Operačný program
Efektívna
verejná správa

Európska únia
Európsky sociálny fond

BOJ PROTI HYBRIDNÝM HROZBÁM V KRAJINÁCH EÚ: PRÍKLADY DOBREJ PRAXE

GLOBSEC
IDEAS SHAPING THE WORLD

BOJ PROTI HYBRIDNÝM HROZBÁM V KRAJINÁCH EÚ: PRÍKLADY DOBREJ PRAXE

GLOBSEC je nezávislá mimovládna organizácia aktívna v oblasti domácej, medzinárodnej a európskej politiky a bezpečnosti viac ako 20 rokov. Vďaka medzinárodnému tímu, projektom a 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.

AUTORI

Katarína Klingová, analytička, GLOBSEC

Daniel Milo, vedúci programu Strategickej komunikácie, GLOBSEC

GLOBSEC, Bratislava, november 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

Pri nastavovaní štruktúr, legislatívy a opatrení znižujúcich mieru zraniteľnosti Slovenskej republiky voči hybridným hrozbám je vhodné inšpirovať sa príkladmi z iných krajín, ktoré v danej oblasti takéto opatrenia realizovali, a môžu tak slúžiť ako zdroj inšpirácie.

Za týmto účelom analytici GLOBSEC-u spolu so zástupcami vybraných ústredných orgánov štátnej správy realizovali na jeseň 2018 pracovné cesty do krajín, ktoré sú považované za lídrov v prístupe k hybridným hrozbám, a doplnili ich vlastným sekundárnym výskumom.

Táto publikácia ponúka prehľad niektorých inšpiratívnych príkladov z nasledujúcich oblastí:

1. Nastavenie štruktúr bezpečnostného systému
2. Koncepčný prístup k hybridným hrozbám
3. Budovanie kapacít a výmena skúseností
4. Ochrana integrity volieb
5. Zapájanie dobrovoľníkov do obrany proti kybernetickým a informačným hrozbám
6. Využitie dobrovoľníkov a domobrany pri obrane územia

PRÍKLADY DOBREJ PRAXE

- Právna úprava oblasti hybridných hrozieb a štruktúr štátnej správy vo Fínsku
- Definície hybridných hrozieb vo Fínsku
- Celovládny a celospoločenský (whole-of-government / whole-of-society) prístup vo Fínsku
- Psychologická obrana vo Švédsku
- Audit národnej bezpečnosti v Česku

- Nové vojenské štruktúry vybavené čeliť novým bezpečnostných hrozbám v Spojenom kráľovstve
- Informovanie o hybridných útokoch v Holandsku
- Členstvá v centrách excelentnosti Európskej únie a NATO
- Pracovná skupina na ochranu volieb v Katalánsku či Estónsku
- Elfovia bojujúci proti trollom v Pobaltských krajinách
- Estónska obranná liga - jednotka kybernetickej obrany
- Budovanie povedomia o kolektívnej obrane v Poľsku
- Vojská teritoriálnej obrany v Poľsku
- Dobrovoľné vojenské cvičenia pre študentov v Poľsku
- Praktické príručky ako realizovať civilný odboj v prípade napadnutia v Litve

1. PRÁVNA ÚPRAVA OBLASTI HYBRIDNÝCH HROZIEB A ŠTRUKTÚR ŠTÁTNEJ SPRÁVY

Jedným zo základných predpokladov na zvládanie hybridných hrozieb je vytvorenie efektívneho mechanizmu na zdieľanie informácií a ich analýzy pre potreby vrcholných predstaviteľov štátu. Fínsko ako krajina, ktorá je v poslednej dobe vystavená rôznym druhom hybridných hrozieb, preto pristúpilo k prijatiu právnej úpravy, ktorá uľahčila tok informácií a ich zdieľanie medzi jednotlivými zložkami štátnej správy, bezpečnostného systému a ich spracovanie v situačnom centre fínskej vlády (Government Situation Centre). Zákon číslo 300/2017 definoval funkciu, povinnosti a práva vládneho situačného centra (GOVSITCEN) nasledovne:

> ***1 § Funkcie GOVSITCENu:*** *„GOVSITCEN je analytické centrum, ktoré zhromažďuje a analyzuje informácie o možných bezpečnostných hrozbách, ktoré môžu ohroziť životne dôležité funkcie spoločnosti. Ďalej riadi a koordinuje medzirezortnú výmenu informácií, analýz a prognóz. GOVSITCEN taktiež zdieľa informácie o uvedených témach prezidentovi, vláde a ďalším príslušným orgánom. Centrum pôsobí pod vedením Kancelárie predsedu vlády.*
>
> ***2 § Povinnosť informovať GOVSITCEN o incidentoch súvisiacich s bezpečnosťou:*** *GOVSITCEN musí byť informovaný o katastrofách (prírodného alebo ľudského pôvodu) a o iných incidentoch súvisiacich s bezpečnosťou. Tieto informácie môžu byť, no nie sú obmedzené na: rozsiahle poruchy infraštruktúry, terorizmus, kybernetické hrozby atď. Povinnosť informovať GOVSITCEN o takýchto hrozbách majú všetky relevantné ministerstvá a príslušné úrady ako sú Národný úrad vyšetrovania, Bezpečnostná polícia, Centrum pre kybernetickú bezpečnosť, vojenské zložky a podobne. Je na daných orgánoch, ako si splnia túto povinnosť.*
>
> ***3 § Právo prijať informácie:*** *GOVSITCEN má právo prijímať informácie rôzneho druhu a bez ohľadu na bezpečnostnú klasifikáciu, ako sú napríklad informácie o okolnostiach, mieste, čase, dopade, štruktúre velenia, kto nesie zodpovednosť za daný čin a podobne. Cieľom je získať čo najlepšie informácie a hodnotenia, ktoré môžu byť použité pri rozhodovaní vlády. Existujú však aj výnimky, ktoré nemôžu byť dodané GOVCITCENu, a to sú: akademické a štatistické informácie, osobné informácie, medzinárodné spravodajské príspevky (ak tieto informácie vyžaduje zahraničný partner neposúvať ďalej) a metadáta.*

> ***4 § Právo zdieľať informácie a analýzy:*** *Bez ohľadu na bezpečnostnú klasifikáciu, a ak sa informácie považujú za nevyhnutné na podporu rozhodovania, GOVSITCEN má právo odovzdať príslušné informácie a správy prezidentovi, členom vlády a ďalším príslušným orgánom. Cieľom zdieľania týchto informácií je podporiť rozhodovanie v oblasti bezpečnosti a zvýšiť možnosť čeliť okamžitým hrozbám.“*[1]

Prijatie tejto právnej úpravy uľahčilo fínskemu GOVSITCEN-u spoluprácu s ostatnými zložkami bezpečnostného systému a krízového riadenia a vyjasnilo vzťahy v procesoch národného krízového manažmentu. Podobný zákon by mohol byť inšpiratívny aj pre slovenské štátne orgány. V podmienkach SR má podobné postavenie Národné bezpečnostné analytické centrum, ktoré však nepodlieha priamo vláde, ako tomu je v prípade fínskeho modelu, ale je definované ako „analytické, komunikačné a kooperačné pracovisko SIS s celoštátnou pôsobnosťou v oblasti bezpečnostných hrozieb”.[2] Fínsky model je zaujímavý v tom, že umožňuje priamy a bezprostredný kontakt medzi zdrojmi informácií a najvyššími predstaviteľmi výkonnej moci vrátane predsedu vlády.

DEFINÍCIE, KTORÉ UMOŽŇUJÚ FLEXIBILITU

Vo Fínsku ako v národných inštitúciách, tak aj v Európskom centre pre boj proti hybridným hrozbám (Hybrid CoE) je možné pozorovať zaujímavý prístup k terminológii.

Definícia hybridných hrozieb je vo Fínsku aktuálne ponímaná veľmi všeobecne v Bezpečnostnej stratégii pre spoločnosť: Vládne uznesenie (Security strategy for society: Government resolution) z roku 2017. Fíni vo svojej Bezpečnostnej stratégii nepoužívajú termín „hybridná hrozba“, ale „hybridné ovplyvňovanie“ (hybrid influencing), ktoré definujú ako:

„čin, ktorého výsledky dosahuje podnecovateľ prostredníctvom množstva vzájomne sa doplňujúcich metód a prostredníctvom využitia zraniteľností cieľovej komunity.“[3]

---

1 Zákon o vládnom situačnom centre číslo 300/2017 v platnosti od 1. júla 2017, https://www.finlex.fi/fi/laki/alkup/2017/20170300?search%5Btype%5D=pika&search%5Bpika%5D=300%2F2017 [voľný preklad autorov]

2 Slovenská informačná služba, Národné bezpečnostné analytické centrum (NBAC), http://www.sis.gov.sk/o-nas/nbac.html

3 Bezpečnostná rada Fínskej republiky, Bezpečnostná stratégia pre spoločnosť: Vládne uznesenie, prijatá 2. novembra 2017, https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf [voľný preklad autorov]

Pri definícii hybridného ovplyvňovania je dôležitá poznámka, ktorá stanovuje, že *„hybridné ovplyvňovanie môže byť realizované s využitím a prostredníctvom ekonomických, politických alebo vojenských nástrojov. Hybridné ovplyvňovanie môže byť taktiež vykonávané s použitím technológií a sociálnych sietí. Dané metódy môžu byť použité súčasne alebo postupne. Hybridné ovplyvňovanie môže byť ťažké rozpoznať.“*[4]

Všeobecná terminológia a definícia bezpečnostnej hrozby umožňuje, že zamestnanci verejnej správy nie sú limitovaní terminologickými pojmami a ich striktnými bariérami, ale pri svojich analýzach môžu brať do úvahy kontext. Získavajú tak väčšiu flexibilitu v tom, čo považovať za hybridné ovplyvňovanie a čo nie. Štátni zamestnanci, napríklad GOVSITCEN-u, tak môžu hľadať informácie, ktoré obsahujú anomálie s hybridnými elementami, pričom sa môžu riadiť svojou intuíciou namiesto striktného kontrolného zoznamu („checklistu“) pri analýze nezrovnalostí a pri určovaní, či sa jedná alebo nejedná o hybridnú hrozbu.

Podobný prístup možno pozorovať v Hybrid CoE, ktoré chápe hybridné hrozby ako metódy a aktivity cielené na zraniteľnosti oponenta, pričom ponímanie zraniteľnosti je veľmi všeobecné – od historickej pamäti, legislatívnych nedostatkov, geopolitických faktorov až po technologické nedostatky či ideologické rozdiely. Hybrid CoE charakterizuje hybridné hrozby ako:

- koordinované a synchronizované útoky, ktoré sa cielene zameriavajú na systémové zraniteľnosti demokratických štátov a inštitúcií prostredníctvom využitia širokého spektra prostriedkov (od politických, hospodárskych či vojenských nástrojov, občianskych konfliktov a informačných operácií);

- hybridné aktivity prebiehajú na okraji detekcie, využívajú náročnosť odhaľovania aktérov zodpovedných za podvratné aktivity a pohybujú sa na tenkej hranici medzi vojnou a mierom;

- cieľom hybridných aktivít je ovplyvniť rôzne rozhodovacie procesy na miestnej, regionálnej či štátnej úrovni alebo na inštitucionálnej úrovni s cieľom podporiť a/alebo dosiahnuť strategické ciele, podkopávajúc stabilitu a/alebo využívajúc zraniteľnosť svojich objektov.[5]

4 Ibid.

5 Európske centrum excelentnosti pre boj proti hybridným hrozbám, Hybridné hrozby, https://www.hybridcoe.fi/hybrid-threats/

Hybrid CoE aplikuje hybridný prístup k tomu, ako definovať, analyzovať či reagovať na hybridné hrozby. Vychádza z predpokladu, že definície by nemali obmedzovať aktivity a zameranie Centra, a to najmä v takej oblasti, ktorá sa neustále vyvíja a môže pozostávať z množstva rôznych elementov. Tento flexibilný prístup v analyzovaní a detekcii hybridných hrozieb, aký implementuje Fínsko či Hybrid CoE, by mohol byť inšpiráciou aj pre Slovensko.

2. KONCEPČNÝ PRÍSTUP K HYBRIDNÝM HROZBÁM

CELOVLÁDNY A CELOSPOLOČENSKÝ (WHOLE-OF-GOVERNMENT / WHOLE-OF-SOCIETY) PRÍSTUP VO FÍNSKU

Fínsky prístup k riešeniu hybridných hrozieb je bezprecedentný vo svojej šírke a komplexnosti. Aj vďaka exponovanej geografickej a historickej dispozícii pristupuje Fínsko k identifikácii a neutralizácii hybridných hrozieb nezvyčajne zoširoka. Nastavenie fínskeho bezpečnostného systému je na vysokej úrovni - GOVSITCEN zabezpečuje koordinovaný prístup k monitorovaniu, vyhodnocovaniu a riešeniu hybridných hrozieb. Fínska vláda dokonca zriadila post špeciálneho veľvyslanca pre hybridné hrozby. Mandátom špeciálneho veľvyslanca je dosahovať úzku spoluprácu naprieč sektormi, vrátane neziskových organizácií a súkromného sektora pri presadzovaní vonkajších partnerstiev a politík. Vo Fínsku taktiež vytvorili medzivládnu skupinu na informačné ovplyvňovanie, ktorej súčasťou sú všetky fínske ministerstvá a inštitúcie. Cieľom tejto skupiny je zabezpečiť konsolidovaný *situation awareness*, posilňovať povedomie o informačných operáciách, vzdelávať štátnu správu a novinársku obec. Kurzami prešlo cez desať tisíc zamestnancov štátnej a verejnej správy, ako aj novinári, ktorí získali základné poznatky o hybridných a informačných aktivitách. Na vzdelávaní štátnych zamestnancov sa ako partner podieľala aj Harvardova univerzita. Fínske Ministerstvo zahraničných vecí podporuje svojich zamestnancov, aby sa v tejto téme vzdelávali a aktívne o nej komunikovali s verejnosťou. Zároveň sa však ministerstvo snaží nezveličovať dopady podvratných aktivít zahraničných aktérov. Zahraniční aktéri často len využívajú nedostatky, nepripravenosť a zraniteľnosti národných inštitúcií a občianskej spoločnosti. Preto sa Fínsko zameralo v prvom rade na budovanie odolnej spoločnosti a zaplátavanie medzier a nedostatkov vo svojich lokálnych či národných štruktúrach.

ŠVÉDSKA PSYCHOLOGICKÁ OBRANA

Podobné zmýšľanie ako vo Fínsku v prístupe voči podvratným aktivitám zahraničných aktérov možno pozorovať vo Švédsku. Začiatkom roka 2018 švédsky predseda vlády, Stefan Löfven, deklaroval zriadenie centrálneho štátneho orgánu, ktorý by sa zameriaval na budovanie psychologickej obrany švédskej spoločnosti.[6] Takýto prístup vo Švédsku nie je ničím novým. Už počas studenej vojny v 50. rokoch 20. storočia existovala vo Švédsku Národná komisia pre psychologickú obranu, predchodkyňa Národnej rady

6 The Local, Švédsko by malo vytvoriť nový orgán poverený bojom proti dezinformáciám, január 2018, https://www.thelocal.se/20180115/sweden-to-create-new-authority-tasked-with-countering-disinformation

na psychologickú obranu, ktorej aktivity boli v roku 2009 začlenené pod švédsku Civil Contingencies Agency (MSB)[7] Ministerstva obrany Švédskeho kráľovstva. MSB zodpovedá za národné situačné krízové riadenie a vedie aktivity švédskej vlády proti nepriateľskému podvratnému vplyvu.[8] Švédsky prístup je založený na princípe, že najlepšou obranou je mať odolnú a aktívnu občiansku spoločnosť, ktorá si uvedomuje hrozby a zraniteľnosti, a ktorá bude aktívne nahlasovať dezinformácie a prispievať k ich vyvracaniu. V rámci svojich aktivít pripravila MSB aj príručku pre verejnú správu ako identifikovať, analyzovať a odpovedať na snahy o informačné ovplyvňovanie - Vyvracanie aktivít informačného ovplyvňovania: Manuál pre komunikátorov.[9] Podobným celovládnym a celospoločenským prístupom k podvratným informačným aktivitám ako aj poskytovaním vzdelania a podpory pre zamestnancov verejnej správy by sa Slovensko mohlo inšpirovať.

AUDIT NÁRODNEJ BEZPEČNOSTI ČESKEJ REPUBLIKY

V roku 2016 zrealizovala Česká republika (ČR) Audit národnej bezpečnosti. Na Audite, ktorý mal preveriť obranyschopnosť a pripravenosť českého bezpečnostného systému voči tzv. tradičným aj hybridným hrozbám, sa podieľalo vyše 120 národných a medzinárodných bezpečnostných expertov. Audit analyzoval obranyschopnosť ČR v 10 oblastiach, ktoré boli vopred vyhodnotené ako najzávažnejšie hrozby pre vnútornú bezpečnosť ČR. Medzi tieto hrozby patrili podvratné aktivity zahraničných aktérov a hybridné hrozby. Zatiaľ čo Audit preukázal, že český bezpečnostný systém je dobre pripravený na tzv. tradičné hrozby, odhalil jeho nedostatky čeliť moderným hybridným hrozbám. Audit identifikoval, že schopnosti štátnych inštitúcií a bezpečnostných zložiek odhaliť a koordinovane riešiť prepojené útoky by mali byť posilnené. Na základe poznatkov z Auditu sa ČR rozhodla posilniť monitoring, medzirezortnú spoluprácu, praktické cvičenia či výmenu skúseností prostredníctvom spolupráce so zahraničnými partnermi.[10] Audit národnej bezpečnosti Českej republiky by mohol byť inšpiráciou pre Slovensko, prostredníctvom ktorého by sa odhalili reálne nedostatky a zraniteľnosti slovenských bezpečnostných zložiek a štátnych orgánov.

7 Niklas H. Rossbach, Psychologická obrana: Základ pre švédske obranné schopnosti, Švédska agentúra pre výskum obrany, november 2017, https://www.foi.se/report-search/pdf?fileName=D%3A%5CReport-Search%5CFiles%5C10bf3c21-4ba1-4c33-93c5-44fd5457b02d.pdf

8 Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee a Madeline McCue, Riešenia hybridných hrozieb, Centrum pre štúdium asymetrických hrozieb v spolupráci s Európskym centrom pre boj proti hybridným hrozbám, máj 2018, https://www.hybridcoe.fi/publications/addressing-hybrid-threats/

9 MSB, Vyvracanie aktivít informačného ovplyvňovania: Manuál pre komunikátorov, júl 2018, https://www.msb.se/RibData/Filer/pdf/28698.pdf

10 Ministerstvo vnútra Českej republiky, Audit národnej bezpečnosti, https://www.mvcr.cz/cthh/clanek/audit-narodni-bezpecnosti.aspx

3. BUDOVANIE KAPACÍT A VÝMENA SKÚSENOSTÍ

BRIGÁDA 77 SPOJENÉHO KRÁĽOVSTVA: NOVÉ VOJENSKÉ ŠTRUKTÚRY VYBAVENÉ ČELIŤ NOVÝM BEZPEČNOSTNÝCH HROZBÁM

Informačné operácie sú a vždy boli neoddeliteľnou súčasťou a podporou vojenských operácií. Vyzerá to tak, že v dnešnom svete však boj s nepriateľom prebieha primárne, niekedy až výlučne, prostredníctvom informačných operácií. Informačné operácie majú však niekoľko elementov. Po prvé, aktéri, či už domáci alebo zahraniční, bojujú o pozornosť a priazeň verejnosti. Po druhé, systematické šírenie rôznych dezinformácií podkopáva napríklad dôveryhodnosť obyvateľstva voči štátnym inštitúciám, demokratickým procesom, vojenskej intervencii či, v prípade očkovania, aj voči základnej zdravotnej starostlivosti. Preto treba na dezinformácie aktívne poukazovať a informovať o nich verejnosť. Propaganda je boj o „srdcia a myseľ“ občanov, preto je šírenie vlastných príbehov a naratívov dôležitým, tretím elementom informačných operácií. Novodobý vojenský konflikt či podvratné aktivity spájajú všetky tieto elementy a predstavujú boj na všetkých spomenutých úrovniach informačných operácií. Na túto zmenu chápania a vedenia vojenských a informačných aktivít zareagovali štáty rôznym spôsobom. V Spojenom kráľovstve vytvorili v roku 2015 špeciálnu vojenskú jednotku, 77. brigádu, ktorá sa skladá z viacerých častí britskej armády, vrátane skupiny pre mediálne operácie a skupiny pre psychologické operácie, ako aj ľudí z civilného sektora. 77. brigáda sa stala odpoveďou Spojeného kráľovstva na nový typ boja odrážajúceho dnešnú dobu. Predstavuje nový druh neortodoxnej sily v prostredí, kde je potrebné efektívne zanalyzovať a komunikovať informácie určitej skupine či skupinám obyvateľstva. Členovia brigády editujú a produkujú videá, nahrávajú podcasty, komunikujú s verejnosťou na sociálnych sieťach, majú k dispozícii grafikov a vedia zacieliť svoj obsah pomocou platenej reklamy. Inými slovami, členovia 77. brigády sú reakciou Británie na novodobé informačné operácie.[11]

Aktivity 77. brigády zahŕňajú:

- včasnú analýzu recipientov informácií, aktérov a protivníkov;
- plánovanie a integráciu informačných aktivít a ich aktívne šírenie;
- zabezpečenie informačnej podpory;
- podporu v boji proti konkurenčným naratívom/aktérom;

11 Carl Miller, Vo vnútri tajného informačného stroja britskej armády, Wired, november 2018, https://www.wired.co.uk/article/inside-the-77th-brigade-britains-information-warfare-military

- medzirezortnú spoluprácu;
- zber, tvorbu a šírenie digitálneho a širšieho mediálneho obsahu na podporu určených úloh;
- monitorovanie a hodnotenie informačného prostredia.[12]

Adaptácia bezpečnostných štruktúr na to, aby boli schopné reagovať na nové bezpečnostné hrozby, bude skôr či neskôr nevyhnutná aj v slovenských reáliách.

INFORMOVANIE O HYBRIDNÝCH ÚTOKOCH

Krajiny a ich predstavitelia by mali otvorene komunikovať o hrozbách, útokoch či snahách o podvratné aktivity štátnych a neštátnych aktérov. Poukazovať na incidenty a zdieľať informácie o útokoch a aktéroch so svojimi partnermi je dôležité pre zvyšovanie informovanosti a ostražitosti potenciálnych cieľov voči dezinformačným operáciám a iným hybridným hrozbám.[13] Jedným z dobrých príkladov informovania o podvratnej činnosti zahraničného aktéra je napríklad oznámenie Holandského kráľovstva o zmarení kybernetického útoku na Organizáciu pre zákaz chemických zbraní (OPCW) so sídlom v Haagu. 4. októbra minister obrany Holandského kráľovstva informoval o pokuse o útok na OPCW štyrmi agentmi ruskej vojenskej rozviedky GRU, pri ktorom boli prichytení 13. apríla 2018 v Haagu. Zverejnením informácií o pokuse o hackerský útok a o „hackeroch“ - agentoch GRU, chcela holandská vláda vydať jasný signál, že aktéri podobných kybernetických útokov už nebudú môcť vykonávať svoje aktivity beztrestne.[14]

ČLENSTVÁ V CENTRÁCH EXCELENTNOSTI EURÓPSKEJ ÚNIE A NATO

V rámci štruktúr NATO a EÚ existuje viacero špecializovaných centier, ktoré na báze dobrovoľnosti združujú kapacity jednotlivých členských štátov a umožňujú im prístup k najnovším poznatkom a nástrojom v danej tematickej oblasti. V súčasnosti takýchto centier existuje v NATO 24,[15] a niektoré z nich sa zaoberajú aj problematikou hybridných hrozieb.

12 Armáda Spojeného kráľovstva, 77. brigáda: Vplyv a dosah, https://www.army.mod.uk/who-we-are/formations-divisions-brigades/force-troops-command/77-brigade/

13 Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee a Madeline McCue, Riešenia hybridných hrozieb, Centrum pre štúdium asymetrických hrozieb v spolupráci s Európskym centrom pre boj proti hybridným hrozbám, máj 2018, https://www.hybridcoe.fi/publications/addressing-hybrid-threats/

14 Ministerstvo obrany Holandského kráľovstva, List o zabránení kybernetickým operáciám GRU v Haagu, október 2018, https://www.defensie.nl/binaries/defensie/documenten/kamerstukken/2018/10/04/letter-to-the-house-of-representatives-regarding-disruption-of-a-gru-cyber-operation-in-the-hague/Letter+to+the+-House+of+Representatives+regarding+Disruption+of+a+GRU+cyber+operation+in+The+Hague.pdf

15 NATO, Centrá excelentnosti, https://www.nato.int/cps/en/natolive/topics_68372.htm#

Jedným z nich je Centrum excelentnosti NATO na kooperatívnu kybernetickú obranu (NATO Cooperative Cyber Defence Centre of Excellence) v Talline, ktoré bolo akreditované v roku 2008. Slovenská republika je jeho súčasťou od samotného vzniku. Druhým podobným centrom je Centrum excelentnosti NATO na strategickú komunikáciu (NATO Stratcom Centre of Excellence[16]), ktoré vzniklo v roku 2014 v Lotyšsku. Hlavným cieľom Centra je spracovávať komplexné analýzy a poskytovať včasné poradenstvo a praktickú podporu členom Aliancie v oblasti strategickej komunikácie. Od konca roku 2017 prebieha v uvedenej inštitúcii proces schvaľovania členstva SR.[17]

Najnovším centrom excelentnosti, ktoré sa svojím charakterom trochu vymyká vyššie uvedeným, je European Centre of Excellence for Countering Hybrid Threats – Európske centrum excelentnosti pre boj proti hybridným hrozbám (Hybrid CoE). Odlišuje sa najmä tým, že jeho členmi sú členské štáty EÚ aj NATO, a aktívne spolupracuje s oboma organizáciami.

Členstvo v Hybrid CoE prináša výhody v podobe prístupu k informáciám zozbieraným z analýz a výstupov Centra, networkingu a výmeny informácií. Centrum vykonáva výskum a analýzu hybridných hrozieb a vypracováva metodiku na boj proti takýmto hrozbám. Vedie dialóg s vládnymi i mimovládnymi expertami a odborníkmi z celého radu špecializovaných odvetví zameraných na zlepšenie situačného povedomia o hybridných hrozbách. Expertíza Centra sa ďalej zameriava na hodnotenie bezpečnostného prostredia z pohľadu hybridného pôsobenia tretích strán, na charakteristiku a zmeny hybridných stratégií, strategickú kultúru, mapovanie trendov či vypracovávanie scenárov a analýz. Intenzívne podporuje vytváranie záujmových sietí (networking) s cieľom posilňovať kapacity v multidisciplinárnych oblastiach. Pozornosť venuje aj edukačným činnostiam zameraným na pochopenie hybridných hrozieb. Centrum podporuje v členských krajinách tréningy a výcvik vypracovávaním príručiek či cielených štúdií. Hybrid CoE slúži ako centrum expertízy, ktoré aktívnym spôsobom podporuje individuálne a kolektívne úsilie jeho členských štátov posilniť ich civilno-vojenské schopnosti, odolnosť a pripravenosť čeliť hybridným hrozbám. Centrum úzko spolupracuje s EÚ a NATO a má ponúkať podporu a zhromažďovať skúsenosti a odborné znalosti v prospech všetkých jeho členských štátov.[18]

16 Viac informácií o Centre excelentnosti NATO na strategickú komunikáciu je dostupných na https://www.stratcomcoe.org/

17 Ministerstvo obrany Slovenskej Republiky, Správa o činnosti Vojenského spravodajstva za rok 2017, júl 2018, http://mepoforum.sk/wp-content/uploads/2018/07/Spr%C3%A1va-o-%C4%8Dinnosti-Vojensk%C3%A-9ho-spravodajstva-za-rok-2017.pdf

18 Európske centrum excelentnosti pre boj proti hybridným hrozbám, Čo je Hybrid CoE?, https://www.hybridcoe.fi/what-is-hybridcoe/

Preto by sa Slovenská republika mala stať aktívnym členom v špecializovaných medzinárodných organizáciách, konkrétne členom EU Hybrid CoE[19] a NATO StratCom CoE.[20] Aktívne členstvo SR v týchto inštitúciách zvýši odbornosť národných expertov a obranyschopnosť SR. Zatiaľ čo Slovensko by sa malo stať členom NATO StratCom CoE už začiatkom roka 2019, prípadné členstvo v EU Hybrid CoE sa zvažuje.

19 Viac informácií o Európskom centre pre boj proti hybridným hrozbám je dostupných na https://www.hybridcoe.fi/.

20 Viac informácií o Centre excelentnosti NATO na strategickú komunikáciu je dostupných na https://www.stratcomcoe.org/

4. OCHRANA INTEGRITY VOLIEB

PRACOVNÁ SKUPINA NA OCHRANU VOLIEB

Ochrana integrity volebných procesov je jedným zo základných predpokladov demokratickej legitimity v zastupiteľskej demokracii. Vzhľadom na narastajúci počet incidentov spojených so zásahmi do volebného procesu je vhodným riešením vytvorenie pracovnej skupiny na bezpečnosť volieb – *Election security task force*.

Princípy jej fungovania sú podrobne popísané v Compendium on Cyber Security of Election Technology.[21] Takáto pracovná skupina na bezpečnosť volieb je užitočná pri prípravách na voľby (ako metóda spolupráce a koordinácie zúčastnených strán), ako aj počas volieb ako nonstop podpora, ktorá je k dispozícii 24 hodín denne. Mala by zahŕňať riadiaci orgán pre voľby a organizáciu zodpovednú za informačnú bezpečnosť vo voľbách, ako aj príslušné vládne a národné tímy CSIRT.

Je nevyhnutné, aby organizátori volieb a osoby zodpovedné za kybernetickú bezpečnosť volieb mali priamy kontakt s organizáciou zodpovednou za riešenie IT incidentov vo verejnej správe, ako sú CSIRT. Komunikačné kanály medzi orgánmi zodpovednými za organizáciu volieb a ostatnými relevantnými aktérmi by mali byť vytvorené v dostatočnom predstihu a chránené pred vonkajšími zásahmi. Mali by zahŕňať komunikačný kanál určený čisto na tento účel a dostupný 24 hodín denne, ako napríklad kontakty na príslušných jednotlivcov v dotknutých inštitúciách.

Okrem ochrany samotnej IT infraštruktúry je však dôležité zamerať sa aj na iné aspekty integrity volieb. Nedávne kybernetické útoky na voľby vo viacerých krajinách sveta obsahovali informačné operácie zamerané na ovplyvnenie ich výsledkov. Preto by sa okrem samotnej volebnej technológie mali brať do úvahy incidenty v oblasti počítačovej bezpečnosti, ktoré by mohli ovplyvniť verejnú mienku. Za typický príklad možno pokladať neoprávnené vniknutie do IT systémov politickej strany či volebného tímu, a následné ukradnutie a zverejnenie informácií o kandidátoch či politických stranách s cieľom ovplyvnenia volebných výsledkov.

21 NIS Cooperation Group, Compendium on Cyber Security of Election Technology, http://ec.europa.eu/information_society/newsroom/image/document/2018-30/election_security_compendium_00BE09F9-D2BE-5D69-9E39C5A9C81C290F_53645.pdf

Pri vytváraní takejto pracovnej skupiny na bezpečnosť volieb je potrebné zabezpečiť a pripraviť:

- jednotné kontaktné miesto pre takéto incidenty;
- rebríček eskalácie kríz, v ktorom sa podrobne uvádzajú druhy a úrovne ich závažnosti;
- jasné rozdelenie úloh a zodpovedností medzi jednotlivých členov pracovnej skupiny;
- komunikačné prostriedky;
- flexibilné prideľovanie zdrojov;
- primeraný výcvikový plán.

Takáto pracovná skupina bola vytvorená a nasadená v nedávnych voľbách v Katalánsku. V deň volieb tam bol nasadený tím, ktorý dohliadal a spravoval každú udalosť dňa. Pracovná skupina priamo komunikovala s tímami zodpovednými za systémy, vývoj, komunikáciu, bezpečnosť a forenzné analýzy, ako aj s DoS[22] tímami. Stretávali sa každé tri hodiny počas volieb a v čase sčítania výsledkov každú hodinu.[23]

V Estónsku, ktoré zaviedlo elektronické hlasovanie prostredníctvom internetu (I-voting),[24] celý proces volieb riadi pracovná skupina, ktorá spája organizátora volieb, Úrad pre informačný systém a poskytovateľov služieb, na ktorých sa spolieha I-hlasovanie, s vývojárom softvéru. Komunikáciu riadi tím, ktorý sa skladá zo zástupcov organizátora volieb, Úradu vlády a v prípade I-hlasovania aj z Úradu pre informačný systém.[25] V podmienkach Slovenskej republiky by takáto pracovná skupina na ochranu volieb mohla vzniknúť ako dočasný orgán Úradu štátnej komisie pre voľby a financovanie politických strán, ktorý zriaďuje Ministerstvo vnútra Slovenskej republiky.[26]

22 DoS - Denial of Service - typ útoku na počítačovú infraštruktúru spočívajúci v zaplavení servera veľkým množstvom požiadaviek spôsobujúci jeho nedostupnosť. Jeden z najzakladanejších druhov kybernetických útokov na infraštruktúru.

23 NIS Cooperation Group, Compendium on Cyber Security of Election Technology, http://ec.europa.eu/information_society/newsroom/image/document/2018-30/election_security_compendium_00BE09F9-D2BE-5D69-9E39C5A9C81C290F_53645.pdf

24 I-voting, https://e-estonia.com/solutions/e-governance/i-voting/

25 NIS Cooperation Group, Compendium on Cyber Security of Election Technology, http://ec.europa.eu/information_society/newsroom/image/document/2018-30/election_security_compendium_00BE09F9-D2BE-5D69-9E39C5A9C81C290F_53645.pdf

26 § 15 ods.4 zákona č. 180/2014 Z.z. o podmienkach výkonu volebného práva a o zmene a doplnení niektorých zákonov

5. ZAPÁJANIE DOBROVOĽNÍKOV DO OBRANY PROTI KYBERNETICKÝM A INFORMAČNÝM HROZBÁM

ESTÓNSKA OBRANNÁ LIGA - JEDNOTKA KYBERNETICKEJ OBRANY

V oblasti kybernetickej bezpečnosti a kybernetických hrozieb dochádza k čoraz častejšiemu stieraniu rozdielov medzi štátnymi aktérmi, súkromnými spoločnosťami a ideologicky motivovanými dobrovoľníkmi. Masívne kybernetické útoky, ktorým čelilo v roku 2007 Estónsko, boli realizované kombináciou štátnych aktérov a ideologicky motivovaných jednotlivcov,[27] a rovnako tomu bolo aj v prípade konfliktu na Ukrajine, ktorý okrem fyzickej roviny prebiehal (a stále prebieha) aj v rovine kybernetickej, kde na oboch stranách bojujú rôzni aktéri – štáty, súkromné spoločnosti aj skupiny hackerov.[28]

Tak, ako sú kybernetické útoky niektorých štátnych aktérov často „outsourcované“ rôznym skupinám operujúcim mimo zákonné rámce, aj kybernetická ochrana v mnohých krajinách spája štátne inštitúcie so súkromným sektorom. V boji proti kybernetickým hrozbám vznikli v niektorých krajinách zaujímavé formy zapájania dobrovoľníkov do opatrení kybernetickej obrany, ktoré dokážu preklenúť rozdiel v kapacitách (personálnych, finančných, technických) v prípade menších štátov, ktoré čelia mnohonásobne väčšiemu útočníkovi.

Za najzaujímavejší príklad takejto praxe je možné považovať jednotku kybernetickej obrany Estónskej obrannej ligy (The Cyber Defence Unit of the Estonian Defence League[29]). V čase svojho vzniku získala celosvetovú pozornosť ako inovatívny model zapojenia dobrovoľníkov do národnej kybernetickej obrany. Vznikla na základe dlhoročnej spolupráce odborníkov na kybernetickú bezpečnosť v štátnom a súkromnom sektore v Estónsku, ktorá začala v dôsledku rozsiahleho kybernetického útoku na Estónsko v roku 2007. Jednotka sa zameriava na posilnenie zručností odbornej kybernetickej obrany svojich dobrovoľných členov s cieľom pripraviť a rozšíriť podporné kapacity, ktoré možno poskytnúť v prípade útoku či krízy.

27 Damien McGuinness, Ako kybernetický útok transformoval Estónsko, BBC, apríl 2017, https://www.bbc.com/news/39655415

28 Andy Greenberg, Ako sa celý národ stal testovacím laboratóriom pre ruskú kybernetickú vojnu, Wired, 20. jún 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/ alebo Natalia Zinets, Ukrajina obvinila Rusko z nového kybernetického útoku na jej infraštruktúru, Reuters, 15. február 2017 https://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN15U2CN

29 Estónska obranná liga – Kaitseliit, http://www.kaitseliit.ee/en/cyber-unit

Hlavný význam jednotky kybernetickej obrany Estónskej obrannej ligy je v tom, že podporuje spoluprácu medzi verejným a súkromným sektorom v oblasti kybernetickej bezpečnosti, posilňuje informovanosť o kybernetickej bezpečnosti medzi obyvateľmi a podporuje prevenciu a reakciu na kybernetické hrozby.

Úloha Estónskej obrannej ligy vo vnútroštátnej kybernetickej bezpečnosti je uznaná niekoľkými politickými a legislatívnymi dokumentmi vrátane Stratégie národnej bezpečnosti a Plánu rozvoja národnej obrany na roky 2013-2022. Nedávno prijatý zákon Estónskej obrannej ligy výslovne integruje jednotku kybernetickej obrany do národného obranného systému a poskytuje jej zákonne stanovený cieľ a rámec pre štruktúru, riadenie, členstvo a fungovanie.[30]

Príklad Estónskej kybernetickej obrany je zaujímavý a relevantný pre Slovensko najmä preto, lebo ukazuje, ako môže aj menší štát s obmedzenými kapacitami využiť kapacity svojho obyvateľstva na zvýšenie svojej pripravenosti a ochrany voči kybernetickým útokom.

ELFOVIA BOJUJÚCI PROTI TROLLOM

Vo viacerých pobaltských a severských krajinách existujú aktívni občania, ktorí dobrovoľne overujú správy a komentáre v online diskusiách. Pomáhajú tak novinárom a zároveň zabraňujú šíreniu rôznych dezinformácií. V Estónsku, Litve aj Lotyšsku sú ich už tisíce. Títo dobrovoľníci, ktorí sa na začiatku samovoľne stretli a spojili v rôznych online skupinách, bojujú proti dezinformáciám, nahlasujú falošné profily na Facebooku, identifikujú a debatujú s online trollmi v diskusiách, či odhaľujú IP adresy zo zahraničia. Svojím konaním chcú redukovať aktivity a vplyv falošných správ a diskutérov - trollov. Elfovia bojujúci proti trollom sa tak stali online domobranou, ktorá bojuje a háji záujmy jednotlivých krajín v informačných operáciách a voči podvratným aktivitám rôznych zahraničných aktérov. Táto iniciatíva uvedomelých občanov vznikla v roku 2014 v Litve a postupne sa rozšírila do ďalších pobaltských krajín.

Aktivity elfov sú už v niektorých krajinách zorganizované do rôznych štruktúr a vedia sa veľmi rýchlo zorganizovať a reagovať na šírenie rôznych hoaxov. V niektorých prípadoch sa dajú aktivity elfov porovnať s aktivitami kontrarozviedky. Napriek tomu je však ich práca stále na dobrovoľnej báze a ich identity nie sú verejné známe. Sú to občania, ktorí si uvedomujú možné bezpečnostné riziká propagandy a svojím zapojením podporujú demokratické

30 Kadri Kaska, Anna-Maria Osula, LTC Jan Stinissen, Jednotka kybernetickej obrany Estónskej obrannej ligy, Analýza legislatívy, politík a organizácie, Centrum excelentnosti NATO pre kybernetickú bezpečnosť, 2013 https://ccdcoe.org/sites/default/files/multimedia/pdf/CDU_Analysis.pdf

mechanizmy v ich krajinách. Ich centrálou je Google skupina, na ktorej si zdieľajú informácie a koordinujú svoje aktivity.[31]

Budovanie obranyschopnosti obyvateľstva a ich aktívne zapojenie do vyvracania dezinformácií a propagandy zvyšuje odolnosť spoločnosti voči informačným operáciám a podvratným aktivitám rôznych aktérov, či už domácich alebo zahraničných. Zatiaľ čo na Slovensku možno pozorovať zárodky mobilizácie a organizácie skupín obyvateľov, akou je napríklad facebooková skupina #somtu, ich úspechy sú stále marginálneho charakteru v porovnaní s elfmi, preto by bolo vhodné v širšej miere využiť skúsenosti elfov z Pobaltia a aplikovať ich aj na Slovensku.

31 Michael Weiss, Pobaltskí elfovia bojujú proti ruským trollom, The Daily Beast, marec 2016, https://www.thedailybeast.com/the-baltic-elves-taking-on-pro-russian-trolls?ref=scroll

6. BRANNÁ VÝCHOVA A ZAPOJENIE DOBROVOĽNÍKOV DO OBRANY ŠTÁTU

V regióne celej strednej Európy sa v posledných rokoch znovu objavil fenomén polovojenských skupín. Význam a využitie dobrovoľných polovojenských síl v ozbrojených konfliktoch vo svete je čoraz výraznejšie, a najmä v oblasti teritoriálnej obrany sa ukazuje ako vhodná alternatíva v čase profesionalizácie armády. Tá, okrem nesporných pozitív, so sebou priniesla aj zníženie možností na zapojenie najmä mladých ľudí do aktivít súvisiacich s obranou a vojenstvom, ku ktorému mnohí prirodzene inklinujú. Na napĺňanie takýchto potrieb vzniklo v poslednej dobe množstvo polovojenských skupín rôzneho charakteru. So vznikom takýchto polovojenských skupín sa však spájajú aj mnohé riziká, keďže predstavujú častý objekt záujmu cudzích spravodajských služieb. Vo viacerých krajinách však vznikli spôsoby zapojenia dobrovoľníkov do bezpečnostných štruktúr, ktoré eliminujú takéto riziká a dokážu nasmerovať záujem mladých ľudí správnym smerom, a prispievajú tak k zvyšovaniu pripravenosti a kapacít daného štátu na prípadný ozbrojený konflikt.

BUDOVANIE POVEDOMIA O KOLEKTÍVNEJ OBRANE V POĽSKU

Krajinou, ktorá má veľmi dobrý systém budovania povedomia o kolektívnej obrane a aktívnej občianskej participácii je Poľsko. Vojna v Gruzínsku v roku 2008 viedla v Poľsku k vzniku „vojenskej hodiny“ (wojskowe klasy)[32] na stredných školách. Tieto lokálne iniciatívy učiteľov, rodičov a žiakov, podporované aj štátnymi inštitúciami, majú zvýšiť pripravenosť obyvateľstva na potencionálny vojenský ozbrojený konflikt. Pripravené a sebestačné obyvateľstvo, ktoré má základné poznatky napríklad o poskytnutí zdravotnej starostlivosti či základy prežitia v lese, je cennou devízou v prípade napadnutia.

VOJSKÁ TERITORIÁLNEJ OBRANY

Vojská teritoriálnej obrany (Wojska Obrony Terytorialnej – WOT) v Poľsku sú príkladom začlenenia dobrovoľníkov z radov polovojenských skupín do oficiálnych štruktúr poľských ozbrojených síl.[33] Vzhľadom na ruské podvratné a expanzné aktivity v regióne v novembri 2016 poľský minister obrany Antoni Macierewicz deklaroval zámer investovať 800 miliónov eur (3.5 miliárd zlotých) na zriadenie paramilitárnych jednotiek s počtom 53 tisíc príslušníkov do roku 2019. Každé zo 16 vojvodstiev Poľska má mať paramilitárne jednotky s 3000-

32 Fideles et Instructi Armis, Vojenské hodiny, https://fia.com.pl/klasy-wojskowe/

33 Ministerstvo národnej obrany Poľskej republiky, Vojská teritoriálnej obrany, http://en-m.mon.gov.pl/polish-armed-forces/wojsko-polskie/territorial-defence-forces-k2017-05-10/

5000 príslušníkmi. Jednotky majú pozostávať prevažne z dobrovoľníkov, ktorí absolvujú 16-dňový vojenský výcvik. Šesť až osem percent príslušníkov jednotiek majú tvoriť profesionálni vojaci, ktorí budú dobrovoľníkom veliť.[34]

DOBROVOĽNÉ VOJENSKÉ CVIČENIA PRE ŠTUDENTOV

Ďalšou zaujímavou iniciatívou v Poľsku je akademická légia (legia akademicka)[35] – dobrovoľné vojenské cvičenia pre študentov stredných škôl počas školských prázdnin. Tento program je priamo podporovaný poľským Ministerstvom školstva a Ministerstvom obrany a doteraz sa ho zúčastnilo okolo 12 tisíc žiakov stredných škôl. Takéto tréningy nielen motivujú mladých ľudí a budujú v nich zmysel pre zodpovednosť a zdravý patriotizmus, ale zároveň nedávajú priestor organizovať podobné cvičenia a zneužívať túto agendu rôznym polovojenským skupinám s pochybnou orientáciou a smerovaním, ako napríklad Slovenskí branci, ktorí mali sériu prednášok a praktických cvičení na slovenských školách v roku 2017.

PRAKTICKÉ PRÍRUČKY AKO REALIZOVAŤ CIVILNÝ ODBOJ V PRÍPADE NAPADNUTIA

Zaujímavý prístup k tomu, ako zvyšovať obranyschopnosť a pripravenosť obyvateľov na potenciálne napadnutie a následné ovládnutie krajiny cudzími mocnosťami, má Ministerstvo národnej obrany Litovskej republiky, ktoré vydalo tri príručky, v ktorých poskytuje informácie, ako sa brániť a reagovať na potenciálnu agresiu primárne zo strany Ruskej federácie. Prvú príručku Ako postupovať v prípade mimoriadnych okolností či vojenského konfliktu (How to Act in Extreme Situations or Instances of War) vydalo Ministerstvo národnej obrany ešte v roku 2014 ako odozvu na anexiu Krymu Ruskom. Príručka obsahovala konkrétne pokyny a návrhy občianskeho vzdoru a neposlušnosti – od štrajkov a blokád cez šírenie dezinformácií až po realizovanie kybernetických útokov proti nepriateľovi, ktoré by občania Litvy mohli aplikovať v prípade okupácie.

Druhý revidovaný manuál aj s karikatúrami s názvom Pripravte sa, ako prežiť výnimočné stavy núdze a vojnu: veselý pohľad na závažné odporúčania (Prepare to Survive Emergencies and War: a Cheerful Take on Serious Recommendations) vydalo ministerstvo v roku 2015. Zatiaľ čo prvé dve príručky sa do veľkej miery

34 Pre viac informácií o prístupoch k paramilitárnym jednotkám a možnostiach ich využitia pozri Katarína Klingová a Tomáš Nagy, Paramilitárne skupiny v krajinách V4: Hrozba alebo príležitosť?, GLOBSEC, december 2017, https://www.globsec.org/wp-content/uploads/2018/11/Paramilitárne-skupiny-v-krajinách-V4.pdf

35 Poľské ozbrojené sily, Legia Akademicka, http://www.wojsko-polskie.pl/pl/pages/pilotazowy-program-ochotniczego-szkolenia-studentow-legia-akademicka-l/

venovali nenásilnému odboju a poskytovali občanom praktické usmernenia, ako sa správať a ako reagovať na rôzne udalosti, ktoré sa môžu vyskytnúť v prípade stavu núdze, mimoriadnych udalostí či vojny, najnovšia publikácia s názvom Čo potrebujeme vedieť o odboji: Príručka k aktívnemu odboju (What We Need to Know about Resistance: Guide to Active Resistance) sa venuje aj prípadom aktívnej opozície občanov, ktorí sú na území okupovanom nepriateľom, konkrétne Ruskom.[36]

Príručka rozoberá veci typu: ako rozpoznať ruské zbrane, tanky, nášľapné míny a inú vojenskú techniku, ako podať prvú pomoc či ako prežiť v divočine. Litovská príručka taktiež vychádza z predpokladov, že civilní obyvatelia môžu slúžiť ako informátori v rámci systému včasného varovania a môžu poskytovať cenné informácie o pohybe a aktivitách nepriateľa. Preto samotný manuál aktívne vyzýva občanov, aby špehovali a podávali správy o nepriateľoch, ak by sa Litva znovu dostala pod ruskú okupáciu.[37]

Vyše 30 tisíc kópií najnovšej príručky bolo distribuovaných do škôl, knižníc a iných verejných inštitúcií v Litve. Elektronická verzia všetkých troch publikácií je voľne dostupná na internetovej stránke Ministerstva národnej obrany Litovskej republiky.[38] Informovaní občania zvyčajne nepodliehajú panike a vedia, ako majú konať v rôznych situáciách. Pripravené obyvateľstvo, ktoré vie, čo má robiť v prípade napadnutia cudzími mocnosťami a vie, aké aktivity môže realizovať a vytvoriť tak silný a efektívny odboj, môže radikálne spomaliť postup nepriateľa a oslabiť jeho aktivity. Aj Slovensko by malo začať aktívne budovať obranyschopnosť svojho obyvateľstva s využitím podobných princípov pod vedením jednotlivých rezortov, Ministerstva obrany SR, Ministerstva vnútra SR či Ozbrojených síl SR.

36 Ministerstvo národnej obrany Litovskej republiky, Ako postupovať v prípade mimoriadnych okolností či vojenského konfliktu, http://kam.lt/lt/katurimezinoti.html

37 Nic Robertson, Antonia Mortensen, Elizabeth Roberts a Woj Treszczynski, Litva vydala príručku o tom, čo robiť, ak ju Rusko napadne, CNN, október 2016, https://edition.cnn.com/2016/10/28/europe/lithuania-war-manual/index.html

38 Ministerstva národnej obrany Litovskej republiky, Ako postupovať v prípade mimoriadnych okolností či vojenského konfliktu, http://kam.lt/lt/katurimezinoti.html

ZOZNAM POUŽITÝCH SKRATIEK

GOVSITCEN - Government Situation Centre - vládne situačné centrum

EÚ - Európska únia

NATO - Severoatlantická aliancia

SIS - Slovenská informačná služba

NBAC - Národné bezpečnostné analytické centrum

Hybrid CoE - Európske centrum excelentnosti pre boj proti hybridným hrozbám

MSB - Švédska Agentúra pre civilnú ochranu (Swedish Civil Contingencies Agency)

ČR - Česká republika

SR - Slovenská republika

GRU - Hlavné riaditeľstvo Generálneho štábu ozbrojených síl Ruskej federácie

OPCW - Organizácia pre zákaz chemických zbraní

WOT - Vojská teritoriálnej obrany (Wojska Obrony Terytorialnej)

POZNÁMKY