“[15]

Hybrid CoE identifikuje hybridné hrozby podľa nasledovných charakteristických rysov:

1. Koordinovaná a synchronizovaná akcia, ktorá účelovo cieli na zraniteľné miesta demokratických štátov a inštitúcií, pričom využíva široké spektrum spôsobov (politické, ekonomické, vojenské, civilné a informačné).
2. Aktivity, ktoré sú na prahu medzi vojnou a mierom a zneužívajú ťažkosti pri ich detekovaní a prisúdení (konkrétnemu aktérovi).
3. Cieľom je ovplyvniť rôzne formy rozhodovacích procesov na lokálnej (regionálnej), štátnej alebo inštitucionálnej úrovni za účelom uprednostniť a/alebo dosiahnuť strategické ciele a zároveň podkopať a/alebo zraniť cieľ.[16]

Na Slovensku tiež môžeme nájsť viacero dokumentov, ktoré obsahujú a definujú pojem *hybridné hrozby*. Vychádzajú zväčša z terminológie prijatej na úrovni EÚ. Termín *hybridné hrozby* je obsiahnutý aj v *Terminologickom slovníku krízového riadenia Bezpečnostnej rady SR,*[17] ktorý uvádza nasledovnú definíciu:

„Súbor nátlakových a podvratných činností, konvenčných a nekonvenčných, vojenských a nevojenských metód, ktoré môžu štátne aj neštátne subjekty koordinovaným spôsobom využívať na dosiahnutie konkrétnych cieľov bez formálneho vyhlásenia vojny.“

Tento pojem sa premietol aj do textu *Bezpečnostnej stratégie SR* prijatej uznesením vlády SR č. 459/2017 zo dňa 4.10.2017, ktorá na str. 9 uvádza:

„Situácia na juhu a východe Ukrajiny je varovaním, že ozbrojený konflikt v Európe nemusí mať iba podobu priameho vojenského stretu medzi štátmi, ale aj hybridného spôsobu vedenia bojových činností. ***Hybridná hrozba predstavuje súbor nátlakových a podvratných činností, konvenčných a nekonvenčných, vojenských a nevojenských metód a nástrojov, využívaných koordinovane na dosiahnutie konkrétnych politických cieľov bez formálneho vyhlásenia vojny a pod prahom zvyčajnej reakcie. Zahŕňať môžu ovplyvňujúce, centrálne riadené spravodajské a informačné pôsobenie, pôsobenie neštátnych aktérov, vrátane polovojenských skupín, či nasadenie ozbrojených síl štátneho aktéra bez označenia.*** *Takéto hybridné aktivity sa môžu začať skôr než dôjde k otvorene deklarovaným vojenským operáciám. Polarizujú spoločnosť, vnášajú neistotu, a tým podkopávajú legitimitu, dôveryhodnosť, akcieschopnosť štátnych inštitúcií a demokratický ústavný poriadok a majú tak negatívny vplyv na realizáciu bezpečnostných záujmov štátov, ktoré sú im vystavené. Hybridné aktivity môžu byť zamerané aj na oslabovanie podpory verejnosti pre plnenie medzinárodných záväzkov, či ochromenie reakcie medzinárodného spoločenstva.“*[18]

15 Hybrid CoE, Countering Hybrid Threats, 2018, https://www.hybridcoe.fi/hybrid-threats/
16 Ibid.
17 Bezpečnostná rada SR, Terminologický slovník krízového riadenia, 2017, http://www.vlada.gov.sk/data/files/7200_terminologicky-slovnik-uprava.pdf
18 Vláda SR, Bezpečnostná stratégia Slovenskej republiky, 2017, https://rokovania.gov.sk/RVL/Material/22364/1

Toto znenie sa premietlo aj do *Koncepcie Slovenskej republiky na boj proti hybridným hrozbám,*[19] v ktorej stojí:

„Súčasne pôsobiace aktivity, ktoré ohrozujú základné atribúty štátu alebo ich funkčnosť, sa označujú ako hybridné hrozby. ***Hybridná hrozba je definovaná ako súbor nátlakových a podvratných činností, konvenčných a nekonvenčných, vojenských a nevojenských metód, ktoré môžu štátne aj neštátne subjekty koordinovaným spôsobom využívať na dosiahnutie konkrétnych cieľov bez formálneho vyhlásenia vojny a pod prahom zvyčajnej reakcie. Sú realizované aktivitami charakterizovanými centrálne riadeným spravodajským a informačným pôsobením, pôsobením neštátnych aktérov, vrátane polovojenských skupín, či nasadením ozbrojených síl štátneho aktéra bez označenia.*** *Takéto aktivity sa môžu začať skôr, než dôjde k otvorene deklarovaným vojenským operáciám. Polarizujú spoločnosť, vnášajú neistotu, a tým podkopávajú legitimitu, dôveryhodnosť, akcieschopnosť štátnych inštitúcií a demokratický ústavný poriadok a majú tak negatívny vplyv na realizáciu bezpečnostných záujmov štátov, ktoré sú im vystavené.“*

Z uvedeného je zrejmé, že v kontexte SR sa pracuje s konceptom hybridných hrozieb, ktorý v zásade vychádza z podobných definícií prijatých na pôde EÚ, a hlavné definičné znaky hybridných hrozieb sú totožné so znením prijatým v *Spoločnom rámci EÚ na boj proti hybridným hrozbám*. Zároveň v slovenskom prístupe k hybridným hrozbám dochádza k spájaniu vojenských a nevojenských ohrození, a teda aj konceptu *hybrid threats* a *hybrid warfare*, čo je v rozpore s prístupom napríklad Hybrid CoE, ktorý sa sústreďuje výlučne na nevojenské aspekty hybridných hrozieb.

VYUŽÍVANIE KONCEPTU HYBRIDNÝCH HROZIEB ŠTÁTNYMI A NEŠTÁTNYMI AKTÉRMI

V súvislosti s hybridnými hrozbami sa vzhľadom na vývoj na Ukrajine, ale i na snahy o zasahovanie do volebných procesov najčastejšie hovorí o Ruskej federácii. Odkaz na konflikt na Ukrajine, anexiu Krymu Ruskou federáciou a podporu pro-ruských separatistov sa objavuje v množstve dokumentov prijatých tak na pôde EÚ,[20] ako aj na pôde NATO.[21] Z tohto dôvodu obsahuje východisková štúdia aj časť venovanú historickému pohľadu na využívanie konceptu hybridných hrozieb Sovietskym zväzom a jeho nástupníckym štátom Ruskou federáciou, aj keď pod inými označeniami. Neznamená to však, že využitie hybridných hrozieb štátnymi aktérmi je výlučne doménou Ruskej federácie. Rovnaké alebo podobné postupy využívajú viaceré krajiny. Ruská federácia je však v ich používaní najďalej a vzhľadom na polohu SR, ako i špecifickú zraniteľnosť slovenskej spoločnosti[22] a členstvo SR v EÚ a NATO, predstavuje využívanie hybridných hrozieb zo strany Ruskej federácie najväčšie potenciálne riziko pre SR.

Ruská federácia

Spôsoby oslabovania protivníka popísané vyššie, ako napríklad aktívne opatrenia alebo reflexívna kontrola, ktoré mali v Sovietskom zväze dlhú tradíciu, ale vymizli s koncom studenej vojny, boli znovuoživené začiatkom druhého tisícročia. Stalo sa tak najmä vzhľadom na zmenu zahraničnej politiky Ruskej federácie - deklarovanie tzv. zóny vplyvu v krajinách bývalého Sovietskeho zväzu alebo obnovené identifikovanie Západu ako hlavného protivníka Ruska. Takéto vnímanie sa premietlo napríklad do prejavu prezidenta Ruskej federácie Vladimíra Putina na Mníchovskej bezpečnostnej konferencii v roku 2007, kde okrem iného uviedol: *„Rusko je neustále poučované o demokracii. Ale z nejakého dôvodu sa tí, čo poučujú, nechcú sami poučiť.“* Tvrdej kritike tiež podrobil USA, ktoré podľa neho každý deň prekračujú hranice svojej krajiny a snažia sa svetu nanútiť svoju vôľu. Putin tiež kritizoval NATO a jeho rozširovanie. To má predstavovať provokáciu, ktorá znižuje úroveň vzájomnej dôvery.[23]

19 Koncepcia Slovenskej republiky pre boj proti hybridným hrozbám, schválená vládou SR dňa 11. júla 2018 uznesením č. 345/2018, http://www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=27668
20 Európska komisia, Spoločný rámec pre boj proti hybridným hrozbám, 2016, https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:52016JC0018&from=EN
21 Parlamentné zhromaždenie NATO, Výbor pre obranu a bezpečnosť, Countering Russia's Hybrid Threats: An update, Draft Special Report, 2018,https://www.nato-pa.int/download-file?filename=sites/default/files/2018-04/2018%20-%20COUNTERING%20RUSSIA%27S%20HYBRID%20THREATS%20-%20DRAFT%20SPRING%20REPORT%20JOPLING%20-%20061%20CDS%2018%20E.pdf
22 Zraniteľnosť SR voči pôsobeniu Ruskej federácie je popísaná napr. v analýze Vulnerability Index, GLOBSEC, 2017 https://www.globsec.org/publications/vulnerability-index-subversive-russian-influence-central-europe/
23 JRL Russia List, Transcript: 2007 Putin Speech and the Following Discussion at the Munich Conference on Security Policy, Russia List, 2014, http://russialist.org/transcript-putin-speech-and-the-following-discussion-at-the-munich-conference-on-security-policy/

Vo formálnej rovine sa takáto zmenená pozícia Ruska prejavila v aktuálnom znení Vojenskej doktríny Ruskej federácie prijatej v roku 2014, ktorá identifikuje NATO ako primárnu hrozbu.[24] Využívanie hybridných spôsobov vedenia boja bolo obnovené ako asymetrická odpoveď na jasný rozdiel v ruských konvenčných vojenských a technologických možnostiach a „mäkkej sile“ v porovnaní so Západom. O rozšírenie akceptácie tohto konceptu sa zaslúžil aj pokrok v informačnej a komunikačnej technológii, ktorý umožnil vznik nových spôsobov ovplyvňovania postojov občanov pomocou informačných technológií v doteraz nevídanom rozsahu.[25]

Konflikt na Ukrajine v roku 2014, vrátane obsadenia Krymu neoznačenými ruskými vojakmi, znamenal nasadenie konceptu hybridného spôsobu vedenia vojny v omnoho väčšom rozsahu než kedykoľvek predtým. Bola to práve kombinácia nasadenia neoznačených vojakov, mobilizácie domácich polovojenských skupín podporovaných spravodajskými službami a kybernetických a informačných operácií, ktoré sa stali typickými pre využitie tohto konceptu na Ukrajine. Následná eskalácia a nasadenie regulárnych síl ruskej armády[26] prišli až v ďalšej fáze konfliktu ako reakcia na narastajúci tlak zo strany ukrajinskej armády na tzv. ľudové republiky na východe Ukrajiny.

Asi najznámejším popisom toho, čo dnes označujeme ako hybridné spôsoby vedenia vojny, sa stal - hoci neprávom - prejav náčelníka generálneho štábu ozbrojených síl Ruskej federácie Valerija Gerasimova na Akadémii vojenských vied, publikovaný v odbornom časopise Promyšlenno-Vojennyj Kurier v roku 2013.[27] Vo svojom prejave popisuje tzv. nelineárnu vojnu a zdôrazňuje význam nevojenských prostriedkov pri dosahovaní geopolitických a strategických cieľov. V predmetnom článku, ktorý je prepisom jeho prejavu na výročnom zasadnutí Akadémie vojenských vied, Gerasimov popisuje to, čo vníma ako zasahovanie Západu v iných krajinách, analyzuje Arabskú jar, zvrhnutie Muammara Kaddafího v Líbyi a iné krízové udalosti a, okrem iného, konštatuje:

„Samotné ‚pravidlá vojny' sa zmenili. Úloha nevojenských prostriedkov na dosiahnutie politických a strategických cieľov narástla a v mnohých prípadoch prekročila silu zbraní v ich účinnosti.“[28]

Tento prejav získal značnú pozornosť najmä po udalostiach na Ukrajine v roku 2014, ktoré vykazovali znaky a postupy opísané v predmetnom článku - súbežné a koordinované nasadenie širokej palety nevojenských nástrojov: informačnej kampane, kybernetických útokov, využívanie polovojenských skupín, energetický nátlak (v súčinnosti a koordinácii s vojenskými nástrojmi a prostriedkami) a ich kombinácia na dosahovanie strategických a geopolitických cieľov. Aj z tohto dôvodu bol označovaný predmetný článok niektorými bezpečnostnými analytikmi ako tzv. Gerasimova doktrína[29]. Takéto vnímanie je trochu zjednodušujúce a nepresné, nakoľko v predmetnom článku sa nevyskytuje priamo popis aktuálnej ruskej vojenskej doktríny, ale naopak, popis toho, čo Rusko vníma ako využívanie nevojenských metód na dosiahnutie geopolitických cieľov zo strany Západných mocností (reprezentovaných najmä USA).

24 Vojenská doktrína Ruskej federácie, 2014, http://www.mid.ru/documents/10180/822714/41d527556bec8deb3530.pdf/d899528d-4f07-4145-b565-1f9ac290906c

25 Parlamentné zhromaždenie NATO, Výbor pre obranu a bezpečnosť, Countering Russia's Hybrid Threats: An update, Draft Special Report, 2018, https://www.nato-pa.int/download-file?filename=sites/default/files/2018-04/2018%20-%20COUNTERING%20RUSSIA%27S%20HYBRID%20THREATS%20-%20DRAFT%20SPRING%20REPORT%20JOPLING%20-%20061%20CDS%2018%20E.pdf

26 Prítomnosť vojsk Ruskej federácie na východnej Ukrajine bola potvrdená vo viacerých oficiálnych dokumentoch prijatých na pôde EÚ, napr: Rozhodnutie Rady 2015/241 z 9. februára 2015, ktorým sa mení rozhodnutie 2014/145/SZBP o reštriktívnych opatreniach vzhľadom na konanie, ktorým sa narúša alebo ohrozuje územná celistvosť, zvrchovanosť a nezávislosť Ukrajiny, https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:32015D0241&from=EN
Presný popis jednotiek ozbrojených síl Ruskej federácie, ktoré sa zapájali do bojov na východnej Ukrajine, je napríklad v analýze Igora Sutyagina z britského think-tanku RUSI (Royal United Services Institute) z roku 2015, Russian Forces in Ukraine, https://rusi.org/sites/default/files/201503_bp_russian_forces_in_ukraine.pdf

27 Ценность науки в предвидении. Новые вызовы требуют переосмыслить формы и способы ведения боевых действий Promyšlenno-Vojennyj Kurier, 23.2.2013, https://www.vpk-news.ru/articles/14632, anglický preklad článku Valerija Gerasimova “Hodnota vedy je v predvídaní - Nové požiadavky si vyžadujú prehodnotenie foriem a spôsobov vykonávania bojových operácií“, https://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art008.pdf

28 Ibid.

29 Za pôvodcu tohto pojmu sa považuje popredný bezpečnostný analytik zaoberajúci sa Ruskom, pôsobiaci v Institute of International Relations, Mark Galeotti, ktorý ako prvý použil názov Gerasimova doktrína vo svojom blogu z roku 2014, ”Gerasimova doktrína a ruská nelinárna vojna”, https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/. V marci 2018 uverejnil vo Foreign Policy článok, v ktorom žiada o nepoužívanie termínu “Gerasimova doktrína”, pretože je podľa neho nepresný a zavádzajúci. Zároveň v ňom však konštatuje, že “je nepochybné, že Západ čelí rozsiahlej, mnohostrannej, rozvracajúcej a rozdeľujúcej kampani využívajúcej skryté politické, aktívne opatrenia zo strany Ruska, https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/

Existujú však iné texty ruských vojenských stratégov, ktoré sú v popise nástrojov a techník využívaných Ruskou federáciou oveľa otvorenejšie. Napríklad ruský plukovník Sergei Chekinov a ruský generálporučík Sergei Bogdanov poukazujú na to, že informácie môžu byť využité na dezorganizáciu, vyvolanie chaosu s cieľom oklamať súpera, ovplyvniť verejnú mienku a postupne oslabiť vôľu súpera odolávať vonkajšiemu tlaku.[30] To všetko môže spôsobiť destabilizáciu a chaos a potenciálne dláždiť cestu pre jednoduchý vojenský útok. Ako príklad uvádzajú Chekinov a Bogdanov situáciu na Ukrajine vo vzťahu ku Krymskému polostrovu. Tiež tvrdia, že vo vojnách budúcnosti bude informačná prevaha zohrávať kľúčovú úlohu. Preto je podľa nich nutné sa v budúcnosti viac špecializovať na oblasť informačných technológií s cieľom získať v nich nadradenosť. Podľa Chekinova a Bogdanova je tiež dôležité získať kontrolu nad informačným tlakom, ktorý môže byť následne využívaný proti súperovi prostredníctvom médií, mimovládnych organizácií, propagandy a dezinformácií s cieľom vyvolať chaos v spoločnosti. Rusko si je vedomé týchto nových spôsobov vedenia vojny, preto bude uplatňovať spôsoby, ktoré mu pomôžu sa proti týmto hrozbám ubrániť.

To, že v otvorených zdrojoch z prostredia Ruskej federácie nenájdeme priamy popis koordinovaného plánovaného nasadenia jednotlivých komponentov hybridných hrozieb ako súčasť ich vojenskej doktríny neznamená, že sa v praxi neuplatňujú. Bolo by veľmi naivné myslieť si, že skutočná doktrína popisujúca taktické postupy a ich kombináciu v operačnom nasadení by bola voľne prístupná v otvorených zdrojoch. Najlepším dôkazom o využívaní jednotlivých druhov útokov spadajúcich do kategórie hybridných hrozieb sú napríklad správy špeciálneho prokurátora FBI, ktoré detailne popisujú spôsoby a prostriedky nasadené zo strany Ruska v amerických prezidentských voľbách.[31] Príkladom hybridných hrozieb je aj nedávny prípad pokusu o otrávenie Sergeja Skripaľa v Salisbury (Veľká Británia), z ktorého boli usvedčení dvaja príslušníci GRU[32], alebo nedávny pokus z apríla 2018 o nabúranie počítačových systémov Medzinárodnej organizácie pre zákaz chemických zbraní v Haagu v Holandsku, pri ktorom boli prichytení opäť príslušníci GRU.[33]

Iní štátni a neštátni aktéri

Rusko nie je jediný štát, ktorý používa hybridné hrozby. Patria sem napríklad aj Irán, Severná Kórea či Čína. Pre Irán je typické využívanie kombinácie vojenských aj paramilitárnych nástrojov či kybernetických a informačných operácií za účelom ovplyvniť aktérov vo svojom regióne.[34] Severná Kórea je zase známa masívnou propagandou dovnútra aj navonok štátu, vytváraním dezinformácií, kybernetickými útokmi či ďalšími manipulačnými technikami, ktorými sa snaží ovplyvniť napríklad aj obyvateľov Južnej Kórey. Čína využíva hybridné hrozby okrem iného aj voči Taiwanu,[35] pričom používa propagandu či dezinformácie na formovanie verejnej mienky. Viacerí akademici si tiež myslia, že je možné, že Čína sa v budúcnosti inšpiruje ruským modelom a pokúsi sa získať celosvetovo väčší vplyv.

30 S. G. Chekinov and S. A. Bogdanov, "On the Character and Content of Wars of a New Generation," Voennaya Mysl 10 (Military Thought 10), 2013, 13–24.
31 Špeciálny prokurátor Robert Mueller vzniesol v júli 2018 obvinenie voči 12 ruským dôstojníkom spravodajskej služby. Sú obvinení z hacknutia počítačových sietí členov volebného tímu Hillary Clinton, Demokratického národného výboru a Výboru pre demokratickú kongresovú kampaň. Obžaloba uvádza časový sled udalostí, ktoré sa stali v roku 2016 a mohli ovplyvniť priebeh amerických prezidentských volieb. V obžalobe stojí, že okolo roku 2016 riadila Ruská federácia vojenskú spravodajskú agentúru Hlavné riaditeľstvo Generálneho štábu ozbrojených síl Ruskej federácie (skratka GRU). GRU malo viacero jednotiek, vrátane Jednotiek 26165 a 74455, ktoré boli zapojené do kybernetických operácií, ktoré postupne zverejňovali dokumenty ukradnuté počítačovými útokmi. Tieto jednotky viedli obrovské kybernetické operácie s cieľom zasahovať do prezidentských volieb. Obžaloba tiež uvádza presný popis práce obvinených vrátane ich postavenia v rámci GRU či falošných identít, ktoré používali na internete. Približne 21 strán obžaloby obsahuje konkrétne činy, ktorých sa obžalovaní dopustili, https://www.justice.gov/file/1080281/download
32 Prejav Amb. Karen Pierce, stálej zástupkyne Veľkej Británie pri OSN, 2018, https://www.gov.uk/government/speeches/you-dont-recruit-an-arsonist-to-put-out-a-fire-you-especially-dont-do-that-when-the-fire-is-one-they-caused
33 Prejav veľvyslanca Veľkej Británie v Holandsku, 2018, https://www.gov.uk/government/speeches/minister-for-europe-statement-attempted-hacking-of-the-opcw-by-russian-military-intelligence
34 Dalton, M. G., How Iran's hybrid-war tactics help and hurt it, Bulletin of Atomic Scientists, 2017, https://thebulletin.org/2017/09/how-irans-hybrid-war-tactics-help-and-hurt-it/
35 Lin, Y. Y., China's Hybrid Warfare and Taiwan, The Diplomat, 2018, https://thediplomat.com/2018/01/chinas-hybrid-warfare-and-taiwan/

Okrem štátov používajú hybridné hrozby aj neštátni aktéri ako Hizballáh,[36] libanonská politická a vojenská organizácia považovaná za teroristov, Hamas, palestínska teroristická polovojenská organizácia, ale aj Islamský štát (ISIS). Práve jednomesačná vojna medzi Hizballáhom a Izraelom v roku 2006 bola ako jedna z prvých opisovaná ako hybridná.[37] Niektorí odborníci dokonca tvrdia, že aj vojna na Balkáne v deväťdesiatych rokoch niesla znaky hybridnej vojny kvôli kombinácii politického boja, propagandy, diplomacie a vojenskej sily[38]. Použitie prostriedkov hybridných spôsobov vedenia boja, najmä nepravidelných vojenských jednotiek a masívnej propagandy, tiež dopomohli ISIS k rýchlemu ovládnutiu území v Iraku v roku 2014.

36 Hoffman, F. G., Lessons from Lebanon: Hezbollah and Hybrid Wars, FPRI, 2006, https://www.fpri.org/article/2006/08/lessons-from-lebanon-hezbollah-and-hybrid-wars/

37 Hashim, A. S., State and Non-State Hybrid Warfare, Oxford Research Group, 2017, https://www.oxfordresearchgroup.org.uk/Blog/state-and-non-state-hybrid-warfare

38 Back to Basics on Hybrid Warfare in Europe: A Lesson from the Balkans, Christopher J. Lamb a Susan Stipanovich, National Defence University, Joint Force Quarterly č. 81, 2016, http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-81/jfq-81_92-101_Lamb-Stipanovich.pdf

2. LEGISLATÍVNY RÁMEC A VEREJNÉ POLITIKY TÝKAJÚCE SA HYBRIDNÝCH HROZIEB

Najvýznamnejšou a najkomplexnejšou verejnou politikou na úrovni EÚ v oblasti hybridných hrozieb je *Spoločný rámec na boj proti hybridným hrozbám* zo 6. apríla 2016.39 Spoločný rámec bol prijatý Európskou komisiou a vysokou predstaviteľkou Únie pre zahraničné veci a bezpečnostnú politiku s cieľom aktivovať koordinovanú reakciu na úrovni EÚ a stavať na európskej solidarite, vzájomnej pomoci a Lisabonskej zmluve.

Tento rámcový dokument navrhuje 22 operačných akcií zameraných na:

- zvyšovanie informovanosti (zriadenie špeciálnych nástrojov na výmenu informácií medzi členskými štátmi; koordináciu krokov EÚ v oblasti strategickej komunikácie);
- budovanie odolnosti (v kritických odvetviach – kybernetická bezpečnosť, kritické infraštruktúry/ energetika, doprava, vesmír, ochrana finančného systému, ochrana verejného zdravia, podpora boja proti násilnému extrémizmu a radikalizácii);
- prevenciu, reakciu na krízy a obnovu (vymedzenie účinných postupov v rámci doložky o solidarite /článok 222 ZFEÚ/ a doložky o vzájomnej obrane /článok 42 ods. 7 ZEÚ/ v prípade, že dôjde k rozsiahlemu a závažnému hybridnému útoku);
- zintenzívnenie spolupráce medzi EÚ a NATO, s ostatnými partnerskými organizáciami (rešpektujúc zásady autonómie rozhodovacieho procesu každej z týchto organizácií) a s tretími krajinami.

Zároveň však tento dokument zdôrazňuje, že boj proti hybridným hrozbám je vo veľkej miere vnútroštátnou záležitosťou, keďže primárnu zodpovednosť zaň nesú členské štáty. Cieľom *Spoločného rámca* je preto pomôcť členských štátom v boji proti hybridným hrozbám a zlepšiť ich odolnosť v situáciách, keď takýmto hrozbám čelia, a to účinnejším skĺbením európskych a vnútroštátnych nástrojov, než tomu bolo doposiaľ.

Najnovším dokumentom prijatým na pôde EÚ v tejto oblasti je *Spoločné oznámenie Európskemu parlamentu, Európskej rade a Rade: Zvyšovanie odolnosti a posilňovanie spôsobilosti riešiť hybridné hrozby*[40] z júna 2018. Vo svojom texte Európska komisia uvádza, že hybridné činnosti aj naďalej predstavujú závažnú a akútnu hrozbu pre EÚ a jej členské štáty, pričom úsilie zamerané na destabilizáciu krajín sa stáva stále bežnejším javom.

Toto spoločné oznámenie, ktoré okrem toho, že konštatuje pretrvávajúce nebezpečenstvo hybridných hrozieb, vytyčuje konkrétne opatrenia v nasledovných oblastiach:

- Situačné povedomie – lepšia schopnosť odhaľovať hybridné hrozby;
- Posilnené opatrenia proti chemickým, biologickým, rádiologickým a jadrovým hrozbám;
- Strategická komunikácia – šírenie zrozumiteľných informácií;
- Budovanie odolnosti a odstrašujúceho účinku v sektore kybernetickej bezpečnosti;
- Budovanie odolnosti voči nepriateľskej spravodajskej činnosti.

39 Európska komisia, Spoločný rámec pre boj proti hybridným hrozbám, 2016, https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:52016JC0018&from=sk https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:52016JC0018&from=sk
40 Európska komisia, Zvyšovanie odolnosti a posilňovanie spôsobilosti riešiť hybridné hrozby, 2018, https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:52018JC0016&from=en

BEZPEČNOSTNÁ STRATÉGIA SR

Prvým slovenským dokumentom verejných politík, kde sa objavila zmienka o hybridných hrozbách, bola *Biela kniha o obrane SR* z roku 2016[41]. Tá spomína hybridné hrozby najmä vo vojenskom kontexte - hybridný spôsob vedenia vojny. Komplexnejšie sa im venuje *Bezpečnostná stratégia SR* z roku 2017,[42] ktorá okrem definovania pojmu hybridné hrozby obsahuje aj viacero bodov určujúcich úlohy a ciele SR v danej oblasti. Konkrétne v bode č. 79 sa SR zaviazala prijať koncepciu týkajúcu sa oblasti hybridných hrozieb, zvyšovať svoju odolnosť voči hybridným hrozbám a spolupracovať s MVO:

*„Slovenská republika prijme a bude implementovať **koncepciu zvyšovania odolnosti voči hybridným hrozbám**. Bude vytvárať adekvátne k**apacity pre strategickú komunikáciu doma a v zahraničí**, najmä v informačnom prostredí EÚ a NATO. S cieľom zvyšovania odolnosti štátu a jeho ochrany voči hybridným hrozbám **prehĺbi partnerstvo s relevantnými mimovládnymi organizáciami.**“*

V bode 59 SR deklarovala svoj záujem rozvíjať spoluprácu medzi EÚ a NATO aj v oblasti hybridných hrozieb:

*„Slovenská republika bude presadzovať všestranný **rozvoj strategickej spolupráce medzi EÚ a NATO**, zahŕňajúcu aj oblasť spoločného situačného prehľadu a koordinovaného systému včasného varovania. **Bude podporovať koordinovaný prístup EÚ a NATO k riešeniu otázok spoločného záujmu**, vrátane kybernetickej bezpečnosti a kybernetickej obrany, čelenia **hybridným hrozbám**, civilného krízového manažmentu či spoločných cvičení.“*

Z hľadiska komplexnosti a relevantnosti je najvýznamnejším dokumentom Koncepcia Slovenskej republiky na boj proti hybridným hrozbám, ktorá bola schválená vládou SR dňa 11. júla 2018 uznesením č. 345/2018.43 Koncepcia má tri základné časti. V prvej časti popisuje zmenu bezpečnostného prostredia a dôvody, prečo je nasadenie hybridných hrozieb čoraz častejšie. V druhej časti popisuje koncepcia situáciu v podmienkach SR a upozorňuje na viaceré zraniteľnosti SR. V tretej časti Koncepcia popisuje inštitucionálny rámec, a zároveň uvádza indikátory hybridných hrozieb a spôsob ich vyhodnotenia v praxi. Táto časť má pre praktickú použiteľnosť Koncepcie veľký význam, nakoľko obsahuje výpočet indikátorov hybridných hrozieb a vymenúva jednotlivé druhy ohrození ako aj okolnosti, za ktorých ich súčasné a koordinované použitie spĺňa náležitosti hybridných hrozieb:

- *„externý alebo interný politický nátlak na najvyšších štátnych predstaviteľov a štátne inštitúcie;*
- *ekonomický alebo energetický nátlak ako rozšírenie politického nátlaku;*
- *rozsiahle sabotáže proti kľúčovej infraštruktúre;*
- *kybernetické útoky s potenciálom spôsobiť škody veľkého rozsahu;*
- *informačné a propagandistické operácie s cieľom podkopať dôveru v štátne inštitúcie, vyvolať spoločenské nepokoje a vážne destabilizovať politickú a bezpečnostnú situáciu;*
- *ovplyvňovanie etnických, náboženských a kultúrnych menšín a ich manipulácia na politické účely;*
- *hrozba použitia vojenskej sily.*

Uvedené indikátory sami o sebe sú známymi a dlhodobými hrozbami, ale ich individuálny výskyt nemožno ešte považovať za hybridnú hrozbu. Podstatnou črtou hybridného spôsobu boja je súčinnosť a prepojenie rôznych prvkov hybridnej hrozby a ich paralelné nasadenie tak, aby vytvorili kvalitatívne vyššiu a zložitejšiu viacdimenzionálnu hrozbu.

41 Ministerstvo obrany Slovenskej republiky, Biela kniha o obrane Slovenskej republiky, 28. september 2016, http://www.mod.gov.sk/data/BKO2016_LQ.pdf
42 Vláda SR, Bezpečnostná stratégia Slovenskej republiky, 2017, https://rokovania.gov.sk/RVL/Material/22364/1
43 Koncepcia pre boj SR proti hybridným hrozbám, 2018, http://www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=27668

Hybridnou hrozbou sa rozumie až kombinované použitie niekoľkých, najmenej troch vyššie uvedených indikátorov v širšej kampani so zjavnou snahou aktéra útoku zasahovať do situácie v SR, pričom samotný aktér nie je známy alebo popiera svoju účasť na organizovaní a realizácii útoku/kampane.“

Rovnako dôležitou súčasťou Koncepcie je vymedzenie kompetencií a pôsobnosti jednotlivých orgánov a inštitúcií pri monitorovaní a reakcii na hybridné hrozby. Primárnu úlohu v zmysle Koncepcie majú Situačné centrum zriadené na Úrade vlády SR, ktoré plní úlohu národného kontaktného miesta pre hybridné hrozby, a Národné bezpečnostné analytické centrum (NBAC) zriadené na Slovenskej informačnej službe, ktoré plní úlohu národného kooperačného centra pre hybridné hrozby.

*„Úlohy **národného kontaktného miesta pre hybridné hrozby**, ktoré plní Situačné centrum Slovenskej republiky (ďalej len „SITCEN“), sú najmä:*

a) *prijímať a ďalej distribuovať na národnej úrovni produkty Hybrid fusion cell (ďalej len „HFC“);*

b) *informovať a zdieľať informácie súvisiace s hybridnými hrozbami s HFC;*

c) *byť poradcom HFC pre hybridné hrozby, ktoré sa najviac dotýkajú Slovenskej republiky;*

d) *asistovať HFC zabezpečovaním vypracúvania analýz bezpečnostnej situácie relevantnými orgánmi SR pri hodnotení a predpovediach vývoja;*

e) *aktualizovať svoje kontaktné údaje pre hladký tok informácií;*

f) *byť pripravený ku kontaktovaniu zo strany HFC v prípade krízovej situácie;*

g) *zúčastňovať sa stretnutí národných kontaktných bodov (ďalej len „POCs“) v Bruseli;*

h) *zabezpečovať kontaktovanie relevantných osôb v členskej krajine.“*

*„Úlohy **národného kooperačného centra pre hybridné hrozby**, ktoré plní Národné bezpečnostné analytické centrum (ďalej len „NBAC“), sú najmä:*

a) *prijať informáciu ktorejkoľvek zložky štátneho orgánu alebo odôvodnený podnet fyzickej osoby alebo právnickej osoby s podozrením na hybridnú hrozbu a zaradiť ju do procesu vyhodnocovania vytvorením dokumentu NBAC;*

b) *po vyjadrení štátnych orgánov zastúpených v NBAC v spolupráci so SITCEN doplniť do príslušného dokumentu NBAC súvislosti z pohľadu bezpečnostných záujmov EÚ a NATO a rozhodnúť o potrebe spracovania výstupu pre príjemcov;*

c) *v spolupráci so SITCEN doplniť súvislosti z pohľadu bezpečnostných záujmov EÚ a NATO a rozhodnúť o potrebe spracovania výstupu pre príjemcov.“*[44]

44 Ibid.

3. TEMATICKÁ ANALÝZA

3.1 STRATEGICKÁ KOMUNIKÁCIA

Katarína Klingová

ÚVOD

Vojenský konflikt v 21. storočí sa neobmedzuje len na využívanie vojenskej techniky, ako sú tanky, lietadlá a rakety, ale čoraz väčšiu úlohu zohráva informačné pôsobenie, preniknutie do počítačových sietí, psychologické operácie, mediálne manipulácie a ovládnutie rozhodovacích procesov. Dosiahnuť zmenu postojov u populácie, zmeniť geopolitickú orientáciu alebo minimálne ochromiť vôľu konať na obranu vlastného územia a záujmov prostredníctvom šírenia dezinformácií a propagandy je lacnejšie a oveľa efektívnejšie ako vojenské napadnutie štátu. Preto niektorí aktéri, ako napríklad jednotlivci, samozvané „alternatívne" médiá, štátni predstavitelia či štátne inštitúcie rôznych krajín, systematicky a účelovo klamú, šíria svoje „alternatívne" pravdy a manipulujú s faktami. Organizované a cieľavedomé šírenie dezinformácií je jedným z hlavných nástrojov využívaných v rámci hybridných operácií. Obranou a prevenciou pred pôsobením podvratných informačných operácií je strategická komunikácia.

Strategická komunikácia je v širokom ponímaní komunikácia s jasným plánom a agendou. Termín strategická komunikácia predstavuje *„konzistentné a vytrvalé hovorenie správnej veci, správnym ľuďom, v správnom čase, mobilizovanie sociálnej sily/moci, a (teda možnosť ako) šíriť svoj informačný naratív spôsobom, aby ste dosiahli tak krátkodobé ciele, ako i dlhodobé víťazstvá"*.[45] Správa Chatham House z roku 2011 definuje pojem strategická komunikácia ako *„sériu systematických, nepretržitých a koherentných aktivít vykonávaných na strategickej, operačnej a taktickej úrovni, ktoré umožňujú pochopenie cieľových skupín a identifikujú účinné komunikačné nástroje na podporu a udržanie konkrétneho typu správania."*[46]

PREHĽAD VEREJNÝCH POLITÍK

Slovenská republika sa v posledných rokoch stala predmetom intenzívneho pôsobenia širokej škály nástrojov zo strany Ruskej federácie smerujúcich k zmene nálad a postojov obyvateľstva, politických predstaviteľov, propagandy na strategickej úrovni a aktivity spravodajských služieb (napríklad vojenská rozviedka Generálneho štábu ozbrojených síl RF – GU)[47] či bývalých členov elitných ruských jednotiek SPETZNAZ. Toto sa potvrdzuje, okrem iného, aj vo výročných správach Slovenskej informačnej služby za rok 2015 či 2017 a Vojenského spravodajstva za rok 2017, ktoré zhodne zaznamenali zvýšenú aktivitu Ruskej federácie a s ňou spojených subjektov na území SR smerujúcich k ovplyvňovaniu postojov a nálad obyvateľstva. Na absenciu a potrebu stratégie na komunikáciu o obrane štátu upozorňovala tiež *Biela kniha o obrane Slovenskej republiky*[48] z roku 2016, ktorá definovala *„propagandu na strategickej úrovni"* ako vážnu bezpečnostnú hrozbu. Nová Bezpečnostná stratégia SR z roku 2017 taktiež deklaruje, že *„propagandistické a dezinformačné pôsobenie vonkajších a vnútorných aktérov"* prehlbuje pokles dôvery verejnosti voči EÚ a NATO.[49] Existenciu propagandistickej kampane šíriacej dezinformácie na Slovensku deklaruje aj *Koncepcia pre boj Slovenskej republiky proti hybridným hrozbám* schválená vládou SR v júli 2018.[50]

45 Wlachovský, M., Vyhodnocovanie informačného prostredia a strategická komunikácia ako nástroj v boji proti hybridným hrozbám, MepoForum.sk, 2018, http://mepoforum.sk/staty-regiony/europa/staty-eu-plus/vysehradska-4/slovensko/vyhodnocovanie-informacneho-prostredia-a-strategicka-komunikacia-ako-nastroj-v-boji-proti-hybridnym-hrozbam-miroslav-wlachovsky/

46 Cornish, P., Lindley-French, J., Yorke, C., Strategic Communications and National Strategy, Chatham House Report, 2011, https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r0911stratcomms.pdf

47 V minulosti sa označovala skratkou GRU - Glavnoje Razvedyvatel'noje Upravlenije - Hlavné riaditeľstvo rozviedky, v súčasnosti sa nazýva GU – Generalnoje Upravlenie.

48 Ministerstvo obrany Slovenskej republiky, Biela kniha o obrane Slovenskej republiky, 28. september 2016, http://www.mod.gov.sk/data/BK02016_LQ.pdf

49 Vláda SR, Bezpečnostná stratégia Slovenskej republiky, 2017, https://rokovania.gov.sk/RVL/Material/22364/1

50 Koncepcia pre boj Slovenskej republiky proti hybridným hrozbám schválená 11.7.2018 vládou SR uzn. č 345/2018, http://www.rokovania.sk/File.aspx/ViewDocumentHtml/Mater-Dokum-219866?prefixFile=m_

Pojem *strategická komunikácia* sa od roku 2017 začína vyskytovať v strategických a bezpečnostných dokumentoch Slovenskej republiky. Tie v minulosti zvyčajne poukazovali na zraniteľnosť informačných a komunikačných systémov z pohľadu kybernetickej bezpečnosti a zraniteľnosti informačných tokov, ktoré identifikovali ako rastúcu hrozbu. Toto možno pozorovať aj v *Bezpečnostnej stratégii Slovenskej republiky* z roku 2005, ktorá je stále platným dokumentom schváleným Národnou radou Slovenskej republiky.

Napriek tomu v roku 2017 možno pozorovať zmenu v ponímaní problematiky a nutnosti aktívnej činnosti aj v tejto oblasti. Strategická komunikácia sa v minulom roku dostala do viacerých strategických dokumentov. Nová *Bezpečnostná stratégia SR* z roku 2017, ktorá bola prijatá Vládou SR, ale do dátumu zverejnenia tejto štúdie nebola schválená NR SR, deklaruje, že *„Slovenská republika bude v rámci posilňovania dôvery a podpory občanov a v záujme presadzovania svojich bezpečnostných záujmov klásť väčší dôraz na strategickú komunikáciu s verejnosťou naprieč všetkými vládnymi inštitúciami.“* Podobne na potrebu budovania kapacít v tejto oblasti poukazuje aj Správa o činnosti Vojenského spravodajstva za rok 2017, ktorá deklaruje, že *„bezpečnostnou výzvou vo vzťahu k problematike realizácie významných projektov rozvoja obrany, udržiavania existujúcich spôsobilostí a prípravy, výcviku a doplňovania personálu zostáva nedostatok strategickej komunikácie rezortu vo vzťahu k spoločnosti a širokému spektru ďalších cieľových skupín.“*[51] Návrh novej *Obrannej stratégie SR*, ktorá je momentálne v procese prípravy, dokonca uvádza, že Slovensko bude aktívnym členom štruktúr v Centre excelentnosti NATO v oblasti strategickej komunikácie.[52]

Nie je však jasné, ako jednotlivé orgány štátnej správy narábajú s pojmom *strategická komunikácia* a čo pod týmto termínom rozumejú. Pojem *strategická komunikácia* sa nenachádza ani v aktuálnej verzii *Terminologického slovníka krízového riadenia a zásad jeho používania* Bezpečnostnej rady Slovenskej republiky z novembra 2017.[53] Mať presnú definíciu tohto pojmu ale nie je nevyhnutné. Oveľa dôležitejšie je budovanie inštitucionálnych kapacít v oblasti strategickej komunikácie a jej aktívna implementácia.

Momentálne jediný ústredný orgán štátnej správy, ktorý má vytvorené špecifické štruktúry a aktívne pracuje s konceptom strategickej komunikácie ako v teoretickej, tak aj v praktickej rovine na dennej báze, je Ministerstvo zahraničných vecí a európskych záležitostí SR (MZVaEZ), ktoré v júli 2017 vytvorilo Oddelenie strategickej komunikácie (StratCom oddelenie) – koordinačný útvar v priamej riadiacej pôsobnosti ministra. StratCom oddelenie zároveň pôsobí ako stály sekretariát Pracovnej skupiny pre strategickú komunikáciu, na ktorej práci sa podieľajú členovia kabinetov ministra a štátnych tajomníkov, odbor politických vzťahov EÚ, odbor vnútorných záležitostí a inštitúcií EÚ, odbor bezpečnostnej politiky, odbor analýz a plánovania, odbor verejnej diplomacie, tlačový odbor, odbor vzdelávania a prípravy a finančný odbor. V auguste 2017 vedenie MZVaEZ SR schválilo materiál *Koncepcia strategickej komunikácie.*[54]

Hlavným cieľom StratCom oddelenia MZVaEZ SR je vyvíjať dlhodobé a systematické komunikačné aktivity zamerané na budovanie podpory verejnosti pre strategickú orientáciu európskej, zahraničnej a bezpečnostnej politiky SR. V rámci týchto aktivít sa zameriava na štyri prioritné oblasti – EÚ, NATO, poslanie a význam zahraničnej politiky pre štát a jeho obyvateľov a boj proti dezinformáciám a nepriateľskej propagande. S týmto zámerom spustilo MZVaEZ SR dva komunikačné programy, ktorých cieľom je zvyšovať povedomie verejnosti o členstve Slovenska v EÚ a NATO a zdôrazňovať, že Slovensko patrí k pro-európsky a pro-atlanticky orientovaným krajinám.

Komunikačný program *#MYSMEEÚ* vytvára priestor pre celospoločenskú diskusiu o tom, aké má byť postavenie SR v EÚ a aká je jej budúcnosť vo svetle výziev, ktorým dnes čelí. *#MYSMEEÚ* je séria diskusií na slovenských univerzitách, na ktorých sa okrem študentov zúčastňujú zástupcovia politických strán, mimovládnych organizácií, médií a podnikateľskej sféry. Jej súčasťou sú aktivity zamerané na budovanie povedomia študentov a pedagógov o EÚ a NATO, budovanie odolnosti voči dezinformáciám a posilňovanie schopností študentov myslieť kriticky. V rámci komunikačných aktivít o NATO sa MZVaEZ SR ako jedna

http://www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=2766

51 Správa o činnosti Vojenského spravodajstva za rok 2017, 2018, http://vs.mosr.sk/sprava-o-cinnosti-vs-2017/

52 LP/2017/640 Návrh Obrannej stratégie Slovenskej republiky, 2016, https://www.slov-lex.sk/legislativne-procesy/-/SK/LP/2017/640

53 Bezpečnostná rada SR, Terminologický slovník krízového riadenia, 2017, http://www.vlada.gov.sk/data/files/7200_terminologicky-slovnik-uprava.pdf

54 Jedná sa o interný materiál MZVaEZ SR, ktorý nie je verejne dostupný.

z 5 pilotných krajín zapojilo do programu *#WeAreNATO* (My sme NATO). Jeho úlohou je vysvetľovať verejnosti význam Aliancie pre slovenskú bezpečnosť a informovať najmä mladšie generácie, ktoré nemali bezprostrednú skúsenosť s politickou realitou a okolnosťami spred roku 1989, o hodnotách a úlohách NATO, o jej prioritách a fungovaní.

Pri strategickej komunikácii MZVaEZ SR využíva sociálne siete – hlavne facebookový profil *„Zahraničná politika sa nás týka“*, kde neformálnym a audiovizuálne pútavým spôsobom informuje najmä mladých ľudí a študentov o prioritách zahraničnej politiky SR. Nevyhnutnou súčasťou strategickej komunikácie je však aj osobný kontakt s verejnosťou. Diskusie o EÚ a NATO s verejnosťou, na stredných a vysokých školách, či odborné školenia pre stredoškolských učiteľov, pripravuje ministerstvo aj v spolupráci s mimovládnymi organizáciami. MZVaEZ sa sústredí hlavne na vytváranie vlastného pozitívneho naratívu zdôrazňujúc hodnoty, na ktorých je založená naša spoločnosť. Pre tento účel je však potrebné aktívne zapojenie viacerých ministerstiev a ďalších inštitúcií štátnej správy s ohľadom na splnenie základného predpokladu efektívnosti a účinnosti strategickej komunikácie: tzv. *„whole-of-government-approach“*.

Otázke strategickej komunikácie je venovaná čoraz väčšia pozornosť aj na pôde EÚ a NATO. V júni 2015 EÚ prijala *Akčný plán na strategickú komunikáciu*.[55] Akčný plán vypracovala na podnet Európskej rady[56] vysoká predstaviteľka Únie pre zahraničné veci a bezpečnostnú politiku, Federica Mogherini, v spolupráci s inštitúciami EÚ a členskými štátmi. Akčným plánom sa zriadila osobitá pracovná skupina EÚ pre strategickú komunikáciu v rámci Európskej spoločnej verejnej činnosti (EEAS) s názvom East StratCom Task Force ako reakcia na pretrvávajúce dezinformačné kampane Ruskej federácie.[57] Ciele akčného plánu boli veľmi jednoznačné:

- *“efektívna komunikácia európskych politík a hodnôt voči krajinám Východného partnerstva*
- *posilnenie mediálneho prostredia vrátane podpory nezávislých médií;*
- *zvýšiť povedomie verejnosti o dezinformačných aktivitách externých aktérov a zlepšiť schopnosť EÚ predvídať a reagovať na tieto aktivity.”*[58]

V novembri 2016 prijal Európsky parlament *Uznesenie č. 2016/2030(INI) o strategickej komunikácii EÚ s cieľom bojovať s propagandou tretích strán zameranou proti Únii.*[59] V bode 37 tohto uznesenia Európsky parlament *„zdôrazňuje zodpovednosť členských štátov za to, aby aktívne, preventívne a v spolupráci bojovali proti nepriateľským informačným operáciám na svojom území alebo namiereným proti ich záujmom; naliehavo vyzýva vlády členských štátov, aby vytvorili vlastné schopnosti v oblasti strategickej komunikácie.“* V januári 2018 zriadila Európska komisia Expertnú skupinu na vysokej úrovni, zaoberajúcu sa falošnými správami a dezinformáciami šírenými na internete. Expertná skupina na vysokej úrovni vypracovala v marci správu *A multi-dimensional approach to disinformation,*[60] ktorá skúma príklady dobrej praxe v oblasti odolnosti voči dezinformáciám a vhodných spôsobov reakcií na dezinformácie. EÚ tiež na jar zrealizovala verejnú konzultáciu, ako aj špecializovaný Eurobarometer.[61] V júli 2018 predstavila Expertná skupina na vysokej úrovni návrh kódexu postupov proti šíreniu dezinformácií.[62]

Aby NATO vhodne, včas, presne a pohotovo informovalo o vývoji svojich úloh, cieľov a misií, zriadilo v roku 2014 v Lotyšsku Centrum excelentnosti NATO pre strategickú komunikáciu (NATO StratCom COE). Centrum prispieva k zlepšeniu komunikačných kapacít v rámci Aliancie, ale aj spojeneckých štátov. Strategická komunikácia sa stala integrálnou súčasťou politických a vojenských cieľov Aliancie. Slovenská republika by mala mať svojho poverenca v NATO StratCom COE od roku 2019.

55 Akčný plán EÚ na strategickú komunikáciu (Ref. Ares(2015)2608242 – 22/06/2015), 2015, http://archive.eap-csf.eu/assets/files/Action%20PLan.pdf
56 Závery zasadnutia Európskej rady z 19-20. marca 2015, http://data.consilium.europa.eu/doc/document/ST-11-2015-INIT/en/pdf
57 Aktuálne Strategic Communication Division obsahuje 3 pracovné skupiny – East, Western Balkans a South StratCom Task Force.
58 Akčný plán EÚ na strategickú komunikáciu (Ref. Ares(2015)2608242 – 22/06/2015), 2015, http://archive.eap-csf.eu/assets/files/Action%20PLan.pdf
59 Európsky parlament, Uznesenie Európskeho parlamentu z 23. novembra 2016 o strategickej komunikácii EÚ s cieľom bojovať s propagandou tretích strán zameranou proti Únii, 2016, http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2016-0441&language=SK&ring=A8-2016-0290
60 Európska komisia, Finálna správa Expertnej skupiny na vysokej úrovni pre oblasť falošných správ a dezinformácií, 2018, https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation
61 Európska komisia, Výsledky konzultácií, 2018, https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-fake-news-and-online-disinformation
62 Európska komisia, Návrh kódexu postupov proti šíreniu dezinformácií, 2018, https://ec.europa.eu/digital-single-market/en/news/draft-code-practice-online-disinformation

3.2 KYBERNETICKÁ BEZPEČNOSŤ

Pavol Draxler

ÚVOD

Informačné a komunikačné technológie predstavujú vzhľadom na ich vplyv na chod štátu jeden z hlavných cieľov hybridného útoku na krajinu. Útočiaca krajina je s relatívne nízkymi nákladmi a z bezpečia kancelárií domovskej krajiny schopná spôsobiť rozsiahle ekonomické škody, dokonca až ochromiť chod krajiny. Jeden z prvých významných útokov, ktorý dostal ochranu informačných a komunikačných technológií (IKT) medzi priority národnej bezpečnosti, sa odohral voči Estónsku v roku 2007. V tom čase bola informatizácia v Estónsku na ďaleko vyššej úrovni ako v ostatných krajinách EÚ. Jednalo sa o vcelku primitívny útok znefunkčnenia štátnych webstránok zahltením. Útok bol dôsledkom vtedy aktuálnej diplomatickej roztržky medzi Estónskom a Ruskom. Aj napriek slabým následkom tento útok demonštroval motiváciu využiť možnosť útokov na IKT proti inej krajine. Od tohto útoku ubehlo už viac ako desaťročie. Za tú dobu sa aktivity vo významnej miere presunuli z fyzického do virtuálneho sveta. Krajiny sa stali zraniteľnými a doslova závislými na IKT. Útoky cez IKT infraštruktúru preto predstavujú veľmi efektívny nástroj v medzinárodných konfliktoch.

PREHĽAD RELEVANTNEJ LEGISLATÍVY A JEJ STRUČNÁ ANALÝZA

SR dnes do veľkej miery nie je proaktívna, čo sa týka legislatívy upravujúcej pôsobnosti v oblasti informačnej ochrany. Legislatíva značne kopíruje medzinárodné záväzky a legislatívu EÚ. Významné sú v tomto ohľade predovšetkým dve nariadenia Európskej komisie, ktoré boli premietnuté do národnej legislatívy. V prvom rade sa jedná o nariadenie k bezpečnosti informačných systémov a sietí, tzv. NIS,[63] ktoré bolo premietnuté do národnej legislatívy v podobe zákona o kybernetickej bezpečnosti.[64] Čiastočne bezpečnosť informácií a budovania ochrany rieši aj nariadenie EK GDPR[65] o ochrane osobných údajov. Značná časť tohto nariadenia ukladá povinnosti chrániť osobné údaje a budovať bezpečnosť ich spracovávateľom. Nariadenie GDPR bolo premietnuté do národnej legislatívy zákonom č. 18/2018 o ochrane osobných údajov. Obe tieto nariadenia boli prijaté európskymi inštitúciami v roku 2016 s účinnosťou od mája 2018.

EÚ sa problematike kybernetickej bezpečnosti venuje systematicky od deväťdesiatych rokov. Základy súčasnej podoby integrovanej informačnej ochrany EÚ boli položené v roku 2001 prijatím návrhu politiky pre Sieťovú a informačnú bezpečnosť COM 2001-298.[66] Politika definovala potreby ochrany kritickej digitálnej infraštruktúry a vznik národných CSIRT tímov. V roku 2006 EK prijala *Stratégiu pre bezpečnú informačnú spoločnosť* COM 2006-251.[67] Definovala potrebu koordinácie národných CSIRT tímov a pôsobnosť Európskej agentúry pre bezpečnosť sietí a informácií (ENISA). ENISA sa medzičasom stala lídrom v koordinácii a metodike pre informačnú bezpečnosť v Európe. Materiály a práca ENISA predstavujú dnes kvalitný základ metodík pre prácu ako národných tak aj privátnych CSIRTov.

63 Európsky parlament, Rada EÚ, Smernica 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii, 2016, https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:32016L1148&from=EN
64 Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti, ktorý nadobudol účinnosť 1. apríla 2018
65 Európsky parlament, Rada EÚ, Nariadenie 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa ruší smernica 95/46/ES (všeobecné nariadenie o ochrane údajov), 2016, https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:32016R0679&from=EN
66 The Council of the European Union, Network and Information Security: Proposal for a European Policy Approach, 2001, http://ec.europa.eu/transparency/regdoc/index.cfm?fuseaction=list&coteId=1&year=2001&number=298&language=EN
67 Komisia Európskych spoločenstiev, Stratégia pre bezpečnú informačnú spoločnosť – „Dialóg, partnerstvo a aktívne pôsobenie“, 2006, https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:52006DC0251&from=en

Komisia v roku 2009 prijala oznámenie o ochrane kritických informačných infraštruktúr s názvom *Ochrana Európy pred rozsiahlymi kybernetickými útokmi a narušeniami: zvyšovanie pripravenosti, bezpečnosti a odolnosti*, ktorým sa ustanovuje plán (ďalej len „akčný plán CIIP“)[68] na posilnenie bezpečnosti a odolnosti životne dôležitých infraštruktúr v rámci informačných a komunikačných technológií. Tieto návrhy politík boli neskôr pretavené do aktuálneho nariadenia NIS.

Aj napriek tomu, že sa jedná o rozdielne pôsobnosti ako ochrana dôležitých hospodárskych odvetví v prípade NIS a ochrana osobných údajov v prípade GDPR, ide o prelomové nariadenia, ktoré po prvý raz ukladajú jasné povinnosti informačnej ochrany dotknutým subjektom plošne. Takáto povinnosť sa do prijatia týchto nariadení týkala len niektorých regulovaných odvetví a nebola vždy konzistentná. Prijatie tejto legislatívy, predovšetkým NIS, jasne pomenovalo kritické odvetvia, v prípade ktorých, ak by došlo k bezpečnostnému incidentu, by následkom boli vážne dopady na občanov krajiny. Pred prijatím nariadenia NIS taktiež absentovala konzistencia štátnych útvarov, ktoré sa mali venovať problematike informačnej ochrany v krajinách EÚ, ako aj ich pôsobnosť. To prinášalo problémy v medzinárodnej spolupráci, ktorá má v tejto oblasti obzvlášť vysokú dôležitosť, keďže v prípade informačných technológií hranice štátov pri útokoch nehrajú veľkú rolu.

Slovenská implementácia zákona o kybernetickej ochrane do veľkej miery vychádza z nariadenia NIS. Slovenskému zákonu sa však dá vytknúť, že je orientovaný predovšetkým represívne voči súkromnému sektoru a na druhej strane sú štátne inštitúcie, do veľkej miery konštituované ako uzavreté jednotky so slabo vyšpecifikovanou transparentnosťou. Taktiež spolupráca so súkromným sektorom, ktorá je pre ochranu informačného prostredia kritická, je v spomínanom zákone adresovaná značne vágne. Existuje preto oprávnená obava, že vzniknuté inštitúcie nenadobudnú potrebnú dôveru súkromného sektora, čo v konečnom dôsledku môže ohroziť využitie potenciálu dosiahnutej úrovne celkovej bezpečnosti krajiny proti hybridným hrozbám.

PREHĽAD VEREJNÝCH POLITÍK

Slovenská republika prijala v oblasti ochrany informačného prostredia niekoľko materiálov. Všetky materiály boli prijaté so značným oneskorením oproti ostatným členským štátom EÚ a tiež neskôr, ako bolo pôvodne oznámené. To môže ilustrovať, že táto oblasť nebola vždy považovaná za prioritnú, čo spôsobilo, že stratené roky dobiehame dodnes. Národná stratégia pre informačnú bezpečnosť v Slovenskej republike69 prijatá v roku 2008 bola prvým komplexným materiálom, ktorá sa venovala problematike informačnej bezpečnosti a vytýčila predpoklady pre zriadenie kontaktného miesta pre riešenie bezpečnostných incidentov – CSIRT. SK a problematika informačnej bezpečnosti bola zaradená do gescie Ministerstva financií. Úlohy z tejto národnej stratégie boli rozpracované v Akčnom pláne informačnej bezpečnosti na roky 2009-2013[70]. *Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020*[71] túto problematiku na centrálnej národnej úrovni preniesla na Národný bezpečnostný úrad. Koncepcia sa venovala hlavne oblasti zodpovednosti a kompetencii strešného štátneho útvaru a podriadeným útvarom, pod ktoré by problematika mala spadať.

68 Komisia Európskych spoločenstiev, „Ochrana Európy pred rozsiahlymi kybernetickými útokmi a narušeniami: zvyšovanie pripravenosti, bezpečnosti a odolnosti“, 2009, https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:52009DC0149&from=EN

69 Vláda Slovenskej republiky, Národná stratégia pre informačnú bezpečnosť v Slovenskej republike, (č. mat. ÚV-18175/2008) schválila 27. augusta 2008 uznesením č.570/2008.č

70 Vláda Slovenskej republiky, Akčný plán na roky 2009 až 2013 k dokumentu Národná stratégia pre informačnú bezpečnosť v Slovenskej republike schválený uznesením vlády č. 46/2010 zo dňa 19.1.2010 http://www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=12605

71 Schválená vládou SR 17. júna 2015 vláda uznesením č. 328/2015,

V aplikačnej rovine je dôležitý ***Akčný plán realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020.***[72] Akčný plán obsahuje návrh úloh, ktorých cieľom je zabezpečiť primeranú ochranu kybernetického priestoru štátu pred potenciálnymi hrozbami, ktorých uplatnením by mohli vzniknúť Slovenskej republike nenahraditeľné škody, čím by mohla byť narušená dôveryhodnosť štátu či organizácie. Akčný plán ku Koncepcii je jeden zo základných dokumentov definujúcich zoznam úloh na obdobie rokov 2016 až 2020 zameraných na tvorbu právnych predpisov, štandardov, metodických pokynov, pravidiel, bezpečnostných politík, medzinárodnej spolupráce, zvyšovania povedomia a spôsobilostí, ako aj iných aktivít potrebných k zaisteniu ochrany a obrany národného kybernetického priestoru.

Zásadným materiálom bola štúdia uskutočniteľnosti ***Národné systémy riadenia incidentov kybernetickej bezpečnosti vo verejnej správe***[73] z roku 2018. Dokument vyhodnotil aktuálny stav štyroch centrálnych útvarov, ktoré majú na starosti ochranu strategických oblastí štátnej správy a priniesol sumu potrebnú pre investície do infraštruktúry. Oficiálne materiály predstavujú možnosť, ako komunikovať verejnosti zámery štátnej správy, zadefinovať ciele, merateľné kritéria a odôvodniť efektivitu využitia zdrojov. Táto štúdia bola ale podrobená kritike odbornej verejnosti pre jej kvalitu, metodológiu a hlavne netransparentnosť.[74]

72 Návrh akčného plánu vláda Slovenskej republiky schválila dňa 2. marca 2016 uznesením č. 93/2016,
73 Úrad podpredsedu vlády SR pre investície a informatizáciu, Verejné prerokovanie v národnom projekte kybernetickej bezpečnosti vo verejnej správe, 2018,
74 TASR, K novým štátnym IT projektom majú odborníci viacero výhrad, Pravda, 2016, https://spravy.pravda.sk/ekonomika/clanok/477609-k-novym-statnym-it-projektom-maju-odbornici-viacero-vyhrad/

3.3 ENERGETICKÁ BEZPEČNOSŤ

Matúš Mišík

ÚVOD

Energetická infraštruktúra patrí medzi jedny z najrozvinutejších, a preto sa hrozby, vrátane tých hybridných, ktoré zasahujú rôzne typy infraštruktúry, dotýkajú aj tohto typu. Predovšetkým kybernetické hrozby môžu zasahovať aj vysoko sofistikovanú a elektronizovanú energetickú infraštruktúru, ako napríklad elektrifikačné siete (vrátane rozvodní), plynovody, ropovody, skladiská ropy a ropných produktov, zásobníky plynu a pod. Nielen prepravná infraštruktúra sa však môže stať terčom hybridných hrozieb, ale aj ďalšie časti energetickej infraštruktúry, ako napríklad elektrárne, môžu byť cieľom. Hybridné útoky môžu mať značné následky nielen z pohľadu energetickej bezpečnosti (neočakávané výpadky dodávok rôznych druhov energie), ktorá má významné prepojenie s ďalšími rizikami (výpadky elektrického prúdu, nedostatok zemného plynu a pod.), ale taktiež pre oblasť tzv. „hard security" (napríklad pri kybernetickom útoku na jadrovú elektráreň). Niektorí analytici zaraďujú medzi hybridné hrozby aj vysokú závislosť na dodávkach energetických surovín z tretích krajín.[75]

VÝZNAM HYBRIDNÝCH HROZIEB SPOJENÝCH S ENERGETICKOU BEZPEČNOSŤOU PRE SLOVENSKO

Keďže Slovensko patrí medzi významné tranzitné krajiny a produkuje veľké množstvo elektrickej energie z jadra, hybridné hrozby prepojené s energetickou bezpečnosťou predstavujú významný, avšak koncepčne zatiaľ takmer úplne nepodložený prvok celkovej bezpečnostnej situácie krajiny.

Slovensko patrí ku krajinám EÚ s najvyšším podielom jadrovej energie na elektrickom energetickom mixe (ktorý hovorí o zložení zdrojov, z ktorých sa elektrická energia vyrába). Z celkovej vyrobenej elektrickej energie na Slovensku (27.1 TWh) pochádzalo v roku 2016 až 14.8 TWh z jadrovej energie,[76] čo je takmer 55%. O dôležitosti jadrovej energetiky pre Slovensko hovorí nielen to, že druhé miesto v produkcii mala vodná energia s omnoho menším podielom (6.9 TWh), ale aj to, že dva nové reaktory, ktoré majú byť dokončené v najbližšom období (Mochovce 3 a 4), prispejú do rozvodnej siete ďalšími približne 7 TWh elektrickej energie ročne. Následne sa zaradí Slovensko medzi čistého vývozcu energie,[77] čo bude mať následky aj pre existujúcu a práve sa rozvíjajúcu infraštruktúru.

Slovensko je významnou tranzitnou krajinou predovšetkým v oblasti zemného plynu. Eustream, slovenský operátor tranzitnej plynovodnej siete, má jednu z kapacitne najväčších prepravných sietí v Európe (s kapacitou vyše 100 mld m^2 zemného plynu ročne na vstupnom bode z Ukrajiny) a k nej pripojenú najväčšiu kompresnú stanicu v EÚ s výkonom 300MW, ktorá sa nachádza vo Veľkých Kapušanoch, ale aj ďalšie menšie kompresné stanice s výkonom ďalších 200MW. SR je v oblasti zemného plynu prepojená s Českom a Rakúskom pomocou spätného chodu na plynovode Bratstvo, s Ukrajinou tzv. malým reverzom cez Budince a s Maďarskom cez vstupný bod Veľké Zlievce. Prepojenie s Poľskom sa v súčasnosti buduje aj s pomocou finančnej podpory zo strany EÚ.[78] Plánovaný plynovod Eustream, ktorý má nahradiť výpadky prepravy po tom, čo pravdepodobne príde k prerušeniu prepravy cez Ukrajinu po roku 2019,[79] je v počiatočnom štádiu príprav, avšak dostáva výraznú politickú podporu zo strany EÚ ako aj vlády SR.

75 Institute for Security Studies, Hybrid threats and the EU, 2017, https://www.iss.europa.eu/sites/default/files/EUISSFiles/EE%20hybrid%20event%20report.pdf
76 Európska komisia, Energy datasheets: EU28 countries, 2018, https://ec.europa.eu/energy/sites/ener/files/documents/countrydatasheets_august2018.xlsx
77 V súčasnosti Slovensko dováža časť elektrickej energie zo zahraničia, avšak predovšetkým z toho dôvodu, že je to výhodnejšie, než ju produkovať v existujúcich elektrárňach.
78 Plynovodné prepojenie s Poľskom bolo zaradené na zoznam Projects of Common Interest a podporené z Connecting Europe Facility.
79 Súčasná prepravná zmluva medzi Gazpromom and Naftogaz Ukrajiny končí 31.decembra 2019, pričom Gazprom už dlhodobejšie znižuje prepravované objemy plynu do Európy cez Ukrajinu, čo mu umožňuje plynovod Nord Stream. S vybudovaním plynovodu Nord Stream 2 bude môcť Gazprom úplne prerušiť tranzit plynu cez Ukrajinu. Viac v Pirani, S., Yafimava, K. (2016) Russian Gas Transit Across Ukraine Post-2019: pipeline scenarios, gas flow consequences, and regulatory constraints. The Oxford Institute for Energy Studies. Aj najnovšie analýzy potvrdzujú možnosť takéhoto scenára, resp. veľmi výrazného zníženia dodávok na úroveň pod 10% celkovej kapacity: Sharples, J. (2018) Ukrainian Gas Transit: Still Vital for Russian Gas Supplies to Europe As Other Routes Reach Full Capacity. The Oxford Institute for Energy Studies.

V oblasti elektrickej energie je významné najmä prepojenie s Českom, ktoré bolo vybudované počas federácie ako súčasť celorepublikovej sústavy. V súčasnosti sa buduje prepojenie s Maďarskom nielen na zvýšenie energetickej bezpečnosti, ale aj ako možný smer vývozu prebytkovej elektrickej energie po dobudovaní jadrovej elektrárne Mochovce 3 a 4. Taktiež v oblasti ropy máme na Slovensku významnú tranzitnú, ako aj rafinérsku kapacitu (Slovnaft, a.s.). Všetky tieto súčasti energetickej infraštruktúry môžu byť napadnuté hybridnými (predovšetkým kybernetickými) hrozbami, ktoré môžu mať významné dopady nielen na energetickú bezpečnosť, ale aj na oblasť „hard security".

ZNÁME HYBRIDNÉ ÚTOKY V OBLASTI ENERGETICKEJ BEZPEČNOSTI

Prvým zaznamenaným kybernetickým útokom na energetické zariadenia bol škodlivý kód ("vírus") Stuxnet objavený v roku 2010. Predpokladá sa, že tento škodlivý kód pôsobil už od roku 2005, pričom sa podľa dostupných informácií zameriaval na centrifúgy v iránskom jadrovom programe. Spôsobil ich znefunkčnenie zvýšením obrátok nad prevádzkové možnosti, čím výrazne negatívne zasiahol iránsku snahu obohacovať urán. Hoci v tomto prípade sa jedná predovšetkým o oblasť „hard security", napojenie na energetickú infraštruktúru je priame, čo naznačuje možnosť využitia podobných postupov aj na ochromenie energetickej infraštruktúry v iných prípadoch.

Novším prípadom je šírenie škodlivého kódu Dragonfly z konca minulého roka, ktorý sa zameriaval na energetickú infraštruktúru v niekoľkých krajinách (USA, Švajčiarsko, Turecko).[80] Skupina šíriaca tento škodlivý kód mala za cieľ spoznať spôsob fungovania infraštruktúry a nájsť spôsob, ako nad ňou prevziať kontrolu. Prišlo však už aj ku konkrétnym útokom, ktoré spôsobili výpadky v sieti. Na konci roku 2016 prišlo k výpadku elektrickej energie v Kyjeve, pričom prevádzkovateľ siete určil kybernetický útok na rozvodňu ako príčinu výpadku.[81] Černobyľ bol napadnutý vírusom Petya, ktorý znemožnil automatizované merania radiácie v prostredí okolo poškodenej jadrovej elektrárne.[82] Aj rozvodná elektrizačná sieť v Írsku sa stala terčom podobného útoku, hoci v tomto prípade neprišlo k výpadku.[83] V USA bola zaznamenaná snaha vniknúť do počítačových systémov jadrových zariadení.[84]

SITUÁCIA NA ÚROVNI EÚ

Európska únia zahŕňa energetiku medzi mnohé ďalšie oblasti, ktorých sa týkajú hybridné hrozby, predovšetkým v súvislosti s ochranou strategickej infraštruktúry. V hlavnom strategickom dokumente, *Spoločný rámec pre boj proti hybridným hrozbám*, tvrdí, že najlepší spôsob, ako reagovať na hybridné hrozby v oblasti energetickej bezpečnosti, je diverzifikácia v prípade energetických sietí a vytváranie najvyšších možných štandardov bezpečnosti v jadrovej energetike.[85] Tento dokument identifikuje taktiež budovanie „smart" technológií ako možnú rizikovú oblasť v rámci energetiky. *Európska energetická bezpečnostná stratégia*[86] sa sústreďuje predovšetkým na tradičné hrozby, hoci spomína taktiež potrebu „zvýšenej pozornosti" bezpečnosti IT v oblasti strategickej infraštruktúry. EÚ kritizovala členské štáty za nezaradenie nových hrozieb (mimo iných aj kybernetický útok) do scenárov, podľa ktorých sa uskutočnili tzv. „stress testy" energetickej bezpečnosti v oblasti zemného plynu.[87] Veľkú pozornosť hybridným hrozbám v oblasti energetiky venuje aj Európska služba pre vonkajšiu činnosť, ktorá taktiež navrhuje diverzifikáciu a budovanie bezpečnostných štandardov ako odpoveď na tieto hrozby.

---

80 Security Response Attack Investigation Team, Dragonfly: Western energy sector targeted by sophisticated attack group, Symantec, 2018, https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks

81 Polityuk, P., Vukmanovic, O., Jewkes, S., Ukraine's power outage was a cyber attack: Ukrenergo, Reuters, 2017, https://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA

82 Griffin, A., 'Petya' cyber attack: Chernobyl's radiation monitoring system hit by worldwide hack, Independent, 2017, https://www.independent.co.uk/news/world/europe/chernobyl-ukraine-petya-cyber-attack-hack-nuclear-power-plant-danger-latest-a7810941.html

83 McMahon, C., 'State-sponsored' hackers targeted EirGrid electricity network in 'devious attack', Independent, 2018, https://www.independent.ie/irish-news/statesponsored-hackers-targeted-eirgrid-electricity-network-in-devious-attack-36005921.html

84 Periroth, N., Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say, The New York Times, 2017, https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html

85 Európska komisia, Spoločný rámec pre boj proti hybridným hrozbám, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=en

86 Európska komisia, Európska stratégia energetickej bezpečnosti, 2014, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0330&from=EN

87 European Commission, Report on the implementation of Regulation (EU) 994/2010 and its contribution to solidarity and preparedness for gas disruptions in the EU, 2014, https://ec.europa.eu/energy/sites/ener/files/documents/2014_energystresstests_securityofgassupplysegulation_report_0.pdf

SITUÁCIA V SLOVENSKEJ REPUBLIKE

Energetika je v rámci *Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020* zaradená medzi kritickú infraštruktúru,88 a takto je k nej pristupované aj v rámci *Akčného plánu realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020*.[89] Ani *Stratégia energetickej bezpečnosti Slovenskej republiky z roku 2008,*[90] ani *Energetická politika SR* sa však explicitne, ale ani implicitne, nevenujú téme hybridných/kybernetických hrozieb. Hlavný dôraz kladú tieto dokumenty v oblasti infraštruktúry na bezpečnosť dodávok a budovanie alternatívnych prepojení. Týmto síce vytvárajú predpoklad pre zvyšovanie bezpečnosti aj v oblasti hybridných hrozieb, avšak tieto dve témy nie sú v strategických dokumentoch prepojené, a preto je ich prepojenie pri koncepčnom plánovaní a budovaní infraštruktúry otázne. Ani každoročne uverejňované správy o výsledkoch monitorovania bezpečnosti dodávok plynu/elektriny neprinášajú informácie o takýchto hrozbách.

Slovenská elektrizačná prenosová sústava, a.s., ktorá má na zodpovednosti prevádzku prenosovej sústavy v Slovenskej republike, prijala *Politiku informačnej bezpečnosti,*[91] avšak tá sa týka snahy *„minimalizovať možnosti úniku a zneužitia citlivých informácií vyskytujúcich sa pri činnosti spoločnosti SEPS“*, nie hybridných hrozieb a kybernetických útokov. Organizácia sa ale pri vzdelávaní zamestnancov zameriava aj na možné kybernetické ohrozenia.[92] Eustream, a.s. sa nevenuje vo svojich výročných správach hybridným/kybernetickým ohrozeniam svojej transportnej siete,[93] a podobná situácia je aj pri preprave ropy. A to aj napriek tomu, že spoločnosť Transpetrol, a.s. implementovala v roku 2017 nový IT systém na integráciu ropovodného informačného systému IRISP, ktorý umožňuje monitorovať prepravný systém z jedného miesta.[94] Takáto zmena môže byť vnímaná ako zvýšenie rizika externého kybernetického útoku. Slovenské elektrárne, a.s. sa v krátkosti venujú vo svojej záverečnej správe aj téme kybernetickej bezpečnosti[95].

88 NBÚ, Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020, 2016, http://www.nbusr.sk/wp-content/uploads/kyberneticka-bezpecnost/Koncepcia-kybernetickej-bezpecnosti-SR-na-roky-2015-2020-A4.pdf
89 NBÚ, Akčný plán realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020, 2016, http://www.nbusr.sk/wp-content/uploads/kyberneticka-bezpecnost/Akcny-plan-realizacie-Koncepcie-kybernetickej-bezpecnosti-SR-na-roky-2015-2020.pdf
90 Ministerstvo hospodárstva SR, Stratégia energetickej bezpečnosti SR, 2008, http://www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=14372
91 SEPS, Politika informačnej bezpečnosti, 2016, https://www.sepsas.sk/Dokumenty/PIB/2016/07/11/Politika_inf_bezpecnosti.doc
92 SEPS, Individuálna a konsolidovaná výročná správa 2017, 2018, https://www.sepsas.sk/Dokumenty/Vyrocnespravy/2018/SEPS_VS2017.pdf
93 Eustream, Výročná správa 2017, 2018, http://www.eustream.sk/sk_stiahnut-subor/vyrocna-sprava-2017/860a15c9ad62190b73f22456f97791f4
94 Transpetrol, Výročná správa 2017, 2018, http://www.transpetrol.sk/wp-content/uploads/VS_TRANSPETROL_2017_na-USB.pdf.
95 Slovenské elektrárne, a.s., Výročná správa 2017, 2018, https://www.seas.sk/data/publishing/441/file/se-2017-annual-report.pdf.

3.4 PARAMILITÁRNE A EXTRÉMISTICKÉ SKUPINY

Daniel Milo

ÚVOD

Polovojenské a extrémistické skupiny a hnutia spochybňujú suverenitu a legitimitu štátnej moci pomocou svojho programu, svojimi verejnými aktivitami, prípadne priamym použitím sily či hrozbou jej použitia. Podpora takýchto skupín zo strany zahraničných aktérov, s ktorými častokrát zdieľajú spoločné ciele a ideologické východiská, je integrálnou súčasťou hybridných hrozieb.

Využívanie nepravidelných polovojenských zoskupení rôzneho druhu na podporu dosahovania geopolitických alebo aj taktických či priamo vojenských cieľov je súčasťou doktrín viacerých krajín sveta. Používanie takýchto domácich polovojenských skupín namiesto vlastných uniformovaných ozbrojených síl zvyšuje legitimitu ich aktivít v očiach cieľovej populácie, a zároveň umožňuje popierať priame zasahovanie do vnútorných záležitostí zo strany skutočného aktéra. Aj v prípade, že na území daného štátu neprebieha priamy vojenský konflikt, predstavujú paramilitárne skupiny, napojené personálne, organizačne či ideologicky na cudziu moc, vhodnú základňu na regrutovanie ideologických spojencov. Taktiež môžu byť efektívne využité pri informačných operáciách, využívajúc témy patriotizmu, ochrany vlasti a pod.

Podpora politických subjektov, ktoré spadajú do kategórie politického extrémizmu, je rovnako veľmi významným a často používaným nástrojom na skryté presadzovanie mocenských záujmov cudzích veľmocí na území cieľového štátu. Takéto skupiny odmietajú existujúce usporiadanie spoločnosti, vrátane geopolitickej orientácie a členstva danej krajiny v integračných zoskupeniach (EÚ, NATO), a sú preto prirodzenými spojencami cudzích mocností snažiacich sa tieto zoskupenia oslabiť. Veľakrát sa preto stávajú cieľom vplyvových operácií cudzích mocností a v zmysle hesla „nepriateľ môjho nepriateľa je môj priateľ" sú otvorené podpore zo strany zahraničných aktérov, s ktorými zdieľajú ideologické východiská či geopolitické smerovanie. Podpora môže mať rôzne formy a nemusí byť obmedzená len na priame financovanie, ale napríklad môže ísť o sprostredkovanie kontaktov, ideologickú, informačnú, technologickú či komunikačnú podporu.

PREHĽAD RELEVANTNEJ LEGISLATÍVY A JEJ STRUČNÁ ANALÝZA

Cudzia moc a cudzí činiteľ

Pri hodnotení pôsobenia polovojenských a extrémistických skupín je okrem vyhodnocovania ich nebezpečnosti a kapacít podstatné skúmať aj ich napojenie na zahraničných aktérov. Preto je dôležité, ako sú v slovenskom právnom poriadku zakotvené pojmy cudzia moc a cudzí činiteľ.

Pojmy Cudzia moc a cudzí činiteľ sú upravené v § 133 Trestného zákona (TZ), podľa ktorého: *„(1) Cudzou mocou sa na účely tohto zákona rozumejú cudzie štáty a ich vojenské alebo iné zoskupenia predstavované ich organizáciami a orgánmi, akými sú najmä osoby vykonávajúce spravodajskú činnosť, vojenskí funkcionári, diplomati a iní štátni úradníci. (2) Cudzím činiteľom sa na účely tohto zákona rozumie fyzická osoba alebo právnická osoba, ktorá síce nie je orgánom alebo zástupcom cudzieho štátu, ale vzhľadom na svoje politické, hospodárske alebo spoločenské postavenie má významný vplyv vo svojom štáte alebo v medzinárodných vzťahoch."*[96]

96 300/2005 Z.z. Zákon z 20. mája 2005 ,Trestný zákon, http://www.zakonypreludi.sk/zz/2005-300

Oba tieto pojmy sa v zmysle ustanovení TZ vzťahujú na vybrané druhy trestných činov (najmä siedmej hlavy - trestné činy proti Slovenskej republike), ako je napríklad vlastizrada, vyzvedačstvo, ohrozenie utajovanej skutočnosti, a pod. V širšom kontexte sa však dajú aplikovať aj mimo rámca Trestného zákona na iné typy aktivít predstaviteľov cudzej moci a cudzích činiteľov, ktoré sú spôsobilé ohroziť bezpečnosť a bezpečnostné záujmy SR v kontexte hybridných hrozieb.

Polovojenské skupiny

Postavenie polovojenských skupín nie je v slovenskom právnom poriadku presne vymedzené a v slovenskej legislatíve neexistuje definícia polovojenskej/paramilitárnej skupiny. Jediné významné obmedzenie a sankcie sa týkajú **účasti na bojovej činnosti organizovanej ozbrojenej skupiny na území iného štátu.**

V kontexte hybridných hrozieb je dôležité, že trestné je aj **verejné podnecovanie na spáchanie takéhoto trestného** činu, či **poskytovanie finančných prostriedkov alebo súčinnosti na podporu takéhoto konania**. Takéto typy konania boli v nedávnej minulosti viditeľné najmä v súvislosti s konfliktom na území Ukrajiny, kde sa do bojov zapojili na strane pro-ruských separatistov aj viacerí občania SR a na ich podporu sa konali aj na území SR zbierky financií a vybavenia.

§ 419a Účasť na bojovej činnosti organizovanej ozbrojenej skupiny na území iného štátu.

„(1) Kto sa počas vojny na území iného štátu aktívne podieľa na bojovej činnosti organizovanej ozbrojenej skupiny, potrestá sa odňatím slobody na dva roky až osem rokov.

(2) Rovnako ako v odseku 1 sa potrestá, kto:

a) verejne podnecuje na spáchanie trestného činu uvedeného v odseku 1,

b) požiada iného, aby spáchal alebo mal účasť na spáchaní činu uvedeného v odseku 1,

c) poskytuje alebo prijíma znalosti metód alebo techník na výrobu alebo použitie výbušnín, strelných zbraní alebo iných zbraní, škodlivých látok alebo iných nebezpečných látok alebo iných špeciálnych metód alebo techník určených k vedeniu boja na účely spáchania činu uvedeného v odseku 1, alebo

d) poskytne finančné alebo iné prostriedky, služby, súčinnosť alebo vytvorí iné podmienky na účely spáchania trestného činu uvedeného v odseku 1.“[97]

Toto ustanovenie sa ale v praxi zatiaľ nevyužilo.

Iné dôležité obmedzenie aktivít polovojenských skupín vyplýva z dikcie zákona o združovaní občanov (Zákon č. 83/1990 Zb.), ktorý stanovuje v § 4 nasledovné obmedzenia združovacieho práva:

*„Nie sú dovolené združenia a) ktorých cieľom je (.....) **podporovať násilie** alebo inak porušovať ústavu a zákony; b) ktoré sledujú dosahovanie svojich cieľov spôsobmi, ktoré sú v rozpore s ústavou a zákonmi; c) o**zbrojené alebo s ozbrojenými zložkami**; za také sa nepovažujú združenia, ktorých členovia držia alebo používajú strelné zbrane na športové účely.“*

Problémom predmetnej úpravy je otázka, čo všetko spadá pod športové účely a ako oddeliť legitímne kluby vojenskej histórie, paintballové či airsoftové kluby od polovojenských skupín, ktoré sa pripravujú na ozbrojený konflikt a trénujú vojenské zručnosti s veľmi nejasným alebo dokonca priamo nepriateľským úmyslom voči existujúcej štátnej moci.

97 Ibid.

Extrémistické skupiny

Slovenský právny poriadok sankcionuje založenie, podporu a propagáciu extrémistických skupín v zákone č. 300/2005 Zb. (*Trestný zákon*) § 421 - t.č. založenie, podpora a propagácia hnutia smerujúceho k potlačeniu základných práv a slobôd. Skupina osôb sa v zmysle §129 ods. 3 *Trestného zákona* stáva extrémistickou vtedy, keď sa spolčí za účelom spáchania jedného alebo viacerých trestných činov extrémizmu uvedených v §140a (verejné prejavy sympatií k hnutiu smerujúcemu k potlačeniu základných práv a slobôd; výroba, rozširovanie a prechovávanie extrémistických materiálov; popieranie a schvaľovanie holokaustu; hanobenie národa, rasy a presvedčenia, podnecovanie k národnostnej, rasovej a etnickej nenávisti atď.).

Trestný zákon ani *Zákon o združovaní občanov* však neobsahujú nijaké ustanovenia, ktoré by pokrývali podporu takýchto aktivít zo strany cudzej moci alebo cudzích činiteľov.

VEREJNÉ POLITIKY SR

Problematika polovojenských a extrémistických skupín sa týka najmä nasledovných verejných politík:

- *Koncepcia boja proti extrémizmu SR na roky 2015-2019,*[98]
- *Koncepcia boja Slovenskej republiky proti hybridným hrozbám,*[99]
- *Národný akčný plán boja proti terorizmu na roky 2015 – 2018.*[100]

Z uvedených dokumentov sa však aktivít polovojenských a extrémistických skupín v kontexte hybridných hrozieb dotýka len *Koncepcia boja SR proti hybridným hrozbám*, ktorá na str. 3 konštatuje:

*„Potenciálnou hybridnou hrozbou voči bezpečnosti SR môže byť aj **podpora domácich radikálnych organizácií presadzujúcich ciele totožné s cieľmi aktérov hybridných hrozieb. Radikálne subjekty môžu mať politickú a finančnú podporu zo zahraničia s cieľom propagácie nacionalistických a izolacionistických tendencií, šírenia národnostnej alebo náboženskej nenávisti a destabilizácie spoločnosti.** (.....) Vývoj na východe Ukrajiny a na Kryme, ale aj v konfliktných zónach na Blízkom východe a v severnej Afrike ukazuje aj na **zvýšené riziko podpory poskytovanej radikálnym ozbrojeným skupinám alebo jednotlivcom a samozvaným domobranám zo strany štátnych a neštátnych aktérov, ktoré môžu byť zneužité na diverzné útoky proti infraštruktúre, teroristické útoky alebo vyvolávanie nepokojov.“*[101]

Koncepcia boja SR proti hybridným hrozbám je jediným oficiálnym dokumentom verejnej politiky prijatým na úrovni vlády SR, ktorý poukazuje na nebezpečenstvo prepojenia domácich radikálnych a extrémistických či polovojenských skupín na zahraničných aktérov.

98 Koncepcia boja proti extrémizmu na roky 2015 – 2019, 2015, https://www.minv.sk/swift_data/source/policia/naka_opr/nptj/koncepcia%20extremizmus%202015-2019.pdf
99 Koncepcia pre boj Slovenskej republiky proti hybridným hrozbám schválená 11.7.2018 vládou SR uzn. č 345/2018, http://www.rokovania.sk/File.aspx/ViewDocumentHtml/Mater-Dokum-219866?prefixFile=m_
100 Národný akčný plán boja proti terorizmu na roky 2015 – 2018, 2015, https://www.minv.sk/swift_data/source/policia/naka_opr/nptj/NAP%20terorizmus%202015-2018.pdf
101 Koncepcia pre boj Slovenskej republiky proti hybridným hrozbám

EÚ - PREHĽAD NAJDÔLEŽITEJŠÍCH DOKUMENTOV V DANEJ OBLASTI

Problematika paramilitárnych skupín a extrémizmu je na úrovni EÚ upravená najmä v súvislosti s problematikou predchádzania radikalizácie, násilného extrémizmu a terorizmu, vrátane zahraničných bojovníkov (foreign fighters - FF). V tejto súvislosti sú najvýznamnejšími dokumentami:

- *Globálna stratégia pre zahraničnú a bezpečnostnú politiku Európskej únie,*[102]
- *Stratégia EÚ na boj proti terorizmu,*[103]
- *Akčný plán na posilnenie boja proti financovaniu terorizmu,*[104]
- *Stratégia EU pre boj proti radikalizácii a náboru pre účely terorizmu*[105]*,*
- *Rámcové rozhodnutie o boji proti terorizmu.*[106]

S pôsobením polovojenských skupín sa úzko spája fenomén zahraničných teroristických bojovníkov, *„foreign fighters“*. *Európska agenda pre bezpečnosť*[107], prijatá v roku 2015, vyzvala na *„silnú reakciu EÚ na terorizmus a zahraničných teroristických bojovníkov”* a táto výzva bola potvrdená aj v *Oznámení Komisie o podpore predchádzania radikalizácie vedúcej k násilnému extrémizmu*[108] z roku 2016. Vo svojej správe o pokroku vo vzťahu k bezpečnostnej únii začiatkom roku 2018[109] sa fenomén zahraničných bojovníkov, ktorí sa vracajú z konfliktných zón, opäť uznáva ako kľúčová priorita pre bezpečnosť EÚ.

Problematike radikalizácie, ako jednému z aspektov predchádzania terorizmu, bola venovaná pomerne značná pozornosť a v rámci EÚ[110] vzniklo viacero iniciatív a platforiem venovaných radikalizácii. Opäť sa však vo veľkej miere zameriavali najmä na problematiku radikalizácie v kontexte náboženského extrémizmu a opomínali iné zdroje radikalizácie[111]. Žiaden z vyššie uvedených dokumentov však špecificky neadresuje problematiku paramilitárnych skupín či násilného extrémizmu v kontexte hybridných hrozieb.

Najvýznamnejším dokumentom v tejto súvislosti preto ostáva ***Spoločný rámec pre boj proti hybridným hrozbám,***[112] ktorý v časti 4.6 Budovanie odolnosti proti radikalizácii a násilnému extrémizmu uvádza: *„Napriek tomu, že teroristické činy a násilný extrémizmus nemajú sami osebe hybridnú povahu, pôvodcovia hybridných hrozieb sa môžu zamerať na zraniteľných členov spoločnosti, vykonávať ich nábor a radikalizáciu prostredníctvom moderných komunikačných kanálov (vrátane internetových sociálnych médií a skupín priaznivcov) a propagandy.”*

102 Globálna stratégia pre zahraničnú a bezpečnostnú politiku Európskej únie, 2016, https://europa.eu/globalstrategy/sites/globalstrategy/files/eugs_sk_version.pdf
103 Stratégia EÚ na boj proti terorizmu, 2005, http://register.consilium.europa.eu/doc/srv?f=ST+14469+2005+REV+4&l=sk
104 Európska komisia, Akčný plán na posilnenie boja proti financovaniu terorizmu, 2016, https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX%3A52016DC0050
105 Council of the European Union, The Revised European Union Strategy for Combating Radicalisation and Recruitment to Terrorism, 2014 http://data.consilium.europa.eu/doc/document/ST-9956-2014-INIT/en/pdf
106 Council of the European Union, Framework Decision 2002/475/JHA on combating terrorism, 2014, https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/143119.pdf
107 European Commission, The European Agenda on Security, 2015, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf
108 European Commission, supporting the prevention of radicalisation leading to violent extremism, 2016, http://ec.europa.eu/dgs/education_culture/repository/education/library/publications/2016/communication-preventing-radicalisation_en.pdf
109 European Commission, Thirteenth progress report towards an effective and genuine Security Union, 2018, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20180124-progress-report-13-towards-effective-and-genuine-security-union.pdf
110 European Commission, Communication “Preventing Radicalisation To Terrorism and Violent Extremism: Strengthening the EU’s response”, 2014, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2013)0941_/com_com(2013)0941_en.pdf
111 Napr. Oznámenie Komisie Európskemu Parlamentu a Rade EU: Stratégia vnútornej bezpečnosti EÚ: päť krokov k bezpečnejšej Európe - COM/2010/0673 Relevantným je najmä cieľ č. 2: Zabraňovať terorizmu, radikalizácii a náboru nových členov. Oznámenie Komisie Európskemu Parlamentu, Rade, Európskemu Hospodárskemu a Sociálnemu výboru a Výboru regiónov: Predchádzanie radikalizácii vedúcej k terorizmu a násilnému extrémizmu: Posilnenie opatrení EÚ /* COM/2013/0941
112 Európska komisia, Spoločný rámec pre boj proti hybridným hrozbám, 2016, https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:52016JC0018&from=SK

3.5 STRATEGICKÁ KORUPCIA

Michal Piško

ÚVOD

Keď v roku 2017 vydalo medzinárodné združenie investigatívnych novinárov sériu článkov Azerbajdžanská práčka[113] (The Azerbaijani Laundromat) o korupčnom fonde, cez ktorý azerbajdžanské elity uplácali európskych politikov, lobistov a novinárov, zraniteľnosť európskych demokracií sa poodhalila zase o trochu viac. Schéma fungovala pomerne jednoducho. Z fondu, do ktorého prúdili peniaze z neprehľadných schránkových firiem, azerbajdžanských ministerstiev či ruskej zbrojárskej spoločnosti Rosoboronexport, odchádzali vysoké platby na účty vplyvných európskych predstaviteľov, ktorí na oplátku manipulovali verejnou mienkou v prospech autoritatívneho azerbajdžanského režimu.

Spomínaný mechanizmus môžeme bez pochýb označiť za jednu z metód hybridných hrozieb - strategickú korupciu. Ide o prípady, kedy sa štáty alebo iné vplyvné subjekty snažia systematicky využívať korupčné praktiky na získavanie politického vplyvu v zahraničí. Tento vplyv potom využívajú na presadzovanie vlastných geopolitických cieľov. Tieto metódy sú v našom prostredí spájané predovšetkým s mocenskými ambíciami Ruska a niektorých ďalších krajín bývalého Sovietskeho zväzu, ale napríklad aj s Čínou.

PRAX A LEGISLATÍVA

Hrozby vyplývajúce zo strategickej korupcie nie sú v Európe či v Severnej Amerike žiadnou novinkou114 a médiá i verejné inštitúcie venujú týmto témam pozornosť už roky. Široko medializované boli v nedávnej minulosti napríklad podozrenia z napojenia euroskeptických strán vo Francúzsku, Grécku alebo Maďarsku na ruské zdroje financovania.[115]

Hoci Slovensko ako postkomunistická krajina v niekdajšej sfére vplyvu Sovietskeho zväzu patrí medzi zraniteľné štáty, hrozby strategickej korupcie sú u nás takmer neprebádané. Súdy a orgány činné v trestnom konaní dosiaľ takéto prípady neriešili. Ako ukázali viaceré štúdie[116] domácej pobočky Transparency International, na Slovensku sa sústredíme predovšetkým na odhaľovanie malej korupcie. V súvislosti s korupčnými trestnými činmi nebol u nás doteraz právoplatne odsúdený žiadny vysokopostavený politik. V rokoch 2014 až 2017 sa len každý šiesty korupčný prípad pojednávaný na súdoch týkal uplácania nad 5000 eur, v rokoch 2011 až 2014 predstavoval tento pomer dokonca len tri percentá. Prípadom korupcie s účasťou zahraničného verejného činiteľa sa naše súdy za celé sledované obdobie nezaoberali ani raz.

Viaceré indície naznačujúce snahy o získavanie vplyvu a manipulovanie verejnou mienkou aj pomocou utajeného financovania priniesli médiá. Keďže privatizácia štátnych podnikov je na Slovensku už relatívne dávnou minulosťou a dávnejšie boli ukončené aj deblokácie ruského dlhu, medializované prípady sa v posledných rokoch týkali predovšetkým využívania ruského vplyvu v zbrojárskom priemysle a energetike, ako aj podpory pre niektoré politické subjekty alebo takzvané alternatívne médiá.

Nemecká televízia ZDF napríklad minulý rok publikovala podozrenia o napojení viacerých stredoeurópskych strán, vrátane slovenskej parlamentnej Ľudovej strany Naše Slovensko, extrémistu Mariana Kotlebu, na prokremeľských ruských oligarchov.[117] Preverovanie podozrení slovenskou políciou skončilo bezúspešne.

113 Kolektív ČCIŽ, Jak Ázerbájdžán korumpoval evropské politiky, České centrum pro investigativní žurnalistiku, 2017, https://www.investigace.cz/jak-azerbajdzan-korumpoval-evropske-politiky/
114 Applebaum, A., Špinavé peniaze a politická korupcia ničia Západ, musíme sa brániť spoločne, Denník N, 2018, https://dennikn.sk/1220980/spinave-peniaze-a-politicka-korupcia-nicia-zapad-musime-sa-branit-spolocne/
115 Foster, P., Holehouse, M., Russia accused of clandestine funding of European parties as US conducts major review of Vladimir Putin's strategy, The Telegraph, 2016, https://www.telegraph.co.uk/news/worldnews/europe/russia/12103602/America-to-investigate-Russian-meddling-in-EU.html
116 Šípoš, G., Šimalčík, M., Všetko, čo potrebujete vedieť o stíhaní korupcie na Slovensku, Transparency International Slovensko, 2017, https://transparency.blog.sme.sk/c/471000/vsetko-co-potrebujete-vediet-o-stihani-korupcie-na-slovensku.html
117 ČTK, Odhalenie nemeckej televízie: Kotlebovci dostávali peniaze od prokremeľského podnikateľa, Hospodárske noviny, 2017, https://hnonline.sk/svet/969022-odhalenie-nemeckej-televizie-kotlebovci-dostavali-peniaze-od-prokremelskeho-podnikatela

Viaceré médiá informovali aj o zvukovom zázname rozhovoru medzi šéfredaktorom konšpiračného časopisu Zem a Vek Tiborom Eliotom Rostasom a ruským veľvyslancom na Slovensku, Pavlom Kuznecovom, z roku 2014, ktorý sa neskôr objavil na internete.[118] Rostas sa na ňom veľvyslanca pýta na možnosti ruskej podpory pre médium i prípadnú politickú stranu, ktoré by propagovali väčšiu vzájomnosť a užšiu spoluprácu s Ruskom. Kotlebovu stranu a konšpiračný časopis spája okrem slabosti voči mocnému Rusku aj burcovanie verejnosti proti EÚ a najmä proti NATO.

Kým zahraničný politický sponzoring u nás *Zákon o politických stranách a politických hnutiach*[119] jasne zakazuje, pri ďalších subjektoch treba rozlišovať najmä povahu tejto podpory.

V susednom Česku sa napríklad v posledných rokoch veľa diskutuje aj o rizikách spojených s posilňovaním ekonomického a politického vplyvu Číny,[120] ktorá ohlasuje v strednej Európe masívne investície, predovšetkým cez svoje štátne firmy. V tomto prípade môže ísť samozrejme aj o legitímne využívanie podnikateľských príležitostí. Ak by však tieto investície boli podmieňované napríklad privieraním očí či priam obhajobou porušovania ľudských práv komunistickým režimom, ako to naznačujú viacerí českí pozorovatelia,[121] pre demokratickú krajinu by to mal byť nepochybne vážny problém. Časť ohlásených čínskych investícií má pritom smerovať aj na Slovensko a táto téma si preto zasluhuje väčšiu mieru pozornosti.

Ovplyvňovať smerovanie Slovenska a ďalších postkomunistických krajín sa, na druhej strane, cez podporu mnohých aktivít občianskeho či verejného sektora snažia aj viaceré vyspelé demokracie ako sú Spojené štáty americké alebo krajiny západnej Európy. V týchto prípadoch však ide predovšetkým o podporu z oficiálnych schém verejných inštitúcií alebo súkromných fondov a nadácií, kde sú ciele i zdroje tejto podpory jasne verejne deklarované a nijakým spôsobom nepodkopávajú demokratické zriadenie.

Neprebádanosť hrozieb strategickej korupcie na Slovensku sa neprejavuje iba v rozhodovacej činnosti súdov a orgánov činných v trestnom konaní, či vo výstupoch investigatívnych žurnalistov a názoroch verejnosti (v dotazníku GLOBSEC pre zástupcov verejnej správy[122] z augusta 2018 označili Slovensko za veľmi zraniteľné strategickou korupciou iba 3 zo 41 respondentov). Podobný stav panuje aj v oblasti strategických dokumentov, hodnotiacich správ a legislatívy.

Posledná dostupná verejná správa Slovenskej informačnej služby[123] za rok 2017 sa v prípade hrozieb zo zahraničia zameriava predovšetkým na činnosť cudzích spravodajských služieb, teroristické hrozby a energetickú bezpečnosť Slovenska. V otázke hybridných hrozieb osobitne vyzdvihuje činnosť súkromných vojenských spoločností, pri ďalších podrobnostiach sa odvoláva na *Koncepciu boja SR proti hybridným hrozbám,*[124] na ktorej príprave sa podieľala.

Koncepcia vypracovaná pod gesciou premiéra a predsedu Bezpečnostnej rady SR má päť strán a riziká spojené so strategickou korupciou spomína len veľmi všeobecne. Pojem *korupcia* sa v dokumente vôbec nevyskytuje.

Podobne sú na tom aj ďalšie súvisiace koncepčné dokumenty. *Bezpečnostná stratégia SR*[125] hybridné hrozby popisuje iba vo všeobecnosti a korupčné praktiky spája predovšetkým s organizovaným zločinom. *Obranná stratégia SR*[126] z rovnakého roku spomína tieto témy ešte okrajovejšie. *Správa o bezpečnosti SR za rok 2016*[127] redukuje nástroje hybridných hrozieb predovšetkým na kybernetické riziká a dezinformácie.

118 Harkotová, S., Nahrávka ze světa médií ukazuje, jak se žádá o podporu ruské propagandy, neovlivni.cz, 2016, https://neovlivni.cz/nahravka-ze-slovenska-ukazuje-jak-se-zada-o-podporu-ruske-propagandy/
119 Zákon o politických stranách a politických hnutiach, Národná rada SR, 2005, https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2005/85/20160701
120 Šafaříková, K., Součástí obžaloby čínské CEFC z korupce je česká stopa, Respekt, 2018, https://www.respekt.cz/politika/ceska-stopa-je-soucasti-obzaloby-cinske-firmy-cefc-z-korupce
121 Gavenda, J., Češi nechtějí upřednostnit čínské investice před ochranou lidských práv, ukázal průzkum pro ČRo, irozhlas.cz, 2016, https://www.irozhlas.cz/zpravy-domov/cesi-nechteji-uprednostnit-cinske-investice-pred-ochranou-lidskych-prav-ukazal-pruzkum-pro-cro_201603280843_mvydrova
122 GLOBSEC, Mapovanie postojov a povedomia predstaviteľov verejnej správy o problematike hybridných hrozieb, GLOBSEC, 2018
123 Slovenská informačná služba, Správa o činnosti SIS za rok 2017, 2018, http://www.sis.gov.sk/pre-vas/sprava-o-cinnosti.html
124 Vláda SR, Návrh Koncepcie pre boj Slovenskej republiky proti hybridným hrozbám, 2018, https://rokovania.gov.sk/RVL/Material/23100/1
125 Vláda SR, Bezpečnostná stratégia Slovenskej republiky, 2017, https://rokovania.gov.sk/RVL/Material/22364/1
126 Vláda SR, Obranná stratégia Slovenskej republiky, 2017, https://rokovania.gov.sk/RVL/Material/22367/1
127 Vláda SR, Správa o bezpečnosti Slovenskej republiky za rok 2016, 2017, https://rokovania.gov.sk/RVL/Material/22165/1

Komplexnejší prístup poskytujú strategické a koncepčné dokumenty na úrovni EÚ, ako sú *Európsky program v oblasti bezpečnosti,*[128] *Globálna stratégia pre zahraničnú a bezpečnostnú politiku EÚ,*[129] *Akčný plán v oblasti európskej obrany*,[130] *Stratégia kybernetickej bezpečnosti EÚ,*[131] *Rámec proti praniu špinavých peňazí a financovaniu terorizmu*,[132] *Európska stratégia energetickej bezpečnosti*133 *alebo Stratégia námornej bezpečnosti EÚ*.[134]

Kľúčovým dokumentom Únie v tejto oblasti je najmä Spoločný rámec pre *boj proti hybridným hrozbám*[135] z roku 2016, ktorý definuje 22 konkrétnych opatrení na úrovni Únie i členských štátov. Aj tento dokument však riziká strategickej korupcie zaznamenáva skôr okrajovo. Zameriava sa pri nich najmä na sledovanie podozrivých tokov peňazí, ktoré by mohli prispievať k skrytejším formám destabilizácie členských krajín EÚ.

Z hľadiska slovenskej legislatívy spadá protiprávne konanie, ktoré možno spájať s rizikami strategickej korupcie, predovšetkým pod *Trestný zákon*.[136] Ten rieši aj zahraničnú korupciu, ide však iba o trestné činy prijímania úplatku a podplácania, ktorých sa dopustia zahraniční verejní činitelia v súvislosti s výkonom úradných povinností alebo s výkonom ich funkcie. V ostatných prípadoch naša legislatíva zahraničný rozmer spomínaných praktík nerieši. Do úvahy ešte pripadajú trestné činy proti základom republiky alebo ďalšie paragrafy uplatňované v prípade domácej korupcie.

Pri preverovaní finančného pozadia prípadov strategickej korupcie by mohli orgány činné v trestnom konaní použiť aj niektoré ustanovenia *Zákona o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu*[137] či *Zákona o registri partnerov verejného sektora*.[138] Zamestnanci verejných inštitúcií alebo súkromných spoločností s viac ako 50 zamestnancami, ktorí by upozornili na niektoré praktiky spájané so strategickou korupciou u svojho zamestnávateľa, by mohli byť pred neoprávnenými postihmi v pracovnoprávnych vzťahoch chránení aj podľa *Zákona o niektorých opatreniach súvisiacich s oznamovaním protispoločenskej činnosti.*[139]

128 Európska komisia, Európsky program v oblasti bezpečnosti, 2015, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf
129 Európska komisia, Globálna stratégia pre zahraničnú a bezpečnostnú politiku Európskej únie, 2016, https://www.mzv.sk/documents/10182/2463130/160823_OBEP_Globalna_strategia_E%C3%9A.pdf/f47f31dc-af40-4f5b-a1a7-39c252e7eba1
130 Európska komisia, Akčný plán v oblasti európskej obrany, 2016, http://ec.europa.eu/DocsRoom/documents/20372
131 Európska komisia, Stratégia kybernetickej bezpečnosti Európskej únie, 2013, https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:52013JC0001&from=SK
132 Európska komisia, Rámec proti praniu špinavých peňazí a financovaniu terorizmu, 2015, https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/anti-money-laundering-and-counter-terrorist-financing_en
133 Európska komisia, Európska stratégia energetickej bezpečnosti, 2014, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com(2014)0330_/com_com(2014)0330_sk.pdf
134 Európska komisia, Stratégia námornej bezpečnosti EÚ, 2014, http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011205%202014%20INIT
135 Európska komisia, Spoločný rámec pre boj proti hybridným hrozbám, 2016, http://ec.europa.eu/DocsRoom/documents/16201
136 Národná rada SR, Trestný zákon, 2005, https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2005/300/20180701
137 Národná rada SR, Zákon o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu, 2008, https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2008/297/20180315
138 Národná rada SR, Zákon o registri partnerov verejného sektora, 2016, https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2016/315/20170801
139 Národná rada SR, Zákon o niektorých opatreniach súvisiacich s oznamovaním protispoločenskej činnosti, 2014, https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2014/307/20160701

3.6 OVPLYVŇOVANIE VOLEBNÝCH PROCESOV

Daniel Milo

ÚVOD

„Chcem, aby v máji mohli Európania prijať politické rozhodnutia v spravodlivých, bezpečných a transparentných európskych voľbách. Riziko zasahovania a manipulácie je v súčasnom online svete väčšie ako kedykoľvek predtým. Je najvyšší čas, aby naše volebné pravidlá držali krok s digitálnym vekom a chránili tak európsku demokraciu.“

Jean-Claude Juncker, 12. september 2018[140]

Slobodné, priame a férové voľby sú základným stavebným kameňom demokratického právneho štátu. Volebný proces je vo svojej podstate delegovaním vôle ľudu na ním zvolených zástupcov, ktorí v jeho mene vykonávajú správu vecí verejných. Ak do tohto procesu vstupujú vonkajší aktéri, snažiaci sa rôznymi spôsobmi ovplyvniť ich výsledok, predstavuje to podkopanie základných princípov, na ktorých stojí legitimita zvolených zástupcov občanov.

Ovplyvňovanie volebných procesov je však neoddeliteľnou súčasťou hybridných hrozieb. Minimálne od roku 2016 vychádzajú najavo mnohé podrobnosti o týchto aktivitách, napríklad zo strany Ruskej federácie v prezidentských voľbách v USA,[141] prezidentských voľbách vo Francúzsku v roku 2017,[142] o podpore politických strán v Nemecku[143] alebo o vplyve na prezidentské voľby v ČR.[144] Takéto snahy majú väčšinou podobu kombinácie informačného pôsobenia, kybernetických útokov a následného zverejnenia ukradnutých informácií, skrytého financovania politických kampaní alebo celých politických strán a vyvíjania politického či ekonomického tlaku s cieľom ovplyvniť výsledok volieb želaným smerom.

Prehľad relevantnej legislatívy a jej stručná analýza

Z hľadiska slovenskej legislatívy upravujúcej volebný proces v kontexte ovplyvňovania volebných procesov a financovania sú najvýznamnejšie dva právne predpisy: *Zákon o podmienkach výkonu volebného práva*[145] a *Zákon o volebnej kampani.*[146] Financovanie politických strán a hnutí mimo predvolebnej kampane je upravené v *Zákone č. 85/2005 o politických stranách a politických hnutiach.*[147]

Zákon o podmienkach výkonu volebného práva upravuje v § 13 postavenie Štátnej komisie pre voľby a kontrolu financovania politických strán, ktorá je najdôležitejším orgánom vykonávajúcim kontrolu financovania politických strán a politických kampaní.

140 Európska komisia, Stav Únie 2018, https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-factsheet-free-fair-elections_sk.pdf
141 Viď napríklad https://euvsdisinfo.eu/russian-election-meddling-in-the-us-and-beyond/
142 Greenberg, A., THE NSA CONFIRMS IT: RUSSIA HACKED FRENCH ELECTION ‘INFRASTRUCTURE’, The Wired, 2017, https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/
143 Hauteville, J.-M., Russia trip exposes AfD ties to Moscow, Handelsblatt, 2018, https://global.handelsblatt.com/politics/russia-funded-trip-afd-ties-moscow-929887
144 The role of the Kremlin’s influence and disinformation in the Czech presidential elections, Evropské Hodnoty, 2018 https://www.europeanvalues.net/wp-content/uploads/2018/02/The-role-of-the-Kremlin%E2%80%99s-influence-and-disinformation-in-the-Czech-presidential-elections.pdf
145 Zákon č. 180/2014 Z. z. o podmienkach výkonu volebného práva a o zmene a doplnení niektorých zákonov, http://www.zakonypreludi.sk/zz/2014-180
146 Zákon č. 181/2014 Z. z. o volebnej kampani a o zmene a doplnení zákona č. 85/2005 Z. z. o politických stranách a politických hnutiach v znení neskorších predpisov, http://www.zakonypreludi.sk/zz/2014-181
147 Zákon č. 85/2005 Z. z. o politických stranách a politických hnutiach, http://www.zakonypreludi.sk/zz/2005-85

Keďže skryté financovanie politických strán a volebných kampaní je najčastejším spôsobom ovplyvňovania volebných procesov, v tomto zmysle je najdôležitejším predpisom *Zákon o volebnej kampani*. Ten upravuje nasledovné podmienky vedenia a financovania volebných kampaní:

- Stanovuje presné finančné limity vynaložené na kampaň v rôznych typoch volieb (do NR SR a EP, prezidentské voľby, voľby do VÚC a samospráv).

- Zakladá povinnosť pre politické strany, koalície a kandidátov viesť transparentný účet a podmienku úhrady všetkých nákladov spojených s volebnou kampaňou iba z tohoto účtu.

- Určuje, kto môže viesť volebnú kampaň (§ 2 politické strany a hnutia, ich koalície, kandidáti, tretie strany registrované Štátnou komisiou) a zakazuje aktivity ostatných subjektov v prospech alebo v neprospech politických strán, koalícií a kandidátov počas volebnej kampane.

- Pri voľbách prezidenta SR stanovuje pozitívne i negatívne kritériá na subjekty, ktoré môžu a naopak nesmú financovať predvolebnú kampaň alebo poskytovať nefinančnú podporu. Dôležitým obmedzením je možnosť financovania kampane v prezidentských voľbách len pre fyzické a právnické osoby s trvalým pobytom alebo sídlom v SR, čo vylučuje priame financovanie zo strany zahraničných subjektov. Takéto obmedzenie absentuje v prípade volieb do NR SR a EP.[148]

Z hľadiska obmedzenia zasahovania do volebného procesu zo zahraničia je dôležité aj vymedzenie, kto môže byť treťou osobou, ktorá môže vykonávať volebnú kampaň. V zmysle ustanovenia § 8 ods. 2 *Zákona o volebnej kampani* takouto treťou osobou nemôže byť fyzická osoba, ktorá nemá trvalý pobyt na území Slovenskej republiky, ani právnická osoba, ktorá má sídlo v zahraničí.

Financovanie nákladov politických strán mimo obdobia volebných kampaní je podrobne upravené v zákone o politických stranách a hnutiach. Najdôležitejšími zásadami financovania v kontexte tejto správy je zákaz prijímania darov a nefinančných plnení od rôznych druhov mimovládnych neziskových subjektov, ako aj fyzických a právnických osôb s trvalým pobytom alebo sídlom mimo územia SR (§ 24 zákona).

Ďalšie významné obmedzenie sa vzťahuje na formu prijatého finančného daru - strana môže prijať peňažný dar, len ak bol poukázaný formou bezhotovostnej platobnej operácie. Ak z výpisu z účtu nie je možné určiť, kto je darcom peňažného daru, strana je povinná tento peňažný dar vrátiť (§ 24 ods.2).

EÚ

V súvislosti s nadchádzajúcimi voľbami do Európskeho parlamentu v máji 2019 prijala Európska komisia celý rad opatrení a odporúčaní smerujúcich k posilneniu ich ochrany pred protiprávnym zasahovaním a ovplyvňovaním. Ich súhrn je obsiahnutý v *Oznámení Komisie Európskemu parlamentu, Rade, EHSV a Výboru regiónov: Zabezpečenie slobodných a spravodlivých európskych volieb.*[149] V tomto oznámení sa konštatuje: *„Voľby do Európskeho parlamentu v máji 2019 sa budú konať vo veľmi odlišnej situácii než ktorékoľvek voľby predtým... Naše demokracie sú čoraz viac ohrozené politicky motivovanými masovými dezinformačnými kampaňami na internete, ktoré napomáhajú aj tretie krajiny, s osobitným cieľom zdiskreditovať a narušiť legitimitu volieb. Európska únia by mala prijať všetky opatrenia vo svojej právomoci na obranu svojich demokratických procesov pred manipuláciou zo strany tretích krajín alebo súkromných záujmov. Ukázalo sa, že obdobie volieb je obzvlášť náchylné na cielené dezinformácie. Tieto útoky majú nepriaznivý vplyv na etický a spravodlivý priebeh volieb aj na dôveru občanov voči voleným zástupcom a spochybňujú demokraciu ako takú.“*

148 Zákon č. 181/2014 Z. z. o volebnej kampani a o zmene a doplnení zákona č. 85/2005 Z. z. o politických stranách a politických hnutiach v znení neskorších predpisov, http://www.zakonypreludi.sk/zz/2014-181

149 Európska komisia, Zabezpečenie slobodných a spravodlivých európskych volieb, 2018, https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:52018DC0637&from=EN

Oznámenie v reakcii na tieto hrozby popisuje existujúce mechanizmy na úrovni EÚ na ochranu slobodných a spravodlivých volieb, navrhuje opatrenia na zvýšenie odolnosti demokracie, zdôrazňuje význam ochrany údajov vo volebnom procese a sprísňuje pravidlá na financovanie európskych politických strán. Obsah jednotlivých opatrení je nasledovný:

EK odporúča členským štátom vytvoriť sieť pre volebnú spoluprácu, online transparentnosť, ochranu pred kybernetickými incidentami a boj proti dezinformačným kampaniam.[150] Národné siete pre volebnú spoluprácu by mali pozostávať z relevantných inštitúcií (ako sú inštitúcie s kompetenciami v oblasti volieb, kybernetickej bezpečnosti a presadzovania práva). Členské štáty by mali vytvoriť národný kontaktný bod pre voľby, ktorý sa zapojí a bude sprostredkúvať výmenu informácií na európskej úrovni. Takýto mechanizmus umožní štátnym inštitúciám rýchlo odhaliť potenciálne hrozby, vymieňať si informácie a zabezpečí rýchlu a koordinovanú odpoveď.

Komisia taktiež odporúča väčšiu transparentnosť v oblasti online politickej reklamy a cielenej komunikácie. Európske a národné politické strany, nadácie a volebné organizácie by mali zverejniť informácie o ich výdavkoch na online politické kampane, informácie o tom, ktorá strana alebo politicky aktívna skupina je za online politickými reklamami, ako aj informácie o kritériách, ktoré využili na zacielenie danej kampane na občanov. V prípade, ak tieto princípy nebudú aplikované, členské štáty by mali použiť sankcie na národnej úrovni.

Ďalším opatrením na úrovni EÚ je návrh na zmenu pravidiel o financovaní európskych politických strán. Zmena nariadenia z roku 2014 o financovaní politických strán[151] umožní ukladať finančné sankcie za porušenie pravidiel o ochrane osobných údajov s úmyslom cielene ovplyvniť výsledok Európskych volieb. Sankcie budú vo výške 5% z ročného rozpočtu dotknutej európskej politickej strany alebo nadácie. Sankcie budú ukladané úradom pre európske politické strany a európske politické nadácie. Navyše, tie subjekty, ktorých sa budú sankcie týkať, sa nebudú môcť uchádzať o financovanie z rozpočtu EÚ za rok, v ktorom bola sankcia uložená.

150 Európska komisia, Odporúčanie Komisie o posilnení európskeho charakteru a účinného priebehu volieb do Európskeho parlamentu v roku 2019, 2018, https://ec.europa.eu/commission/sites/beta-political/files/recommendation-enhancing-european-nature-efficient-conduct-2019-elections_en.pdf
151 Nariadenie Európskeho Parlamentu a Rady (EÚ, Euratom) č. 1141/2014 z 22. októbra 2014 o štatúte a financovaní európskych politických strán a európskych politických nadácií http://www.epgencms.europarl.europa.eu/cmsdata/upload/9ea74795-cff1-441c-b163-739688998288/REG-1141-2014-SK.pdf

4. MEDZERY A ZRANITEĽNOSTI SLOVENSKEJ REPUBLIKY VOČI HYBRIDNÝM HROZBÁM

STRATEGICKÁ KOMUNIKÁCIA

Slovensko je krajina s nedostatočnými kapacitami na úrovni orgánov štátnej správy a nedostatočnou legislatívou, ktoré by sa strategickou komunikáciou zaoberali. Verejnosť, ako aj zástupcovia štátnej správy, majú nedostatočné povedomie o tejto problematike a preto je Slovensko zraniteľné voči dezinformačným a podvratným aktivitám zo strany ako zahraničných, tak domácich aktérov.

KYBERNETICKÁ BEZPEČNOSŤ

Analytika

Strategické dokumenty sú vo veľkej miere vypracovávané priamo výkonnými útvarmi, čo nie je v súlade s dobrou praxou. Kvalitná analýza je podstatná pre čo najkvalitnejšiu identifikáciu problému a z toho vychádzajúcich opatrení. V súčasnosti absentuje na Slovensku kvalitný analytický útvar, ktorý by produkoval kvalifikované analýzy v oblasti informačnej ochrany.

Merateľný akčný plán

Materiály, ktoré boli v súčasnosti vyprodukované, sa zaoberajú len riešením kompetencií, ako je zadefinovanie ústredného orgánu alebo získanie rozpočtu. Platný *Akčný plán* pre toto obdobie obsahuje iba vágne definované a často nemerateľné úlohy. Slovensku chýba kvalitný komplexný plán s víziou a merateľnými kritériami. Absencia takéhoto plánu so sebou prináša veľa negatív v podobe nejasných merateľných kritérií a tým aj neistotu, či sa skutočne pracuje na zraniteľnostiach alebo len na tých oblastiach, ktoré práve útvarom štátnej správy vyhovujú z iných dôvodov. Následkom je veľa nepokrytých oblastí, ktoré budú predstavovať zraniteľné miesta pre útoky.

Transparentnosť

Transparentnosť má nepochybné pozitívne účinky na kvalitu služieb štátnej správy. Utajenosť bezpečnostných procesov má však v mnohých prípadoch, špeciálne na operačnej úrovni, prirodzený dôvod. Je preto podstatné nájsť rovnováhu medzi utajením nevyhnutného a transparentnosťou. Tvorba útvarov venujúcim sa informačnej bezpečnosti na strane štátu je od začiatku vedená uzavretým spôsobom, ktorý nemá vždy jasné odôvodnenie, a výsledok neprimeraného utajovania a uzatvárania tak môže byť kontraproduktívny. Nezdravá netransparentnosť znemožňuje možnosti spolupráce, zvyšuje riziko korupcie a neefektívneho využívania verejných zdrojov. Následným znížením kvality ochrany robí krajinu zraniteľnejšou voči hybridným hrozbám.

Ľudské zdroje

Štátna správa má dlhodobo problém systematicky riešiť zamestnávanie a udržanie kvalitných pracovníkov. To obzvlášť platí pre atraktívnu oblasť IT, kde štát ťažko konkuruje súkromnému sektoru. Dôvodov, prečo k tomuto stavu dochádza, je viac. Okrem finančného ohodnotenia to je často nejasný kariérny rast a všeobecne málo motivujúce a kreatívne prostredie verejného sektora. V niektorých prípadoch sa snažia túto situáciu riešiť výnimkami, na základe čoho sa podarilo vytvoriť niekoľko kvalitných tímov. Tie sú však kapacitne malé a venujú sa úzkej oblasti a pôsobnosti v rámci štátnej správy. Pre absenciu systematického riešenia sa štátna správa naďalej potýka s kritickým nedostatkom kvalitných ľudských zdrojov v oblasti informačnej bezpečnosti. Tým sa stáva úloha plošného implementovania kvalitnej ochrany informačného prostredia ťažko splniteľnou.

Kooperácia so súkromným sektorom

Aj napriek deklarovanej strategickej spolupráci v *Akčnom pláne*[152] so súkromným sektorom táto spolupráca nie je ani inštitucionalizovaná, ani systematická. Pre tento účel napríklad vznikla na základe *Akčného plánu* z roku 2015 Komisia pre kybernetickú bezpečnosť. Komisia bez badateľných výsledkov fungovala do roku 2016, kedy sa o nej dajú nájsť posledné zmienky. Iná spolupráca má skôr živelný charakter bez zadefinovania cieľov a zodpovedností pre štátne útvary. Siete a kritickosť súkromného sektora majú signifikantný dopad na každodenný život občanov SR. Taktiež súkromný sektor disponuje značným rozpočtom aj ľudskými zdrojmi, ktoré sa venujú informačnej bezpečnosti. Spolupráca medzi súkromným sektorom je preto nevyhnutná a jej absencia predstavuje značne nevyužitý potenciál.

Systematické vzdelávanie

Informovaní užívatelia predstavujú jeden zo základných pilierov bezpečnosti, preto si ich vzdelávanie vyžaduje pozornosť. Vzdelávanie bolo definované ako jeden zo základných cieľov stratégie koncepcie pre aktuálne obdobie, ktoré bolo prenesené do konkrétnych úloh *Akčného plánu*. V bode 4 je možné dohľadať iba zmapovanie súčasného stavu.[153] Uvedené zmapovanie vzdelávania v oblasti kybernetickej bezpečnosti obsahuje v kapitole 7 návrhy opatrení ako napr. zriadenie pracovnej skupiny či implementovanie návrhu systému vzdelávania v oblasti kybernetickej bezpečnosti. Odpočet plnenia týchto úloh ani ďalších úloh z kapitoly 4 *Akčného plánu* žiaľ nebolo možné dohľadať.

Slabo informovaní a nevzdelaní užívatelia na všetkých úrovniach predstavujú zvýšene riziko pre úspešný útok. Preto by malo vzdelávanie predstavovať jeden z hlavných pilierov pre zlepšovanie obrany v tak širokej a dôležitej oblasti.

Inovačné prostredie

Ako *Koncepcia kybernetickej bezpečnosti v Slovenskej republike*, tak jej *Akčný plán* udávajú ako jednu z priorít podporu inovačného prostredia v oblasti kybernetickej bezpečnosti. Pretavenie do konkrétnych úloh, ktoré by viedli k systematickej a koncepčnej podpore výskumu a vývoja obranných informačných technológii, už absentuje. Nevyužitie inovačného potenciálu znižuje možnosti uplatnenia kvalitnej ochrany krajiny pred kybernetickými útokmi.

ENERGETICKÁ BEZPEČNOSŤ

Čo sa týka hybridných hrozieb, v rámci diskusií o energetickej politike sa im venuje iba minimum priestoru. Energetická infraštruktúra je súčasťou širšej diskusie o ohrozeniach kritickej infraštruktúry. Takýto prístup však neberie do úvahy rôznorodosť hrozieb, ktoré sa môžu týkať energetickej infraštruktúry, a ktoré môžu mať dopad nielen na energetickú bezpečnosť (v zmysle prerušenia dodávok energetických zdrojov a nenaplnenia potrieb koncových užívateľov), ale aj na oblasť „hard security" (pri kybernetických útokoch na elektrárne, predovšetkým tie jadrové). Vzhľadom na dôležitosť jadrovej energetiky, ako aj prepravnej infraštruktúry (najmä tej plynovodnej) SR, by mali témy spojené s hybridnými ohrozeniami získať dominantnejšie miesto v rámci bezpečnostného diskurzu. Diverzifikácia je síce považovaná za vhodný spôsob reakcie na hrozby v oblasti energetickej bezpečnosti (diverzifikáciou dodávateľov, zdrojov a trás dodávok energetických surovín sa zníži závislosť na konkrétnom dodávateľovi), avšak nie je odpoveďou na ďalšie následky hybridných, resp. kybernetických, útokov na energetickú infraštruktúru (tých, ktoré spadajú do kategórie „hard security", ako napríklad ohrozenie jadrových elektrární, ale aj veľkých vodných zdrojov).

152 „Súkromný a akademický sektor, ako aj občianska spoločnosť sa aktívne zúčastňujú na formovaní a realizácii politiky Slovenskej republiky v oblasti kybernetickej bezpečnosti." Bod 2.4 Koncepcie kybernetickej bezpečnosti v Slovenskej republike.
153 http://www.informatizacia.sk/ext_dok-narodny_system_vzdelavania_ib/9008c

PARAMILITÁRNE A EXTRÉMISTICKÉ SKUPINY

Najvýznamnejšími medzerami v súčasnej právnej úprave a verejných politikách týkajúcich sa polovojenských a extrémistických skupín je absencia právnej úpravy a pôsobenia polovojenských skupín. Takéto vymedzenie je potrebné na stanovenie jasnej hranice konania a aktivít polovojenských skupín, ktoré sú schopné ohroziť/narušiť bezpečnosť a stabilitu spoločnosti a ich odlíšenia od činnosti záujmových skupín bez ideologického zamerania.

Druhou kategóriou je oblasť prístupu k vojenským znalostiam, zručnostiam, ako i samotným zbraniam. V tomto kontexte sa jedná najmä o využívanie znalostí a zručností príslušníkmi ozbrojených síl pri výcviku polovojenských skupín a nadobúdanie zbrojných preukazov osobami z radov extrémistických a polovojenských skupín. Existujúca právna úprava pôsobenia streleckých klubov a využívania ostrých automatických zbraní takýmito klubmi tiež vytvára potenciál na ich zneužitie.

V neposlednom rade absentuje úprava konceptu cudzej moci a cudzích činiteľov v súvislosti s aktivitami extrémistických a polovojenských skupín ako priťažujúcej okolnosti pri posudzovaní trestnosti ich aktivít.

STRATEGICKÁ KORUPCIA

Je možné konštatovať, že Slovensko patrí ku krajinám ohrozených praktikami strategickej korupcie, no zároveň má verejnosť mizivé povedomie o týchto rizikách a špecifickú pozornosť im nevenuje ani naša legislatíva a verejné politiky.

OVPLYVŇOVANIE VOLEBNÝCH PROCESOV

Existujúca právna úprava pokrýva len obdobie volebnej kampane odo dňa jej vyhlásenia, ktoré sa začína dňom vyhlásenia volieb v *Zbierke zákonov*. Záverečná správa predkladaná politickými stranami a kandidátmi síce musí obsahovať aj prehľad výdavkov za obdobie 180 dní pred vyhlásením volebnej kampane, nevyžaduje však využívanie transparentného účtu. Súčasné znenie legislatívy súvisiacej s financovaním politických strán a kampaní neobsahuje ustanovenia umožňujúce identifikovať skutočných darcov-prispievateľov podobným spôsobom, ako sú upravené tzv. schránkové firmy – t.j. uvedením konečného užívateľa výhod. Podľa súčasného znenia je možné pomerne jednoducho zamedziť transparentnému financovaniu volebných kampaní využitím nastrčených subjektov, ktoré vystupujú ako darcovia, pričom skutočný majiteľ prostriedkov ostáva skrytý.

Na rozdiel od pomerne prísnych pravidiel pre subjekty, ktoré môžu financovať predvolebnú kampaň v prípade prezidentských volieb a volieb do orgánov samospráv, financovanie volieb do NR SR a EP je upravené oveľa voľnejšie a neobsahuje rovnaký typ obmedzení.

Za nedostatok možno tiež považovať pomerne úzke vymedzenie aktivít, ktoré spadajú do rámca predvolebnej kampane (akákoľvek činnosť politických strán, koalícií, kandidátov a tretích strán..., za ktorú sa obvykle platí úhrada, smerujúca k propagácii ich činnosti, cieľov a programu za účelom získania funkcie volenej podľa osobitného predpisu).

Vedenie predvolebnej kampane v prostredí internetu nie je osobitne upravené a spadá pod všeobecnú úpravu napriek zásadnému vplyvu na voličov. Platná právna úprava takisto nepokrýva informovanie voličov o témach, ktoré ovplyvňujú ich volebné preferencie zo strany subjektov organizačne, finančne alebo personálne napojených na politické strany, koalície a kandidátov. Takéto komunikačné taktiky ovplyvňujúce voličské správanie cez cielené informovanie (tzv. „micro targeting“ na sociálnych sieťach) o kontroverzných a emočne nabitých témach s cieľom dosiahnuť zmenu voličského správania, boli viditeľné vo viacerých krajinách sveta počas predvolebnej kampane. Takéto koordinované a cieľavedomé informovanie, nazývané aj informačné operácie, prebieha zvyčajne oveľa dlhšie obdobie ako je samotná volebná kampaň, a v súčasnosti nepodlieha žiadnej regulácii.

5. ODPORÚČANIA PRE TVORBU VEREJNÝCH POLITÍK

STRATEGICKÁ KOMUNIKÁCIA

- Prijať komplexný prístup v boji proti informačnej vojne zahŕňajúci všetky relevantné zložky štátnej a verejnej správy.
- Zriadiť špecializované národné kapacity so zameraním na strategickú komunikáciu, monitorovanie hybridných hrozieb a aktívne informovanie zložiek na štátnej a lokálnej úrovni.

KYBERNETICKÁ BEZPEČNOSŤ

- Zriadiť kvalitné analytické oddelenie, ktoré by sa zaoberalo tvorbou plánov a politík.
- Prijať akčný plán s merateľnými kritériami, ktorý by systematizoval aj vzdelávanie a inovačné prostredie.

ENERGETICKÁ BEZPEČNOSŤ

- Systematicky riešiť otázku hybridných/kybernetických hrozieb v strategických dokumentoch, ktoré sa venujú energetickej politike, resp. energetickej bezpečnosti.
- Klásť väčší dôraz na špecifiká energetického sektora, ktorý je odlišný od iných oblastí kritickej infraštruktúry, pretože hybridné hrozby v tejto oblasti majú dôsledky nielen pre energetickú bezpečnosť, ale aj pre „hard security".
- Identifikovať hybridné hrozby a riešenia nielen na úrovni verejnej/štátnej správy, ale aj v rámci (polo)súkromného energetického sektora, ktorý hrá dôležitú úlohu pri zabezpečovaní energetickej bezpečnosti.
- Zahrnúť „smart" technológie do diskusie o možných hybridných hrozbách v oblasti energetickej bezpečnosti.

PARAMILITÁRNE A EXTRÉMISTICKÉ SKUPINY

- Novelizovať legislatívu v oblasti zbraní a streliva (nadobúdanie zbraní, automatické zbrane, bezpečnostné previerky, strelecké kluby...).
- Prijať legislatívu upravujúcu pôsobenie polovojenských skupín.
- Novelizovať legislatívu a upraviť podporu extrémistických skupín a skupín predstavujúcich bezpečnostné riziko zo strany cudzej moci.
- Vytvoriť ľahko dostupné, nízkoprahové alternatívy pre mládež so záujmom o vojenstvo a históriu, pod dozorom štátu a so zapojením OS SR.
- Dôsledne uplatňovať ustanovenia TZ týkajúce sa účasti na bojovej činnosti organizovanej ozbrojenej skupiny na území iného štátu a jej podpory.

STRATEGICKÁ KORUPCIA

- Zmapovať riziká spojené so strategickou korupciou v podmienkach Slovenskej republiky a navrhnúť vhodné opatrenia na predchádzanie takýmto rizikám strategickej korupcie v spolupráci s odbornou verejnosťou i medzinárodnými partnermi.
- Implementovať vyššie spomenuté opatrenia do koncepčných materiálov venovaných hybridným hrozbám a po zrelej úvahe ich prípadne zohľadniť aj v legislatíve.
- Zintenzívniť spoluprácu s relevantnými inštitúciami EÚ a NATO, podporovať investigatívnu žurnalistiku, ako aj posilňovanie nezávislosti a odborných kapacít domácich inštitúcií a kontrolných a bezpečnostných orgánov. Ďalej posilňovať ďalej medzinárodné, ale aj domáce nástroje na odhaľovanie podozrivých finančných tokov cez schránkové firmy a daňové raje. Tie zatiaľ účinnú verejnú kontrolu garantovať nedokážu.[154]
- Zlepšiť komunikáciu spomínaných rizík smerom (nielen) k laickej verejnosti.

OVPLYVŇOVANIE VOLEBNÝCH PROCESOV

- Prijať legislatívu, ktorá upraví transparentné financovanie politických strán počas celého volebného obdobia, nielen v čase trvania predvolebnej kampane.
- Upraviť okruh subjektov oprávnených financovať volebné kampane počas volieb do NR SR a EP podobným spôsobom, ako je to v prípade prezidentských volieb.
- Zaviesť povinnosť informovania o zadávateľovi online politických reklám aj v čase mimo predvolebnej kampane.

154 Šípoš, G., A Veľkú schránkovú cenu Slovenska vyhráva..., Transparency International Slovensko, 2018, https://transparency.blog.sme.sk/c/490050/a-velku-schrankovu-cenu-slovenska-vyhrava.html