

# **Spravodajské služby v zmenenom operačnom prostredí – aktuálne úlohy a problémy spravodajských služieb**

Asociácia bývalých spravodajských dôstojníkov spolu s Fakultou práva Paneurópskej vysokej školy v Bratislave usporiadali 6. 12. 2016 už 10. medzinárodné sympóziu na tému „Spravodajské služby v zmenenom operačnom prostredí – aktuálne úlohy a problémy spravodajských služieb“. Uverejňujeme referáty, ktoré budú koncom apríla 2017 vydané v printovej verzii zborníka.

## **Obsah**

### **Predslov**

PhDr. Igor Cibula

### **Príhovory**

doc. JUDr. PhDr. Peter Potásch, PhD.

Ing. Pavol Prokopovič

## **HLAVNÉ REFERÁTY**

K. Randák: Příčiny změn operačního prostředí zpravodajských služeb

A. Monckton: Kritika britskej bezpečnostnej stratégie

R. Laml: Transparentnosť a spravodajské služby

R. Kusenda: Výzvy pre spravodajskú komunitu v kontexte hybridných hrozieb

P. Draxler: Vplyv dostupnosti šifrovania na bezpečnosť občanov a štátu

P. Zeman: Pokus o bilanci úspechů a proher polistopadových českých a slovenských zpravodajských služeb

J. Málík: Reflexia zmeneného operačného prostredia v spravodajskej činnosti polície

I. Cibula: Ženy v štruktúrach spravodajských služieb

## **Závery zo sympózia**

## Predslov

Na úvod k príspevkom z 10. medzinárodného sympózia - ktoré 6. decembra 2016 usporiadala Asociácia bývalých spravodajských dôstojníkov (ABSD) v spolupráci s Fakultou práva Paneurópskej vysokej školy v Bratislave – je vhodné pripomenúť, že sympóziu je jediné verejné diskusné fórum na Slovensku, zamerané na otázky súvisiace s činnosťou spravodajských služieb. Keď sme v apríli 2006 založili našu asociáciu, u mnohých prevládal skepticizmus a pochybnosti, či naša organizácia dokáže plniť poslanie a dosiahne ciele, ktoré sme si vytýčili. Predovšetkým sme chceli prekonať negatívny historický stereotyp vnímania tajných služieb a poskytnúť verejnosti príležitosť nahliadnuť do zákulisia spravodajskej komunity. Základným cieľom ABSD je prispievať osvetovou činnosťou k vytváraniu občianskej podpory pre správne fungujúci a zákonný spravodajský systém Slovenskej republiky. Preto sme sa zúčastňovali na verejných a mediálnych diskusiách na túto tému a spolupracovali na príprave legislatívnych zámerov v oblasti spravodajských služieb.

Naše začiatky neboli ľahké, pretože okrem nepriazne niektorých médií sme predovšetkým čelili podozreniam Slovenskej informačnej služby, kde politickí nominanti na čele tejto inštitúcie nás podozrievali z toho, že vykonávame aj aktivity nad rámec našich stanov. Monitorovanie a spravodajské rozpracovanie ABSD zo strany SIS však väčšinu členov asociácie neodradilo od toho, aby pokračovali v plnení našich predsavzatí. Až v marci 2012 po nástupe nového vedenia SIS sa situácia zmenila a vznikli štandardné vzťahy medzi vedením ABSD a spravodajskou službou, ktorá pozitívne reagovala na naše iniciatívy. Pochopenie pre spoločenský význam aktivít asociácie nám umožnilo, aby sme vedeniu SIS systematicky predkladali návrhy a pripomienky k pripravovanému zákonu o spravodajských službách a prezentovali naše stanoviská k aktuálnym problémom spravodajskej komunity na Slovensku.

Osobitný význam pre našu činnosť mala podpora Fakulty práva Paneurópskej vysokej školy v Bratislave a osobitne angažovanosť jej vtedajšieho dekana Prof. JUDr. Jaroslava Ivora, DrSc., ktorý sa s niektorými ďalšími pedagógmi fakulty aktívne podieľal na našich medzinárodných sympóziách. Veľmi dôležitá je pre nás skutočnosť, že fakulta poskytuje materiálno-technickú pomoc pri organizovaní sympózií a podieľa sa tiež aj na jej organizačnom zázemí. Na sympóziách sa zúčastňujú aj študenti fakulty, ktorí si v rámci magisterského štúdia vybrali voliteľný predmet Spravodajské služby; fakulta je jedinou právnickou fakultou na Slovensku, ktorá má tento predmet zaradený vo svojom študijnom programe.

Mimoriadne dôležitú úlohu pri koncipovaní obsahovej náplne sympózií majú naši priatelia z Českej republiky, s ktorými ABSD spolupracuje pri tvorbe obsahového zamerania týchto podujatí. Prakticky pravidelnými lektormi sympózia sú bývalí riaditelia českej rozvedky Petr Zeman a Karel Randák; v minulých rokoch participovali na sympóziu svojimi príspevkami aj kolegovia Peter Púčik, Jan Schneider, Oldřich Černý, Andor Šándor, Ladislav Pokorný a ďalší českí spravodajskí a bezpečnostní experti. Zvlášť si ceníme, že štyrikrát vystúpili na našom sympóziu predstavitelia britskej spravodajskej komunity, vrátane bývalého riaditeľa služby MI6 Sira Richarda Dearlova. Vážime si lektorskú spoluprácu s nebohým riaditeľom maďarskej rozvedky Kálmánom Kocsisom i bývalým liaisonom maďarskej služby v Bratislave Lajosom Tabom, ktorí niekoľkokrát vystúpili na našom sympóziu.

Podobne intenzívne sme spolupracovali aj s bývalými vysokými predstaviteľmi spravodajských štruktúr v Chorvátsku a v Srbsku. Cenným príspevkom k úrovni sympózia bol referát konzultanta ženevského Strediska pre demokratickú kontrolu ozbrojených síl (DCAF) Freda Schreiera, ktorý sa s nami podelil o svoje skúsenosti z oblasti reformy bezpečnostného sektora a spravodajských služieb z obdobia, keď pôsobil ako riaditeľ Strategickej spravodajskej služby vo Švajčiarsku.

Desiate medzinárodné sympóziu nastolilo aktuálne témy spravodajskej komunity a poskytlo priestor na vyjadrenie názorov nielen odborníkom zo spravodajsko-bezpečnostnej oblasti, ale odzneli tu aj referáty 1. viceprezidenta Prezídia Policajného zboru Slovenskej republiky a tiež diplomata z Ministerstva zahraničných vecí a európskych záležitostí SR. Diskusia o úlohách a problémoch spravodajských služieb v zmenenom operačnom prostredí v kontexte so zvyšujúcou sa mierou bezpečnostných rizík a nových bezpečnostných hrozieb si vyžaduje ich otvorenejšiu prezentáciu pred verejnosťou, aby podporovala spravodajskú komunitu a chápala jej potreby a nároky. A v tom spočívalo hlavné poslanie tohto zavedeného medzinárodného podujatia.

PhDr. Igor Cibula,  
predseda Asociácie bývalých spravodajských dôstojníkov

---

## Príhovor

Vážené dámy, vážení páni !

Považujem si za česť privítať Vás na akademickej pôde Fakulty práva PEVŠ, ktorá už desať rokov spolupracuje s Asociáciou bývalých spravodajských dôstojníkov na organizovaní medzinárodných sympózií, venovaných histórii, ale hlavne aktuálnym problémom spravodajských služieb. Spoločne sme vytvorili tradíciu verejných diskusií o témach, ktoré boli kedysi pre väčšinu spoločnosti tabu. Vďaka iniciatíve ABSD schádzajú sa na našej fakulte každý rok bývalí riaditelia spravodajských služieb, bezpečnostní experti a analytici zo spriatelенých krajín, aby priblížili širšiemu okruhu zainteresovaných poslucháčov zainteresovaný pohľad na to, čím žije spravodajská komunita.

Zaslúži si ocenenie, že organizátori tohtoročného sympózia si vybrali osobitne významnú tému – aktuálne úlohy a problémy spravodajských služieb v zmenenom operačnom prostredí. Neregulovaná migrácia hlavne v Európe, explózia medzinárodného terorizmu, hybridné vojny a nebývalý prienik moderných informačných technológií do činnosti spravodajských služieb nastoľujú nové pohľady na fungovanie spravodajských služieb, ktoré zaiste budú prezentované na tomto sympóziu.

Dovolím si pripomenúť, že medzinárodné sympózia o problematike spravodajských služieb neorganizujeme náhodou. Fakulta práva PEVŠ už pred desiatimi rokmi zaradila do akreditovaného magisterského štúdia programu právo predmet spravodajské služby, ktorý prednáša PhDr. Igor Cibula. Každý rok si tento predmet vyberie niekoľko desiatok študentov denného i externého štúdia, ktorí sa potom prezentujú kvalifikovanými prácami. Môžeme sa tak trochu popýšiť aj tým, že tohto roku bude sympóziom už po druhýkrát moderovať absolventka našej fakulty Mgr. Alexandra Janoušková, inak verejnosti dobre známa svojou publicistickou činnosťou ešte pod svojím dievčenským menom Macúchová, pod ktorým moderovala sympóziom pred troma rokmi.

Desiate medzinárodné sympóziom je tak trochu príležitosťou, aby sme bilancovali účasť lektorov, ktorí sa pričínili o úroveň tohto medzinárodného podujatia. Na prvom mieste musím spomenúť, že významnou mierou o kvalifikovanú úroveň predchádzajúcich sympózií sa pričínili bývalí riaditelia spravodajských služieb z Českej republiky, ktorí pravidelne prichádzali do Bratislavy – a aj ich dnešné zastúpenie na 10. medzinárodnom sympóziu svedčí o tom, že česko-slovenské spravodajské spoločenstvo ani po rozdelení Česko-Slovenska neprestalo existovať a efektívne vzájomne komunikovať.

Osobitne sa žiada vyzdvihnúť, že na štyroch našich sympóziách – vrátane dnešného sympózia - sa aktívne zúčastnili predstavitelia britskej spravodajskej komunity, nevynímajúc bývalého generálneho riaditeľa medzinárodne uznávanej MI6 – Sira Richarda Dearlova. Podobne si ceníme produktívnu spoluprácu s predstaviteľmi maďarských spravodajských služieb na čele s nebohým generálom Kálmánom Kocsisom. Prínosom bola tiež účasť bývalých šéfov služieb zo Švajčiarska, Srbska a Chorvátska, ktoré parametrami svojich spravodajských služieb patria do podobnej kategórie, ako služby Slovenskej republiky.

I keď Slovensko je malá krajina s obmedzenými kapacitami spravodajských služieb, predchádzajúce sympózia dokázali, že dokážeme vytvoriť podmienky na plnohodnotnú výmenu názorov o fungovaní spravodajských služieb v geostrategickom priestore, kde sa nachádza Slovenská republika. Verím, že tohtoročné témy sympózia prispievajú svojou mierou k tomu, aby spravodajské služby efektívne plnili svoje poslanie v boji proti aktuálnym bezpečnostným rizikám.

Na záver si dovoľm poďakovať Asociácii bývalých spravodajských dôstojníkov za spoluprácu, ktorá trvá už desať rokov – a zároveň chcem vyjadriť presvedčenie, že tradícia spolupráce Fakulty práva PEVŠ s veteránmi spravodajskej komunity bude ďalej úspešne pokračovať. A patrí sa vysloviť slová uznania môjmu predchodcovi na poste dekana fakulty – prof. JUDr. Jaroslavovi Ivorovi, DrSc., ktorý spoluprácu všestranne podporoval.

Dnešnému – jubilejnemu – 10.medzinárodnému sympóziu želám úspech a úprimnú výmenu názorov. Veľa šťastia!

doc. JUDr. PhDr. Peter Potásch, PhD.  
dekan Fakulty práva Paneurópskej vysokej školy

---

## Príhovor

Vážený pán dekan, vážené dámy, vážení páni !

S potešením som prijal pozvanie na 10. medzinárodné sympóziu, ktoré pravidelne organizuje Asociácia bývalých spravodajských dôstojníkov v spolupráci s Fakultou práva Paneurópskej vysokej školy. Ako predseda Osobitného kontrolného výboru Národnej rady Slovenskej republiky na kontrolu činnosti Slovenskej informačnej služby vo funkčnom období parlamentu v rokoch 2006-2010 som sa zúčastnil prvého ročníka tohto sympózia a pamätám sa, že tu boli bývalí riaditelia 7 spravodajských služieb z Českej republiky, Maďarska a zo Slovenska, ktorí prišli na toto fórum diskutovať o zmenách v spravodajských službách v postkomunistických krajinách strednej a východnej Európy s ďalšími spravodajskými expertmi. Moderoval ho publicista Milan Žitný a v úvodnom príhovore vtedajší dekan fakulty prof. JUDr. Jaroslav Ivor, DrSc. pri tejto príležitosti zdôraznil, že „vysokoškolsky vzdelaný človek alebo akýkoľvek funkcionár, pracovník štátnej správy by mal mať základné informácie, základné poznatky o fungovaní spravodajských služieb, ich úlohách, či už v dejinách, súčasnosti a budúcnosti.“

Priznám sa, že nie celkom som veril, že som svedkom založenia tradície, ktorá potrvá desaťročie a vďaka Asociácii bývalých spravodajských dôstojníkov a Fakulte práva Paneurópskej vysokej školy trvale zakotví ako nenahraditeľné diskusné fórum spravodajskej komunity. Na druhej strane som držal palce odhodlaným bývalým spravodajským dôstojníkom, ako boli Igor Cibula, Vladimír Mitro, Peter Tóth, ale aj ich kolegom z Českej republiky – ako Peter Zeman, Karel Randák i Jan Schneider – ktorí opakovane na tomto sympóziu prednášali svoje názory, ako by mali spravodajské služby fungovať v demokratickej spoločnosti. Veľmi cenné boli aj názory ich kolegov z Veľkej Británie, z Maďarska i zo Švajčiarska, Chorvátska a Srbska, pretože predstavujú rôznorodú spravodajskú kultúru i tradíciu.

Asociácia bývalých spravodajských dôstojníkov upútala na začiatku svojej existencie môj záujem a pozornosť tým, že ešte pred svojim prvým medzinárodným sympóziom preložili a pripravili vydanie publikácie „Zodpovednosť spravodajských služieb: Právne normy a vhodná prax pre dohľad nad spravodajskými službami“, ktorú pôvodne vydalo ženevské Centrum pre demokratickú kontrolu ozbrojených síl spolu so Strediskom pre ľudské práva pri Právnickej fakulte Univerzity v Durhame vo Veľkej Británii a s Výborom na kontrolu spravodajských služieb Nórskeho parlamentu. Vtedy ma o tejto iniciatíve informoval PhDr. Igor Cibula a požiadal o pomoc pri získavaní sponzorskej podpory. Ako predseda Osobitného kontrolného výboru Národnej rady Slovenskej republiky na kontrolu činnosti Slovenskej informačnej služby som uvítal túto aktivitu a získal som sponzora, ktorý publikáciu

vytlačil. Dostali ju všetci poslanci slovenského parlamentu, ako aj niektorí poslanci parlamentu Českej republiky, vrátane činiteľov českej spravodajskej komunity.

Medzinárodné sympózia ABSD – na ktorých sa podieľa Fakulta práva Paneurópskej vysokej školy – sú venované nielen problémom spravodajských služieb na Slovensku, ale zrkadlia témy, ktorými žije spravodajská komunita v širšom, tak povediac globálnom rámci. Dokazuje to aj dnešné sympóziu, venované novým faktorom, meniacim operatívne prostredie spravodajských služieb. Kráčate s duchom času a snažíte sa prispievať k tomu, aby bezpečnostné a spravodajské služby účinne reagovali na nové bezpečnostné riziká a úspešne plnili očakávania spoločnosti, ktorá sa cíti ohrozená neregulovanou vlnou ilegálnej migrácie do Európy, rozmáhajúcim sa medzinárodným terorizmom i nebezpečenstvami, plynúcimi z hybridných vojen.

Dovoľte mi, aby som sa poďakoval Asociácii bývalých spravodajských dôstojníkov a Fakulte práva Paneurópskej vysokej školy, že založili tradíciu, ktorá podľa môjho pevného presvedčenia sa určite dožije aj výročia druhej dekády svojej existencie. Moje presvedčenie je založené hlavne na tom, že sympóziu organizujú bývalí spravodajskí dôstojníci. Táto profesia je známa tým, že ju vykonávajú ľudia, ktorí sú vytrvalí, húževnatí a trpezliví.

Využívam túto príležitosť, aby som vyjadril pánu dekanovi vďaka tiež za to, že na tejto fakulte sa ako na jedinej civilnej vysokej škole na Slovensku prednáša výberový predmet Spravodajské služby. Nepochybujem o tom, že v takomto kontexte je tradícia medzinárodných sympózií aj do budúcnosti garantovaná.

Želám vám úspešný priebeh sympózia a prajem vám, aby toto podujatie bolo prínosom pre všetkých, ktorí sa na tejto akademickej pôde stretli a chcú vyjadriť alebo poznať kompetentné názory na aktuálne problémy spravodajskej komunity.

Ing. Pavol Prokopovič,  
predseda Osobitného kontrolného výboru  
Národnej rady Slovenskej republiky  
na kontrolu činnosti Slovenskej informačnej služby  
(2006-2010)

---

## **K. Randák: Příčiny změn operačního prostředí zpravodajských služeb**

**Karel Randák (1955)** – *Původně vrcholový športovec a tréner cestnej cyklistiky. V období 1992-1996 bol dôstojníkom československej (FBIS) a neskôr českej kontrarozviedky (BIS). V rokoch 1996 až 2007 pôsobil na Úrade pro zahraniční styky a informace, najprv na utajovaných pozíciách, v rokoch 2004-2006 bol riaditeľom ÚZSI. V roku 2006 ho prezident ČR povýšil do hodnosti generála. Od roku 2007 pracuje ako nezávislý konzultant. Od marca 2011 sa angažuje ako člen správnej rady Nadačního fondu proti korupci.*

Téma tohoto sympozia „Zpravodajské služby ve změněném operačním prostředí – aktuální úkoly a problémy služeb“ přímo vybízí k zamyšlení, o čem že to vlastně chceme hovořit. Nejprve mi dovoluňte položit několik, víceméně řečnických, otázek. Co vlastně lze chápat pod pojmem operační prostředí zpravodajských služeb? Existuje jasná definice, co pod tímto pojmem rozumět? Jsou to pouze vnější podmínky, ve kterých služby působí? Nebo do tohoto pojmu můžeme zahrnout i podmínky vnitřní, ať již jimi rozumíme např. politickou podporu, legislativu, upravující kompetence a činnost služeb, finanční možnosti, které služba má, apod.? V čem a v jakém směru se vlastně operační prostředí změnilo? A změnilo se vůbec natolik, že by to mělo vyžadovat od zpravodajských služeb nějaký radikálně inovativní přístup?

Je všeobecným trendem, módou a pro mnoho lidí i dobrou příležitostí sebezprezentace, ať již politické nebo expertní, spolupodílet se na identifikaci tzv. nových hrozeb. Na základě této identifikace pak jsou navrhovány nejrůznější koncepce, reorganizace a další opatření, která by měla zpravodajská a bezpečnostní komunita uvádět do praxe. Jsou-li tyto kroky připravovány na základě skutečných potřeb zpravodajských služeb, resp. vycházejí-li přímo z jejich požadavků a vlastního poznání, pak bývá zpravidla, ne však vždy, vše v pořádku. Horší stav nastává, jsou-li tato opatření motivována konkurenčním bojem mezi službami a jejich snahou prosadit se na úkor jiných. Klasickým příkladem tohoto chování jsou nikdy nekončící spory o kompetence jednotlivých služeb, mnohdy vedoucí k reálným problémům. Přímo katastrofu, v naší politické kultuře však nikoliv výjimečnou, pak představují ta opatření, která jsou diktována shora, bez hlubší znalosti problematiky, funkčnosti a potřeb bezpečnostního systému. V konečném důsledku je zcela nepodstatné, jsou-li tyto snahy vedeny čirým diletantismem nebo mnohdy dokonce nekalým úmyslem. Česká republika je v této disciplíně skutečným šampionem. Můžeme vzpomenout na celá desetiletí trvající a nikam nevedoucí debaty, týkající se architektury zpravodajské komunity, systému kontroly služeb, atp. Jediným výsledkem těchto politických tanečků byly nejasné kompetence jednotlivých služeb a mnohdy i faktická paralýza jejich činnosti. Nejnázornějším, ale také nejvíce odstrašujícím příkladem, je právě proběhlá tzv. policejní reorganizace. Ta se sice zpravodajské komunity dotkla pouze zprostředkovaně, znamenala však radikální změnu operačního prostředí, minimálně pro služby s vnitřní působností. Přitom existuje dostatek důkazů, že se jednalo o krok zcela účelový a motivovaný politickým zadáním. Tato reorganizace byla úplně v rozporu se známým a osvědčeným: „Neměň nic, co funguje“.

Zkusme tedy tuto poučnou větu aplikovat i na téma tohoto sympozia a zopakujme otázku: „Změnilo se vlastně operační prostředí natolik, že je nutno hledat nové přístupy?“ Můj osobní názor je, že nikoliv. Nikde se neobjevil žádný zcela nový, dříve nepoznaný problém či bezpečnostní hrozba, která by službám nebyla známa již

delší dobu. Částečnou výjimku snad můžeme spatřovat v oblasti bezpečnosti kyberprostoru, ale ani zde se nejedná o úplně novou, dříve neidentifikovanou hrozbu. Je jasné, že intenzita jednotlivých hrozeb se mění v čase. Z toho také vyplývají průběžné změny priorit služeb. Jejich kvalitu a profesionalitu pak lze posuzovat podle toho, jak se s tímto měnícím se prostředím dokáží vypořádat. Vždyť největší zbraní zpravodajců by mělo být umění predikovat vývoj a s předstihem mu přizpůsobovat své priority a v neposlední řadě i kapacity. Tato schopnost je přeci nejpádnejším důvodem existence zpravodajských služeb. Nemají-li ji, samy přispívají k tomu, že smysl této existence bude zpochybňován.

V České republice byly v uplynulém týdnu zveřejněny výsledky tzv. bezpečnostního auditu, jehož vypracování bylo iniciováno premiérem Sobotkou v návaznosti na loňské teroristické útoky ve Francii. I přesto, že sepsání tohoto materiálu trvalo rok, není mezi deseti kapitolami, do kterých se audit dělí, žádná nově identifikovaná hrozba. Jinými slovy, před zpravodajskou komunitou nejsou postaveny náhlé neznámé úkoly, se kterými je třeba se bezodkladně vypořádat. A ještě jinak - operační prostředí - jak vyplývá ze závěrů bezpečnostního auditu, se fakticky nemění. Podle vyjádření premiéra Sobotky je bezpečnostní systém ČR nastaven v zásadě dobře, dlouhodobé hrozby jsou podchyceny a není třeba žádných dramatických změn. Ministr vnitra Chovanec přislíbil, že na drobné nedostatky, odhalené auditem, bude reagováno a na příslušných opatřeních se již pracuje. Jmenoval konkrétně systém školení pro státní úředníky, který by zajistil větší odolnost státní správy před ovlivněním z ciziny a potřebu lepší komunikace uvnitř bezpečnostní komunity. Odhlédneme-li od faktu, že naše státní správa je daleko nebezpečněji ovlivňována nejrůznějšími lobystickými tlaky, s těmito opatřeními nelze než souhlasit. Bohužel, dokonce i v této místnosti je několik osob, které se, v relativně dávné minulosti, pokoušeli obdobná opatření realizovat. Nemusím zdůrazňovat, že prakticky s nulovým dopadem na zmíněnou státní správu nebo zpravodajskou komunitu. Není důvod domnívat se, že právě tentokrát by to mohlo vyjít.

Zajímavou pasáží komentáře ministra Chovance bylo sdělení, že ministerstvo vnitra hodlá čelit dezinformacím, objevujícím se ve veřejném prostoru, které mohou zkreslovat politickou soutěž. Jako příklad pak pan ministr uvedl nedávno zveřejněné informace, že prezidentská kampaň Miloše Zemana byla financována ze zahraničí, konkrétně z Ruska. Ministerstvo vnitra tuto informaci vyhodnotilo tak, že pochází z nedůvěryhodného zdroje a je tedy třeba ji uvést na pravou míru. Zůstává přitom na rozhodnutí občana, jak si situaci sám zhodnotí. Ministerstvo prý nemá ambici dělat cenzora. Dovoluji si k tomu říci dvě poznámky. Za první, domnívám se, že nejlepší obranou proti takovému nařčení by bylo transparentní zveřejnění, z jakých zdrojů byla zmíněná kampaň skutečně financována. K tomu však, v případě Miloše Zemana nikdy nedošlo, a to jako u jediného z prezidentských kandidátů. Za druhé, rád bych věřil, že ministerstvo vnitra pod vedením ministra Chovance bude stejně vehementně bojovat za objektivitu informací i v jiných případech, např. těch, které se budou týkat politické opozice.

Zpět ke změnám operačního prostředí. Pokud oficiální auditní zpráva nenalézá ve vyhodnocování hrozeb slabiny, konstatuje tak, že systém funguje na odpovídající úrovni. Bude tedy na jednotlivých člancích tohoto systému, aby dokázaly zhodnotit míru ohrožení v dané problematice a této míře přizpůsobit



intenzitu jejího rozpracování. Jde tedy o správné nastavení priorit daných služeb a o jejich akceptaci ze strany vlády. S tím pak budou úzce souviset otázky finanční a personální. Klasickým příkladem je např. snaha o nábor úzce specializovaných odborníků v oblasti IT, působících v civilním sektoru. Prozatím však neexistují praktické možnosti a nástroje nabídnout jim adekvátní finanční ohodnocení. Za takových podmínek se boj proti hrozbám v kyberprostoru jeví jako pověstný boj s větrnými mlýny. Úspěšné vyřešení podobných problémů lze bez nadsázky považovat za ony nové výzvy v práci zpravodajských služeb. Schopnost přesvědčit politiky a jim podřízený státní aparát, aby vnímali informace i požadavky, které jsou jim sdělovány ze strany bezpečnostních složek, považuji za klíčový úkol. Součástí operačního prostředí je podle mého i to, jaké podmínky pro efektivní práci služeb, je ten který stát schopen a především ochoten vytvořit. Mnohokrát opakovaný fakt, že za funkčnost bezpečnostního systému jsou odpovědni především politici, nepozbývá na aktuálnosti, ba právě naopak. Je třeba odpovědné lidi přesvědčit, popř. je přinutit, aby přešli od bezduchých frází a neustále se opakujících floskulí ke konkrétnímu naplňování svých slibů.

Problém má však i svoji odvrácenou stranu. I když je z pohledu zpravodajských a bezpečnostních složek jakkoliv pochopitelné, že se snaží využít každé příležitosti ke zlepšení svých podmínek, nemělo by se tak dít bez skutečně reálného podkladu. Tím mám na mysli to, že služby by se měly vyvarovat tendence zveličovat bezpečnostní rizika pouze proto, aby se domohly rozšíření svých kompetencí, příp. navýšení rozpočtů. Pravda je, že momentální bezpečnostní situace nejen v Evropě, ale i ve světě, k takovému chování přímo vybízí a političtí představitelé některými svými výroky jen přilévají olej do ohně. Populistická prohlášení a podpora zdánlivě jednoduchých řešení úspěšně rozdělují společnost. Fakticky se tak vytváří velmi široké pole pro nástup a působnost extremistických názorů a skupin. Výsledkem může být nezanedbatelné zhoršení bezpečnostní situace v dané zemi, mnohdy i s přesahem do zahraničí. Přesně to je situace, kdy by zpravodajské služby měly fungovat jako regulátor a měly by podobné výroky korigovat podle reálného hodnocení situace. Měly by tak jednat i přesto, že v očích veřejnosti vlastně zdánlivě snižují roli své důležitosti a v očích populistů se mohou začít jevit jako státní orgán oponující jejich snaze získat co nejvíce politických bodů.

Má-li být státní správa využívána k objektivnímu informování veřejnosti, jak se o tom zmínil ministr vnitra Chovanec, pak by to mělo platit i v těchto případech. Skutečnost je však zcela odlišná. Díky ne zcela objektivnímu popisu rizik, spojených s uprchlickou vlnou, která Českou republiku zasahuje pouze okrajově, se jak ministerstvo vnitra, tak i zpravodajské služby domohly navýšení kompetencí a rozpočtů. Cena, kterou za to platíme, je však vysoká. Ačkoliv k datu 3. prosince 2016 bylo v detenčních zařízeních v ČR všehovšudy 72 uprchlíků, statistiky hovoří jasně. Téměř 80% občanů ČR se v souvislosti s migranty obává o svoji bezpečnost. V lepším případě je to příklad manipulace s veřejným míněním, v horším to lze označit za rozdmýchávání xenofobních nálad a klasifikovat jako šíření poplašné zprávy. Úkolem služeb by mj. mělo být objektivní informování veřejnosti o skutečné úrovni rizika. Nástrojů k tomu mají nepochybně dost.

Ke shrnutí výše řečeného. Lze-li vůbec hovořit o skutečných změnách operačního prostředí, není příliš na místě tyto změny hledat ve vnějším prostředí nebo ve změnách hrozeb, nýbrž ve vnitřních podmínkách, se kterými se služby musí

vyrovnat. A ačkoliv se to může na první pohled zdát paradoxní, řešení tohoto úkolu je podle mého názoru podstatně složitější. Podmínky vnějšího operačního prostředí se pouze periodicky přelévají od jedné priority ke druhé a tyto posuny lze víceméně dlouhodobě predikovat. Služby se tak mohou s relativně dostatečným časovým předstihem připravit na úkoly i problémy, se kterými se vbrzku budou nuceny vypořádat. Otázkou do diskuze samozřejmě je, zda a jak tak činí. Zcela opačná situace je však u podmínek vnitřních. Náhlé změny názorů a okamžitá rozhodnutí politiků o tom, které cíle a metody zpravodajských služeb lze považovat za legitimní a kterým prioritám je třeba se v danou chvíli věnovat, jsou největší překážkou v systematické práci služeb. Právě pro svoji nepředvídatelnost jsou také důvodem problémů, protože na ně nelze včas a adekvátně reagovat. Existuje-li něco, co bychom mohli označit za příčinu změn v operačním prostředí služeb, pak je to právě tato situace. Samozřejmě to není nový jev, je také zcela běžný a odstranitelný. Stačilo by dosáhnout, v rámci odborné diskuse, dlouhodobé shody na prioritách a nepokoušet se získávat politické body nesmyslnými nápady a návrhy. To je stav, kterého se dlouhodobě nedaří dosáhnout a vina rozhodně není na straně služeb. Není potom divu, že nejpopulárnějším rčením pro příslušníky služeb je: „Spokojenost a výkonnost zpravodajského důstojníka je přímo úměrná vzdálenosti jeho pracoviště od centrály“, což jak jistě uznáte, není ideální stav.

## A. Monckton: Kritika britskej bezpečnostnej stratégie

**Anthony Monckton** (1960) –Vyštudoval archeológiu a antropológiu na Cambridge University; potom slúžil ako dôstojník britskej armády v Nemecku a Belize. V roku 1987 nastúpil do služieb Foreign & Commonwealth Office. Pôsobil na zastupiteľských úradoch v Ženeve, Záhrebe, Banja Luke, Belehrade a Viedni. Niekoľko rokov pôsobil v Londýne ako expert v oblasti boja proti terorizmu a potom ako vedúci odboru vzdelávania a rozvoja v rezorte zahraničnej služby. Po odchode do dôchodku v roku 2015 založil konzultačnú firmu pre korporátne vyšetřovanie so sídlom v Londýne a vo Viedni; je erudovaným odborníkom pre oblasť strednej a východnej Európy a Balkánu.

V novembri 2015 zverejnila britská vláda Národnú bezpečnostnú stratégiu a Prehľad strategickej obrany a bezpečnosti. Keď bol David Cameron zvolený za predsedu vlády v roku 2010, jedným z jeho prvých krokov bolo ustanovenie Národnej bezpečnostnej rady, riadenej z úradu vlády. Podľa príkladu z USA taktiež menoval národného bezpečnostného poradcu. Tento poradca mal za úlohu holisticky vyhodnotiť hrozby proti životným podmienkam v Spojenom kráľovstve a plánovať strategickú reakciu. Po prvýkrát si vládni ministri sadli za stôl spoločne s vedúcimi hlavných rezortov zodpovedných za tvorbu politiky ako aj s vedúcimi bezpečnostných a spravodajských inštitúcií s cieľom diskutovať o výzvach pre národnú bezpečnosť. Cameronova vláda z roku 2010 však nezdedila žiadne financie a zaviedla úsporné opatrenia. To predstavovalo závažné zníženia financií na obranu na vyrovnanie rozpočtu, ako aj zastavenie predtým plánovaného rastu spravodajských a bezpečnostných služieb.

Po získaní absolútnej väčšiny vo voľbách v roku 2015 bola vypracovaná revidovaná stratégia a zverejnená v novembri toho roku. V mojom príspevku sa kriticky pozriem na túto stratégiu a položí si otázku, či sa stále hodí na daný účel po nesmierne závažných udalostiach posledných dvanástich mesiacov. Táto stratégia a prehľad majú takmer sto strán a pokrývajú obranu, zahraničnú politiku, zahraničnú pomoc ako aj služby.

Táto stratégia má tri strategické ciele:

**Chrániť náš národ.** „Cieľom národnej bezpečnosti č. 1 je chrániť našich ľudí – doma, v zámorských územiach a v zahraničí, a chrániť naše územie, ekonomickú bezpečnosť, infraštruktúru a spôsob života.“

**Prezentovať náš globálny vplyv.** „Cieľom národnej bezpečnosti č. 2 je prezentovať náš globálny vplyv – znižovať pravdepodobnosť reálnych hrozieb pre Spojené kráľovstvo, naše záujmy a záujmy našich spojencov a partnerov.“

**Podporovať našu prosperitu.** „Cieľom národnej bezpečnosti č. 3 je podporovať našu prosperitu – využívať príležitosti, pracovať inovatívne a podporovať britský priemysel.“

Vo svojom predhovore Cameron uviedol niekoľko závažných vyhlásení:

- „Naša národná bezpečnosť závisí od našej ekonomickej bezpečnosti a naopak. Takže prvým krokom našej Národnej bezpečnostnej stratégie je zabezpečiť, aby naša ekonomika bola a ostala silnou.“
- „Ako obchodujúci národ s piatou najväčšou ekonomikou na svete závisíme od stability a poriadku vo svete.“

Cameron argumentoval, že úsporné opatrenia počas prvého obdobia jeho vlády pomohli zabezpečiť ekonomickú bezpečnosť. Jeden rok od začiatku druhého obdobia konzervatívnej vlády je ekonomická bezpečnosť neistá a svet sa ukazuje ako menej stabilný a neusporiadaný. Cameronovo zlyhanie vyhrať referendum o Brexite a zabezpečiť budúcnosť Británie v EÚ prispelo k tejto neistote. Zvolenie Donalda Trumpa ju ešte ďalej zvýšilo. Toto je však identifikovateľná neistota súvisiaca so štátom. Cameron tiež poznamenal:

- „... nemôžeme si vyberať medzi konvenčnou obranou proti hrozbám na báze štátov a potrebou bojovať proti hrozbám, ktoré neuznávajú štátne hranice. Dnes čelíme obom a musíme na obe reagovať.“

Posledný bod je rozhodujúci pre porozumenie potreby vysporiadať sa s asymetrickým alebo hybridným vedením vojny, vyvolanej štátom alebo neštátnymi aktérmi. Stratégia si je vedomá jedinečnej príležitosti, raz za generáciu, transformovať spravodajskú komunitu.

- „... urobíme viac pre to, aby naše bezpečnostné a spravodajské inštitúcie mali tie zdroje a informácie, ktoré potrebujú na prevenciu a narušenie sprisahání proti tejto krajine v každom štádiu. Takže investujeme dodatočnú sumu 2,5 miliardy libier, vrátane zamestnania ďalších vyše 1900 pracovníkov a posilnenia našej siete protiteroristických expertov na Blízkom východe, v severnej Afrike, južnej Ázii a subsaharskej Afrike.“

Takže na rozdiel od vlády Camerona v roku 2010, vláda v roku 2015 sa rozhodla významne zainvestovať do spravodajskej komunity, so zameraním na terorizmus a kyberhrozby. Odráža táto investícia tie hrozby, ktorým čelíme dnes?

Cameron pridáva predvídavé varovanie:

- „**Dejiny nás učia, že žiadna vláda nedokáže prepovedať budúcnosť.** Nemáme žiadnu možnosť vedieť presne, akým smerom sa udalosti budú uberať v nasledujúcich piatich rokoch: **musíme očakávať neočakávané.** Vieme však zabezpečiť, že sme dostatočne všestranní a máme prostriedky pre reagovanie na nové riziká a hrozby pre našu bezpečnosť, tak ako vznikajú.“

Takže reaguje uvedená stratégia na túto výzvu?

- „Nachádzame sa v centre medzinárodného poriadku založeného na pravidlách. Británia je jediný štát, ktorý je stálym členom Bezpečnostnej rady OSN, NATO, Európskej únie, Commonwealthu, G7 a G 20, Organizácie pre bezpečnosť a spoluprácu v Európe (OBSE), Organizácie

pre hospodársku spoluprácu a rozvoj (OECD), Svetovej obchodnej organizácie, Medzinárodného menového fondu a Svetovej banky.“

- „Svet sa mení rýchlo a podstatne. Sme svedkami dlhodobých posunov v rovnováhe globálnej ekonomiky a vojenskej moci, zvyšujúcej sa konkurencie medzi štátmi a vzniku mocnejších neštátnych aktérov. Je stále viac pravdepodobné, že sa musíme zaoberať nečakaným vývojom.“

Veľká Británia geograficky, ekonomicky a politicky zohráva dôležitú úlohu v súčasných inštitúciách, ktoré dominujú svetovému poriadku. Pre tých, ktorí si želali ostať v Európskej únii, je táto stratégia už nesprávna, ako výsledok hlasovania o Brexite. Iní zasa argumentujú tým, že Británia sa ešte musí vyrovnáť so stratou impéria rovnako ako Rakúsko a že Británia musí povzniesť svoju národnú identitu k vyššiemu liberálno-demokratickému ideálu. Tento názor britský volič odmietol, avšak ak mnohí z tých, ktorí hlasovali za Brexit, sa pozerajú do minulosti na údajné skvelé dni ríše, tak nevnímajú realitu. Británia teraz potrebuje jasne definovať svoju medzinárodnú úlohu, v neposlednom rade v oblasti globálnej bezpečnosti. Táto stratégia bola navrhnutá za predpokladu, že vláda vyhrá referendum, mala byť však dostatočne flexibilná, aby reagovala na zmeny.

V dokumente o stratégii sú dva kľúčové odstavce, ktoré sa týkajú britských hodnôt (moje zvýraznenie -- AM)“

### „Naše hodnoty“

1.5 Spojené kráľovstvo má hrdú tradíciu ochrany svojho ľudu, podpory občianskych slobôd, udržiavania právneho štátu a **budovania rôznorodých integrovaných komunit, tolerantných k rôznym vierovyznaniam a názorom**. Naše demokratické a inkluzívne hodnoty sú základom našej bezpečnosti a prosperity. **Budeme naďalej brániť tieto hodnoty pred tými, ktorých zámerom je ich podkopanie**. Tým, ktorí chcú šíriť extrémistické ideológie v našich komunitách, zabránime v tejto činnosti.

1.6 Naša dlhodobá bezpečnosť a prosperita taktiež závisí od stabilného medzinárodného systému, ktorý zohľadňuje naše základné britské hodnoty. Demokracia, právny štát, otvorené a zodpovedné vlády a inštitúcie, ľudské práva, sloboda prejavu, vlastnícke práva a rovnosť príležitostí, vrátanie posilnenia postavenia žien a dievčat, to sú základy úspešných spoločností. Sú súčasťou zlatej nite podmienok, ktorá vedie k bezpečnosti a prosperite. Ich absencia obmedzuje príležitosti pre jednotlivca a podnecuje nespokojnosť, politickú nestabilitu a konflikty. Zabezpečenie ochrany a rešpektovania práv je podstatné pre riešenie koreňov príčin konfliktov a podporu lepšej správy vecí verejných.“

Pripúšťam, že tieto hodnoty čelili v posledných dvanástich mesiacoch viacerým výzvam, nielen v globálnom meradle, ale aj v rámci Británie. Reputácia Veľkej Británie ako tolerantnej spoločnosti je vážne ohrozená, po hlasovaní o Brexite došlo k rozdeleniu rodín i komunit a stúpajú zločiny z nenávisťi. Hodnoty stratégie 2015 sú liberálno-demokratické hodnoty. Ako podkopáva populistický trend naše schopnosti ich brániť? Čo sa stane, ak nástroje liberálnych západných demokratických spravodajských služieb sa dostanú pod kontrolu nekompromisných demagógov? V tejto stratégii sa však v prehľade hrozieb konštatuje koniec medzinárodného poriadku, založeného na pravidlách.

V skutočnosti stratégia uvádza štyri témy ohrozenia:

„Štyri osobitné výzvy budú pravdepodobne určovať bezpečnostné priority Veľkej Británie v nadchádzajúcom desaťročí. Ich dopady sú okamžité, aj dlhodobé:

- i. Rastúce ohrozenie predstavované terorizmom, extrémizmom a nestabilitou.
- ii. Obnovenie ohrozenia na báze štátov a zintenzívnenie širšej konkurencie štátov.
- iii. Vplyv technológií, najmä kyberhrozieb; širší technologický rozvoj.
- iv. Rozpad medzinárodného poriadku založeného na pravidlách, tým je ťažšie dosiahnuť konsenzus a riešiť globálne hrozby.“

7. Národná bezpečnostná rada triedi domáce a zahraničné riziká do troch úrovní, **na základe zváženia kombinácie pravdepodobnosti a dopadu**. Nie je to teda jednoduché poradie ich dôležitosti.

V prílohe Národná bezpečnostná rada klasifikuje riziká nasledovne:

### ÚROVEŇ 1

<b>TERORIZMUS</b> Útoky na obyvateľov VB a ľudí iných národností vo VB a ich radikalizácia
<b>MEDZINÁRODNÝ VOJENSKÝ KONFLIKT</b> VB zaangažovaná do konfliktu medzi štátnymi a neštátnymi aktérmi
<b>KYBER útoky ovplyvňujúce VB a naše záujmy</b>
<b>VEREJNÉ ZDRAVIE</b> Závažná zdravotná kríza pre ľudí
<b>ZÁVAŽNÉ PRÍRODNÉ OHROZENIA</b> Udalosti, ktoré si vyžadujú celonárodnú reakciu (napr. veľké povodne)
<b>NESTABILITA V ZAHRANIČÍ</b> Závažná nestabilita vytvárajúca hrozby pre VB a naše záujmy

### ÚROVEŇ 2

<b>ÚTOKY A TLAK NA SPOJENCOV</b> Konvenčné a/alebo hybridné útoky
<b>ROZPAD A ZLYHANIE KLÚČOVÝCH INŠTITÚCIÍ</b> Nejednotnosť alebo obmedzenia
<b>ÚTOK „CBRN“</b> Útok s použitím chemických, biologických, radiologických alebo nukleárných zbraní (CBRN)
<b>PROLIFERÁCIA ZBRANÍ</b> Zvýšenie počtu iných pokročilých konvenčných zbraní alebo CBRN technológie
<b>ZÁVAŽNÝ A ORGANIZOVANÝ ZLOČIN</b> Účinok organizovaného zločinu
<b>FINANČNÁ KRÍZA</b> Účinok medzinárodnej finančnej krízy
<b>NEPRIATEĽSKÁ ZAHRANIČNÁ AKCIA</b> Činy namierené proti vláde alebo ekonomickým záujmom VB

### ÚROVEŇ 3

<b>VOJENSKÝ ÚTOK na VB, námorské teritória alebo základne</b>
<b>DODÁVKY PALIVA – ich narušenie alebo cenová nestabilita</b>
<b>ÚNIKY RADIÁCIE ALEBO CHEMIKÁLÍ -- zámerné úniky alebo nehody</b>
<b>NEISTOTA ZDROJOV – narušenie dodávok zo zahraničia (napr. potravín, nerastných surovín, etc.)</b>
<b>NARUŠENIE VEREJNÉHO PORIADKU – rozsiahle verejné nepokoje</b>
<b>POČASIE A INÉ PRÍRODNÉ HROZBY – ako závažné horúce alebo studené vlny</b>
<b>ENVIROMENTÁLNE PRÍHODY – ako ochorenia zvierat alebo závažné znečistenie ovzdušia</b>

Takže, čo to všetko znamená dnes pre spravodajské a bezpečnostné služby? Národná bezpečnostná rada jasne definovala hrozby a riziká, ktorým čelíme. Toto rigorózne stanovenie priorit iba sotva možno spochybniť.

Rada poskytla štruktúru na riadenie programov zmien v rámci komunity. Služby si musia plánovať svoj rast a porozumieť tomu, ako pôsobiť v zmenenom svetovom poriadku. Napadajú ma dve témy: stanovenie priorit a politika. Požiadavky kladené na služby vychádzajú z hodnotení rizík a priorit Národnej bezpečnostnej rady, je však vo svete oveľa viac práce, ako sa dá úspešne zvládnuť. To si od lídrov vyžaduje, aby svojim organizáciám poskytli jasné a ciele zameranie.

Politika je teraz zložitejšia. Ako sa menia politické priority v stále populistickesom svete? Prichádza ohrozenie od extrémne pravicových skupín alebo od tých, ktorí sa cítia vylúčení domácim volebným procesom? Prezident Trump za riaditeľov NSA a CIA menoval zástancov tvrdej línie. To by mohlo ovplyvniť medzinárodnú spoluprácu, keďže štáty, ktoré stále uznávajú liberálno-demokratické hodnoty, považujú spoluprácu za nezákonnú alebo neetickú. Na druhej strane dejiny nás učia, že spravodajské komunity sa dokážu prispôbiť vládam, ktoré im vládnu. Tou obavou, ktorú do stredu pozornosti vniesol Edward Snowden, je – čo ak právomoci „všesledujúceho“ štátu padnú do rúk súčasného Hitlera?

Toto je výzva pre Národnú bezpečnostnú stratégiu. I keď predpokladá rozpad medzinárodného poriadku založeného na pravidlách, vychádza z hodnôt, ktoré čelia výzvam stále rastúceho populistického elektorátu. Pri tom, ako vchádzame do veku populizmu, ako sa vyrovnajú bezpečnostní a spravodajskí dôstojníci v sebe s prácou pre politických lídrov, ktorých názory sú také extrémne? Toto je výzva, ktorej budú čeliť naši americkí kolegovia v januári. V nasledujúcich rokoch by sa to však mohlo stať v Európe hocikomu z nás.

## R. Lami: Transparentnosť a spravodajské služby

**Roman Lami** (1962) - Plk. v. v. absolvoval VPA v Bratislave (1986) a doktorandské štúdium v odbore národná a medzinárodná bezpečnosť na Akadémii ozbrojených síl v Liptovskom Mikuláši (2010). Postgraduálne štúdium v odbore filozofia - história na VVPŠ v Bratislave (1990-1992). Absolvoval tiež kurzy venované bezpečnostnej problematike v Marshall Centre v NSR (1999) a na Národnej univerzite obrany v Číne (2005). V období 1993 - 2008 pôsobil na Ministerstve obrany SR v oblasti bezpečnostnej a obrannej politiky a tiež ako spravodajský analytik vojenskej rozvedky. V súčasnosti pôsobí v mimovládnom sektore

*Motto: „Bezpečnosť a tajné služby sú služby, ktoré sa nesmú komentovať na verejnosti“  
A.Danko (Plus 7 dní, 29. októbra 2016)*

### • Nesúlads pojmov

Transparentnosť a spravodajské služby sú pojmy, ktoré nebývajú veľmi často používané spoločne. Spôsob práce spravodajských služieb je v priamom protiklade s tým, čo si predstavujeme pod transparentnosťou. Napriek tomuto rozporu sa aj v činnosti niektorých spravodajských služieb cielene objavuje snaha o transparentnosť, pri zachovaní všetkých pravidiel fungovania služieb.

### • Ponímanie transparentnosti v kontexte práce spravodajských služieb (možné východisko)

- Transparentnosť neznamená otvorenie spravodajskej služby verejnosti, transparentnosť znamená umožnenie verejnosti participovať na niektorých/možných výsledkoch práce spravodajských služieb

### A SÚČASNE

- Transparentnosť umožňuje spravodajským službám spolupracovať s civilným sektorom a využívať jeho skúsenosti a poznatky pre svoju činnosť.
  - Je to proces, ktorý priblíži (čiastočne otvorí) spravodajské služby verejnosti pri zachovaní všetkých základných atribútov ich činnosti (plnenie úloh, utajenie a pod.)
- 
- **Zmenené operačné prostredie - nové podmienky pre prácu**
    - Prostredie práce spravodajských služieb nie je statické a neustále sa vyvíja. Je preto nutné prispôbovať prácu služieb zmenám reality.
    - Okrem iných zmien, ktorým z hľadiska obmedzeného rozsahu tohto príspevku nebude venovaná pozornosť, ide najmä o zásadnú zmenu z hľadiska aktérov. Oproti minulému obdobiu nie je aktérom najmä štát, ale aj skupiny nadnárodné i národné (finančné, mediálne, priemyselné, teroristické a pod.), ale tiež jednotlivci (najmä v rámci kybernetického priestoru má aj jednotlivec potenciál relevantného aktéra).
    - Zmenil sa vzťah informácie a faktu ako prvku reality. Časť informácií už nie je vyjadrením reality, nositeľom poznania, ale naopak informácie sa usilujú realitu vytvárať. Nie je dôležité, či informácia má vzťah ku skutočnosti, ale je dôležité, aký dopad bude informácia mať.
    - Kybernetické prostredie súčasnosti umožňuje nekontrolované šírenie akýchkoľvek informácií a jedným zo zásadných kritérií dopadu informácií na



spoločnosť je kredibilita nositeľa informácií. Kredibilita nositeľa je subjektívna kvalita, ktorú priraduje prijímateľ často na základe iracionálnych podnetov.

- **Dopady uvedených zmien**

- Tieto, ale aj ďalšie aspekty vyvolávajú potrebu zaistenia a udržania dôveryhodnosti všetkých, ktorí sú (vo verejnom a štátnom zaujme) nositeľmi informácií.
- Pasivita je z tohto pohľadu negatívna, pretože ponecháva priestor na informovanie iným.
- Informačná záplava tak vyvoláva otázku, ako sa dotýka činnosti spravodajských služieb - a to nielen do vnútorného fungovania služieb, ale aj pôsobenia spravodajských služieb vo verejnom priestore. Určitým spôsobom ide o celkom nové informačné konkurenčné prostredie, v rámci ktorého spravodajské služby budú musieť potvrdzovať svoj význam nielen smerom k politikom, ale aj k verejnosti.
- Predstava, že raz za čas spravodajská služba vystúpi z tieňa a prinesie možno aj dôležitú informáciu a táto bude adekvátne rezonovať je pravdepodobne nesprávna, pretože informačný priestor už bude rozdelený a prijímateľa informácií už majú svoje dôveryhodné zdroje.
- Samozrejme, že prvotným adresátom spravodajských informácií sú politické elity. Ale ani tieto nežijú mimo spoločnosť a informačná záplava ich taktiež ovplyvňuje. A taktiež politické elity sú možnými prostredníkmi medzi spravodajskou službou a obyvateľstvom a v konečnom dôsledku ide o vzájomne prepojený vzťah

- ❖ **Transparentnosť spravodajských služieb**

- Prioritná úloha pre služby zostáva nezmenená - poskytovanie relevantných a hodnoverných informácií oprávneným užívateľom/politikom
- Súbežne s procesom tvorby týchto informácií, ktoré z hľadiska svojho zdroja alebo významu majú väčšinou utajovaný charakter, môžu vznikajú „vedľajšie“ produkty, ktoré nie je nutné utajovať a ktoré sú verejne/otvorene využiteľné a spoločensky potrebné
- Cieľ transparentnosti
  - Prezentovať spravodajské služby ako súčasť spoločnosti
  - Podpora plnenia niektorých úloh spoločnosti
  - Získanie dôveryhodnosti, verejnej podpory a spoločenskej akceptovateľnosti
  - „Spravodajsko-politický vzťah“- služby dokazujú politikom svoj význam a politici získavajú argumenty pre verejnosť pri odôvodňovaní financovania/podpory spravodajských služieb (prírodné pohromy - príklady z USA)
- Prístupy
  - Základný/východiskový - web stránka, sociálne siete - rozšírený
  - Systémový - transparentnosť spravodajských služieb ako jeden z oficiálnych a deklarovaných prvkov ich činnosti (USA)
- Riziká  
transparentnosť versus utajenie - informovanie verejnosti znamená aj informovanie protivníka, **ale** zverejnenie niektorých informácií o úspechoch, odhalení môže pôsobiť ako psychologický faktor odstrašenia

- ❖ **Systémový prístup - USA**

- Po svojom nástupe do úradu prezidenta USA v roku 2009 Barack Obama podpísal **Memorandum o transparentnosti a otvorenej vláde (*Memorandum on Transparency and Open Government*)** a v októbri 2009 vydal **Nariadenie o otvorenej vláde (*Open Government Directive*)**. Táto direktíva požaduje, aby federálne orgány, vrátane spravodajskej komunity, uskutočnili konkrétne kroky k dosiahnutiu transparentnosti a spolupráce vo vzťahu k verejnosti.
- Vo svojom prejave o národnej bezpečnosti 17. januára 2014 Obama uviedol, že spravodajská komunita si musí zachovať dôveru amerického ľudu a zrealizovať reformné programy a postupy na zabezpečenie väčšej transparentnosti.
- V tom istom roku prijatá **Národná spravodajská stratégia (*2014 National Intelligence Strategy*)**, ktorá hovorí o „pokračovaní implementácie prístupov, ktoré poskytujú zodpovedajúcu transparentnosť.“
- Vo februári 2015 riaditeľ Národného spravodajstva USA vydal **Princípy spravodajskej transparentnosti pre spravodajskú komunitu (*The Principles of Intelligence Transparency for the Intelligence Community*)**. Boli stanovené štyri základné princípy:
  - a) Uskutočňovať vhodnú transparentnosť vo vzťahu k zvýšeniu verejného porozumenia o spravodajskej komunite.
  - b) Byť aktívnejší a prehľadnejší pri zverejňovaní informácií pre verejnosť.
  - c) Chrániť informácie o spravodajských zdrojoch, metódach a aktivitách.
  - d) Usmerniť poslanie spravodajskej komunity, procesy a činnosti na podporu zavádzania transparentnosti.
- Tieto zásady majú uľahčiť rozhodovanie v oblasti sprístupňovania spravodajských informácií verejnosti spôsobom, ktorý zvyšuje verejné povedomie o spravodajskej činnosti a zároveň zabezpečuje ochranu informácií a zabraňuje poškodeniu národnej bezpečnosti.
- Transparentnosť vyžaduje inštitucionalizovaný, strategicky orientovaný a koordinovaný prístup v rámci spravodajskej komunity, ktorý umožní zvýšenie povedomia verejnosti o spravodajskej komunite a jej činnosti pri zaistení národnej bezpečnosti.
- Transparentnosť vyžaduje nielen adekvátne reagovať na sprístupňovaní informácií podľa zákona, ale taktiež sprístupňovať informácie s využitím rôznych verejne prístupných kanálov.
- Spravodajská komunita by mala komunikovať s verejnosťou prostredníctvom tradičných, ako aj sociálnych médií, priamou komunikáciou s externými účastníkmi procesov, účasťou na akademických a ďalších konferenciách a tiež s využitím iných komunikačných prostriedkov.
- Prioritnou úlohou naďalej zostáva poskytovanie včasných a spoľahlivých informácií pre potreby zaistenia národnej bezpečnosti a s tým súvisiaci ochrana zdrojov a informácií pred neoprávneným zverejnením. Je preto nutné nájsť rovnováhu medzi transparentnosťou a plnením úloh spravodajskej komunity v prospech národnej bezpečnosti.
- Zatiaľ posledným krokom v tomto procese bola charta nového orgánu spravodajskej komunity USA - **Rady spravodajskej transparentnosti (*Intelligence Transparency Council*)**, ktorú riaditeľ Národného spravodajstva USA James Clapper podpísal 5. apríla 2016.
  - Rada sa skladá zo zástupcov každej zo 17 spravodajských agentúr Spojených štátov.

- Jej úlohou je identifikovať a presadzovať vhodné možnosti a oblasti transparentnosti spravodajských služieb

#### ❖ Realizácia – príklady a prístupy

- Informovanie o činnosti (Sprístupňovanie odtajnených dokumentov, správy o činnosti)
  - Vystúpeniach na konferenciách (J.Clapper)
  - Rozhovory v médiách (riaditeľ MI6 v októbri 2016 poskytol obsiahly rozhovor)
- Spolupráca medzi CIA a klimatológmi - CIA umožnila prístup vedcom k získaným údajom zo satelitov a rôznych senzorov, ktoré zachytávajú informácie o prírodných javoch a naopak využíva vedecké poznatky, napríklad o rozširovaní púšti, zvyšovaní hladiny oceánov a podobných javov, ktoré majú potenciálne bezpečnostné dopady.
- Geospatial intelligence (GEOINT) – sprístupňovanie mapových a geografických informácií:
  - od septembra 2015 - informácie o Arktíde – 3D zobrazenie povrchu, námorné trasy, viacvrstvé mapy, zóny ľadu a podobne.
  - pri boji s Ebolou (2015). Sprístupnenie mapových a geografických informácií o Afrike. Medzinárodný Červený kríž, ako aj ďalšie humanitárne organizácie tak získali aktuálne informácie o osídlení, cestách, prírodných prekážkach a podobne, ktoré o niektorých oblastiach Afriky boli nedostatočné.
  - zemetrasenie v Nepále, záplavy v Luisiane, hurikán Mathews apod.
  - Poskytovanie geografických informácií na podporu boja proti nedovolenému obchodu s voľne žijúcimi zvieratami (najmä v Afrike).
- Vytváranie platforiem na spoluprácu:
  - National Intelligence Council (od roku 1979) - výstup - Global Trends Report (spolupráca spravodajskej, politickej a akademickej sféry so súkromným sektorom)
  - The Intelligence National Security Alliance (INSA)  
Mimovládna organizácia, súkromný, verejný, akademický, štátny sektor.  
"Spravodajská komunita by mala rozšíriť svoje kontakty s osobami mimo oblasti spravodajstva tým, že vytvorí aspoň jeden neziskový podporovaný výskumný ústav." (*Komisia o spravodajských spôsobilostiach Spojených štátov týkajúcich sa zbraní hromadného ničenia, 31. marca 2005*)
  - Program ENGAGE - spustenie programu na začiatku 2016, podporuje rast vnútorného znalostí a schopností umiestnením zamestnanca NGA v dočasných pozíciách v priemysle a akademickej sfére. Program tiež ponúka priviesť náprotivky do agentúry s cieľom vyvinúť nové spôsoby schopnosť riešiť problémy a zlepšiť obchodné praktiky k ďalšej inovácii.
- Výstavy - vo Francúzsku aktuálne prebieha výstava „Tajné vojny“, oficiálnym partnerom výstavy je DGSE
- Súťaže – DGSE je oficiálnym partnerom mládežníckej súťaže v dešifrovaní
- Napríklad aj FSB informuje o úspešných akciách, udalosti z histórie, upozornenie na zaujímavé knihy, novinové články a pod.
- Bieloruská KGB je spoluorganizátorom medzinárodnej vedecko-odbornej konferencie: „Príprava kádrov pre národné bezpečnostné služby: História a súčasnosť“.

## ❖ **Závery**

- Transparentnosť, respektíve zvyšujúca miera otvorenosti je významným trendom v činnosti spravodajských služieb.
- Nástroj na podporu fungovania spoločnosti (podpora plnenia úloh verejnej, súkromnej aj akademickej sféry).
- Je to možný nástroj na zvyšovanie kredibility, dôveryhodnosti vo vzťahu k verejnosti, ale aj politikom.
- Spolupráca s civilným sektorom môže byť využitá aj v prospech spravodajských služieb (kontakt s akademickou sférou, manažment apod.).
- Transparentnosť je možný prístup, nie je nutnou a všeobecnou normou.

## R. Kusenda: Výzvy pre spravodajskú komunitu v kontexte hybridných hrozieb

**Radoslav Kusenda** (1970) - Po absolvovaní Filozofickej fakulty Univerzity Komenského v Bratislave (1994) nastúpil na Ministerstvo zahraničných vecí SR; Pôsobil na zastupiteľskom úrade v Moskve (1998-2002) a potom v slovenskej Stálej delegácii NATO v Bruseli (2005-2009 a 2012-2016). Bezpečnostnej problematike sa systematicky venuje od roku 2004; absolvoval viacero kurzov na NATO Defence College a Marshall European Center for Security Studies v Garmisch-Partenkirchene. Aktuálne sa venuje príprave bezpečnostnej stratégie Slovenskej republiky na Odbore bezpečnostnej politiky MZV a EZ SR.

Popri klasických vojenských konfliktoch v súčasnosti, stále viac do popredia vystupujú konfrontácie s použitím hybridných prvkov. Hybridné hrozby však nepredstavujú prevratnú zmenu vo vojenskom strategickom zmýšľaní. Predstavujú komplex politických, informačných, vojenských, ekonomických, finančných, spravodajských a právnych nástrojov\*, ktoré sa využívajú či už v priebehu konfliktu, alebo dlhodobo, podprahovo s cieľom dosiahnuť oslabenie integrity protivníka.

Zvýšenú pozornosť venujeme téme najmä od začiatku konfliktu na Ukrajine v roku 2014, keď Ruská federácia využila celé spektrum hybridných nástrojov na paralyzovanie/rozloženie bezpečnostných zložiek a následné obsadenie Krymu a rozpútanie separatistického konfliktu na východnej Ukrajine. Treba na tomto mieste podčiarknuť, že aplikovateľnosť hybridných nástrojov je unikátna a nedá sa univerzálne použiť na všetky vojenské a spravodajské operácie. Kritériami na efektívne použitie hybridných nástrojov je slabý štát, znefunkčnené bezpečnostné a obranné zložky kontaminované cudzou mocou, cielená propaganda a mediálna kampaň zameraná na získanie obyvateľstva a silné sociálne a humanitárne nástroje v zálohe.

Ruská asertívna vojenská politika, podporená doktrínami a masívna mediálna kampaň zameraná na obyvateľstvo členských krajín Európskej únie a NATO vytvorili podmienky pre odôvodnené úvahy o cieľoch ruskej politiky. Členské krajiny NATO si pomerne rýchlo uvedomili, že je dôležité mať vybudovaný systém včasnej identifikácie hybridných hrozieb, osobitne na východnom krídle aliancie. Ukázalo sa totiž, že spravodajské služby neboli schopné rýchlo identifikovať rozmer a závažnosť prebiehajúcich procesov na Ukrajine. Rovnako si spojenci uvedomili, že rozhodovací proces aliančného krízového riadenia (nemusí hneď ísť o invokáciu čl.5) je neúmerne dlhý a skrýva v sebe mnoho nejednoznačností.

Jedným zo znakov hybridných operácií je fakt, že prebiehajú podprahovo a málokedy je možné ihneď s istotou určiť, kto ich iniciuje a aký majú cieľ. Práve táto nejednoznačnosť kombinovaná s pomalým politickým rozhodovacím procesom oslabovaným ešte aj nejasnou podporou časti obyvateľstva sa javí ako cieľ hybridných operácií protivníka.

Aliančné diskusie vyvrcholili prijatím *Strategy on NATO's Role in Countering Hybrid Warfare* (Stratégia úlohy NATO v boji proti hybridnej vojne) ministrami

---

\* DIMEFIL – Diplomatic/Political, Information, Military, Economic, Financial, Intelligence, Legal.

zahraničných vecí NATO v decembri 2015.\* Následne ministri obrany NATO v balíku dokumentov pripravovaných pre summit vo Varšave schválili v júni 2016 *Implementation Plan for the Strategy on NATO's Role in Countering Hybrid Warfare*.† (Realizačný plán stratégie úlohy NATO v boji proti hybridnej vojne).

Možné postupy aliancie v prípade hybridných hrozieb namierených voči členským štátom boli diskutované a precvičené v NATO už niekoľkokrát, predovšetkým v rámci cvičenia krízového manažmentu CMX (Cvičenie krízového manažmentu - Crisis Management Exercise). Doterajšie diskusie aj cvičenie ukázali hlavný problém spojený s „hybridnou“ hrozbou, t.j. problém identifikácie „thresholdu“ – prahu, pri prekročení ktorého možno jednoznačne určiť, že došlo k napadnutiu spojencov, a teda k situácii podľa článku 5 Severoatlantickej zmluvy.

Výsledkom spoločného úsilia a rokovaní spojencov bol nakoniec text varšavského komuniké, kde sa konštatuje dôležitosť čeliť hybridným hrozbám‡. Povšimnutiahodnými sú odkazy na pripravenosť aliancie pomáhať spojencom čeliť akejkoľvek fáze hybridnej hrozby a takisto odkaz na čl. 5 Washingtonskej zmluvy, ktorý môže byť invokovaný aj v kontexte hybridnej hrozby.

Jednou z prvých vecí, ktorú spojenci iniciovali po vzniku ukrajinskej krízy boli kroky na posilnenie východného krídla NATO (Wales - *Readiness Action Plan* (Akčný plán pripravenosti), Varšava - *Enhanced Forwarded Presence* (Zvýšená predsunutá prítomnosť) a súčasne pokračovanie reformy spravodajských zložiek v NATO§. Toto úsilie vyvrcholilo na jeseň 2016 vytvorením novej spravodajskej divízie – DSI (*Division on Intelligence*). Cieľom bolo dosiahnuť, aby civilné a vojenské spravodajské služby úzko kooperovali a koordinovali svoju činnosť. Úlohou novej divízie je tiež poskytovať komplexné a jednotné spravodajské výstupy Spravodajskej jednotky (*Intelligence Unit*) syntetizujúcej civilné a vojenské spravodajstvo\*\*. Súčasťou tejto divízie je aj fyzická ochrana objektov a personálna bezpečnosť. Keďže divízia existuje len niekoľko týždňov, bolo by predčasné hodnotiť efektivnosť tohto kroku a činnosť jej nového šéfa *Arndt Freytag von Loringhoven*a, osobitne ak nastúpil do funkcie až 1. decembra 2016. Každopádne, stáli predstavitelia pri Severoatlantickej rade už nebudú musieť osobitne venovať pozornosť výstupom civilného a osobitne vojenského spravodajcu.

---

\* <http://www.natolibguides.info/hybridwarfare>

† <http://www.natolibguides.info/hybridwarfare>

‡ *Para 72. We have taken steps to ensure our ability to effectively address the challenges posed by hybrid warfare, where a broad, complex, and adaptive combination of conventional and non-conventional means, and overt and covert military, paramilitary, and civilian measures, are employed in a highly integrated design by state and non-state actors to achieve their objectives. Responding to this challenge, we have adopted a strategy and actionable implementation plans on NATO's role in countering hybrid warfare. The primary responsibility to respond to hybrid threats or attacks rests with the targeted nation. NATO is prepared to assist an Ally at any stage of a hybrid campaign. The Alliance and Allies will be prepared to counter hybrid warfare as part of collective defence. The Council could decide to invoke Article 5 of the Washington Treaty. The Alliance is committed to effective cooperation and coordination with partners and relevant international organisations, in particular the EU, as agreed, in efforts to counter hybrid warfare.*

§ [http://nato.int/cps/en/natohq/opinions\\_136414.htm?selectedLocale=en](http://nato.int/cps/en/natohq/opinions_136414.htm?selectedLocale=en)

\*\* Veľa sa diskutovalo o vytvorení tejto divízie aj v kontexte americkej kritiky o nedostatočnej pozornosti NATO boju proti terorizmu, čo narážalo na silný odpor viacerých spojencov, ktorí by túto úlohu radi prenechali EÚ.

Pre politické rozhodovanie NATO je to dôležitý krok vpred\*. Čo sa však nemení, je princíp práce aliančných spravodajcov, ktorí sa musia spoliehať iba na príspevky národných agentúr, z ktorých sa generuje každoročný civilný *Joint Threat Assessment (Spoločné vyhodnotenie hrozieb)* a vojenský *MC161 (Military Committee dokument č. 161 - Vojenské hodnotenie hrozieb)*. Oba dokumenty predstavujú *agreed language – dohodnutú komunikáciu* spravodajskej komunity, ktorý by mal byť referenčným odkazom pre úvod politického rozhodovacieho procesu v NAC (Severoatlantickej rade). Je otázne, akú úlohu budú tieto dva kľúčové dokumenty zohrávať v budúcnosti, či nedôjde k ich zjednoteniu, či sa nebude v kontexte neustále meniaceho sa bezpečnostného prostredia venovať dôraz skôr na *ad hoc* pripravované správy a hodnotenia. Systém separátnych spravodajských konferencií k špecifickým témam je určite krokom vpred.

Európska únia podobne vníma urgenciu hybridných hrozieb ako NATO. V júli 2015 bol prijatý *Joint Staff Working Document - EU Operational Protocol for Countering Hybrid Threats 'EU Playbook'*.<sup>†</sup> (Pracovný dokument spoločného štábu – Operačný protokol EU pre boj proti hybridným hrozbám – „Manuál EU“). Je to odpoveď na synchronizáciu postupu EU a NATO, kde obe organizácie vypracovali svoje vlastné manuály (*playbooky*). Tu však treba povedať, že ide o dokument pripravený Európskou komisiou a členské štáty ho zatiaľ neprijali do svojho *acquis*. Na základe tohto dokumentu bol vytvorený *EU Hybrid Fusion Cell* (Integrovaná jednotka zameraná proti hybridným hrozbám)<sup>‡</sup> v rámci *EU Intelligence and Situation Center* (EU INTCCEN - Spravodajské a situačné centrum) pri EEAS (Európska služba pre vonkajšie činnosti). *EU Hybrid Fusion Cell* je styčným bodom na spravodajské vstupy týkajúce sa možných hybridných hrozieb. Má za úlohu vyhodnocovať podozrivé incidenty a informuje o strategických rozhodovacích procesoch orgány EÚ. V súčasnosti prebieha proces jeho etablovania, ktorý má dosiahnuť plnú operačnú schopnosť v júni 2017. Bol iniciovaný proces, podľa ktorého členské krajiny majú nominovať svoje kontaktné osoby ako v Bruseli (veľvyslanec SR pri PSC – Politický a bezpečnostný výbor), tak aj v ústredí.

Aktivity EÚ a NATO však na tejto úrovni nekončia. Obe organizácie sú si vedomé, že predpokladom, ako úspešne čeliť hybridným hrozbám, je ich spolupráca a koordinácia. Vyplýva to ako z mandátov oboch inštitúcií, tak aj z povahy samotnej hrozby, ktorá nemá jasne definovaný charakter v civilnej, či vojenskej oblasti. Jedným z konkrétnych výstupov oboch inštitúcií sú koordinované manuály, tzv. *playbooks*, ktoré boli v oboch inštitúciách cirkulované v máji 2016. Návrhy oboch dokumentov sú takmer identické a zameriavajú sa na štyri oblasti spolupráce: (a) Včasné varovanie/

---

\* Problematika formovania novej divízie má viacúrovňovú dimenziu, okrem fúzovania civilnej a vojenskej zložky boli problematické inštitucionálne aranžmány. Napr. NOS (*NATO Office of Security*) má na starosti aj fyzickú a objektovú bezpečnosť, ktorá mala zostať mimo štruktúry novej divízie; nie je zrejmé, ako sa vyriešila otázka fungovania *NATO Steering Board for Intelligence*, ktorá fungovala pod zástupcom generálneho tajomníka A. Vershbowom. Všeobecne A. Vershbow (vo funkcii do 15.10.2016) mal na starosti celú reformu spravodajského sektora NATO. Príchodom novej zástupkyne generálneho tajomníka R. Gotemoeller a vymenovaním nového šéfa spravodajskej divízie o budúcnosti tohto orgánu nie je zatiaľ nič známe.

† <http://statewatch.org/news/2016/jul/eu-com-countering-hybrid-threats-playbook-swd-227-16.pdf>

‡ *EU HYBRID FUSION CELL* - je to útvar, ktorý získava analýzy a zdieľa utajené informácie i informácie z otvorených zdrojov týkajúce sa indikátorov a varovaní súvisiacich s potenciálnymi hybridnými hrozbami od rôznych aktérov v rámci Európskej služby pre vonkajšie činnosti (vrátane delegácií EÚ), služieb Komisie, úradov EÚ a členských štátov EÚ. V súčinnosti s existujúcimi podobnými útvarmi v EU, ako aj na národnej úrovni *Fusion Cell* analyzuje vonkajšie aspekty hybridných hrozieb ovplyvňujúcich EÚ a jej okolie.

Situačné povedomie (Informovanosť o situácii); b) Strategické komunikácie; c) Kybernetická bezpečnosť; d) Civilná a vojenská pripravenosť a reakcia.

Tento predbežný výsledok intenzívnejšej komunikácie v podobe „hybridných manuálov“ možno považovať za historický a prelomový v spolupráci oboch inštitúcií. Pochopiteľne, podstatná bude spolupráca v implementácii manuálov. Je možné predpokladať, že v nej bude istú prekážku predstavovať absencia právneho rámca na výmenu klasifikovaných informácií medzi NATO a EÚ (ten sa roky nedarí dosiahnuť predovšetkým v dôsledku problému v „trojuholníku“ Turecko-Grécko-Cyprus) a tiež viac ako zdržanlivé postoje niektorých členských štátov, najmä v EÚ. Tesne pred júlovým summitom vo Varšave sa podarilo dosiahnuť podpis spoločnej deklarácie medzi EÚ a NATO o vzájomnej spolupráci. Dokument identifikuje vyššie spomenuté štyri oblasti definujúce záber boja voči hybridným hrozbám\*. Cieľ tejto deklarácie je vytvorenie efektívneho mechanizmu koordinácie medzi EÚ a NATO, zameraného na zdieľanie spravodajských informácií, vylepšenie krízových manuálov a do budúcnosti aj možných spoločných cvičení zameraných na boj proti hybridným hrozbám. Teraz v decembri, počas zasadnutia ministrov zahraničných vecí NATO, očakávame diskusiu, ako túto spoluprácu posilniť. V tomto kontexte, slovenské predsedníctvo uskutočnilo 25. októbra 2016 expertný seminár o boji EÚ a NATO proti hybridným hrozbám. Prvý panel bol venovaný zdieľaniu informácií a situačnému povedomiu (*situational awareness*); druhý strategickej komunikácii a tretí posilneniu odolnosti našich partnerov.

Slovenský právny poriadok nepozná pojem hybridnej vojny. Ochrana pred hybridnými útokmi alebo reakcia na ne je zakotvená v rôznych právnych predpisoch. Keďže hybridné útoky sa z hľadiska práva konajú v čase mieru a často nevojenskými prostriedkami, v prvom rade sa nimi zaoberá MV SR.

Zatiaľ jediný dokument schválený vládou SR, ktorý hybridným hrozbám venuje väčšiu pozornosť, je paradoxne z vojenského prostredia - Biela kniha Ministerstva obrany schválená vládou SR v septembri 2016<sup>†</sup>. Z hľadiska vedenia konfliktu sú však ozbrojené zložky poslednou inštitúciou, ktorá nastupuje na scénu. Hybridné hrozby by mali byť predmetom záujmu predovšetkým spravodajských, policajných a protiteroristických zložiek.

---

\* Boost our ability to counter hybrid threats, including by bolstering resilience, working together on analysis, prevention, and early detection, through timely information sharing and, to the extent possible, intelligence sharing between staffs; and cooperating on strategic communication and response. The development of coordinated procedures through our respective playbooks will substantially contribute to implementing our efforts. Zdroj: [http://www.nato.int/cps/en/natohq/official\\_texts\\_133163.htm](http://www.nato.int/cps/en/natohq/official_texts_133163.htm)

<sup>†</sup> 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** (Koncept). Základné myšlienky definované 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 operácií“ použitý.



V oblasti prevencie je to zložitejšie. Jednou z možných odpovedí je vierohodne koncipovaná a realizovaná strategická komunikácia štátu (vlády) ako voči obyvateľstvu, tak voči protivníkovi. Jej úlohou vo vzťahu k spoločnosti je posilňovanie jej odolnosti a uistenie o pripravenosti štátu zaistiť bezpečnosť svojich občanov a demokratického zriadenia. Odolnosť spoločnosti stojí na zdieľaní rovnakých hodnôt a vôle ich chrániť, na občianskom uvedomení a solidarite. Posilňovanie tejto odolnosti je predmetom dlhodobej spoločenskej a politickej diskusie a vzdelávania. Vzhľadom na to je pomerne zložité pokúšať sa definovať priestor na uplatňovanie nejakých špecifických nástrojov na zaistenie bezpečnosti voči hybridným hrozbám. Vo vzťahu k protivníkovi je úlohou strategickú komunikáciu vlády demonštrovať pripravenosť, schopnosť a odhodlanie brániť občana, štát a hodnoty, na ktorých stojí. Súčasťou takéhoto odhodlania by malo byť aj posilňovanie spojeneckých väzieb, osobitne v rámci transatlantického vektora.

Použitie propagandy a dezinformácií ako súčasti hybridnej kampane treba vnímať tak, že poškodzujú záujmy a bezpečnosť štátu a obyvateľstva. Informačné kanály, sociálne siete, ktoré propaganda a dezinformačné kampane využívajú, je potrebné sledovať a vyhodnocovať nepretržite. Toto je jeden z priestorov činnosti spravodajských služieb, nielen civilných, ale aj vojenských (osobitne potom ako NATO vo Varšave uznalo kybernetický priestor za ďalšiu bojovú doménu).

V kontexte formovania Bezpečnostnej stratégie SR je potrebné si položiť otázku, ako je štát pripravený čeliť hybridným hrozbám z inštitucionálneho hľadiska. Ako sa už skôr konštatovalo, hlavnú úlohu zohrávajú rezorty vnútra a obrany a spravodajské služby. Neexistujú pochybnosti, že príslušné zložky majú dostatok zdrojov, materiálnych a ľudských na riešenie transparentných prejavov hybridných aktivít. Otázne je, ako je podchytená prevencia, čím sa myslí predovšetkým vzdelávanie a formovanie bezpečnostného povedomia na školách, ako je riešená otázka komunikácie a zdieľania kritických informácií medzi jednotlivými zložkami silových a spravodajských štruktúr štátu. Ako príklad možno použiť nedostatočnú konektivitu medzi ústrednými orgánmi štátnej správy v utajenom svete a ich prepojenie s centrálnymi v Bruseli.

Dôležitou zostáva otázka vzdelávacieho systému a jeho úloha na formovaní bezpečnostného povedomia mladých ľudí na internete a schopnosť kriticky pracovať s informáciami na internete a sociálnych sieťach. Existujú dve školy výkladu tohto problému. Prvá - evolučná - ponecháva túto možnosť na ľuďoch samotných. Hlavným argumentom je to, že aj v čase pred rokom 1989 ľudia vedeli rozlišovať medzi oficiálnou propagandou a napr. Hlasom Ameriky. Druhá škola interpretuje súčasné prostredie ako zložitejšie, kde sú informácie rýchlejšie a dostupnejšie. To je hlavný dôvod, prečo by sa mal štát venovať posilňovaniu odolnosti obyvateľstva nepodliehať konšpiračným a nepravdivým kampaniam na internete. Tu nehovoríme len o politických konzekvenciách - ako boli teraz voľby v USA, ale napríklad aj o protiočkovacích kampaniach, ktoré môžu mať dopad na zdravie populácie. Ministerstvo školstva v otázke prevencie zatiaľ ponúka pomerne skromné výsledky a dá sa očakávať, že navrhovaná koncepcia Národného programu rozvoja výchovy a vzdelávania bude obsahovať aj komponenty výučby bezpečnostného povedomia. Zložitejšia je situácia v oblasti formovania bezpečnostného systému štátu. Proces bol pozastavený na začiatku tohto decénia a odvtedy sa udialo pomerne málo. Na pôde

SIS sa vybudoval útvar NBAC\* (Národné bezpečnostné analytické centrum), ktorý priebežne vyhodnocuje všetky bezpečnostné riziká primárne spojené s teroristickými hrozbami. Je povzbudzujúce, že na zozname bezpečnostných incidentov a bezpečnostných udalostí, ktorými sa NBAC zaoberá, sú aj také oblasti ako napr. rizikové prejavy v médiách a na internete, a to špecificky: a) vyhlásenia teroristických organizácií, organizovaných ozbrojených bojových skupín alebo iných radikálnych a militantných skupín prezentované v médiách alebo na internete naznačujúce zámer zorganizovať, podporiť alebo vykonať teroristický útok alebo inú násilnú akciu proti štátnym občanom Slovenskej republiky alebo inštitúciám Slovenskej republiky alebo s dosahom na Slovenskú republiku; b) aktivity osôb so vzťahom k Slovenskej republike alebo aktivity týkajúce sa Slovenskej republiky na internete, ktoré súvisia s propagáciou terorizmu a aktivitami teroristických organizácií, organizovaných ozbrojených bojových skupín alebo iných radikálnych a militantných skupín; c) publikovanie a šírenie materiálov propagujúcich terorizmus alebo iné formy násillia alebo neznášanlivosti na území Slovenskej republiky alebo v zahraničí s dosahom na Slovenskú republiku.

Ostáva veriť, že NBAC bude plniť kľúčovú úlohu centrálného uzla na spracovanie hybridných hrozieb v Slovenskej republike. Otázna bude úloha nového SITCEN-u, ktorý je etablovaný pri Bezpečnostnej rade SR na Úrade vlády SR. Nie je zatiaľ zrejmé, aké úlohy bude plniť, no jeho postavenie pri vláde ho predurčuje na lepšie zhostenie sa úlohy centrálnej bunky pre hybridné hrozby. Ich medzirezortný charakter a nutnosť zdieľať vojenské a civilné spravodajstvo je pre tento orgán primeranejší. Nezodpovedanou otázkou naďalej zostáva téma strategickej komunikácie, ktorá zostáva neuchopená.

Ministerstvo zahraničných vecí a európskych záležitostí SR (MZV) si vytvorilo interný nástroj na vyhodnocovanie aktuálnych bezpečnostných hrozieb v zahraničí. Je to zdroj informácií pre činnosť SITCEN, NBAC, Bezpečnostnej rady SR a krízového štábu MZV. Zároveň je to zdroj informácií na včasné prijímanie preventívnych opatrení a systémový nástroj na jednotný postup vyhodnocovania aktuálnej bezpečnostnej situácie v danej krajine a riadenie krízových situácií. Zostáva doriešiť otázku prepojenia na NBAC a SITCEN† (Situačné centrum a Národné bezpečnostné a analytické centrum).

Záveru:

1. Pokračovať v adaptácii bezpečnostného a obranného systému proti hybridným hrozbám a hybridným aktivitám (stratégia a taktika, inštitúcie, právne normy, vládna podpora občianskej spoločnosti a výskumu), vrátane jasného definovania týchto hrozieb a kompetencií štátnych orgánov v oblasti prevencie, reakcie a riešenia následkov.
2. Systematické zdokonaľovanie bezpečnostného systému tak, aby bol schopný obsiahnuť všetky vážne hrozby. Cieľom je vytvoriť primeraný mix vojenských a civilných spôsobilostí na boj proti hybridným hrozbám. Nutným predpokladom bude primerané financovanie.

---

\* <http://www.sis.gov.sk/o-nas/nbac.html>

† Opis krízového manažmentu na MZV a EZ SR: [http://www.iss.europa.eu/uploads/media/Crisis\\_Rooms.pdf](http://www.iss.europa.eu/uploads/media/Crisis_Rooms.pdf); resp. [http://www.mtf.stuba.sk/docs/internetovy\\_casopis/2014/1/1\\_web4\\_Stefankova.pdf](http://www.mtf.stuba.sk/docs/internetovy_casopis/2014/1/1_web4_Stefankova.pdf)

3. STRATCOM (Strategická komunikácia) - prijať stratégiu na efektívnejšiu komunikáciu s verejnosťou, treba vysvetliť, čo sú hybridné hrozby, čo je s nimi späté a prečo je dôležité sa im postaviť.
4. Spravodajská komunita hrá jednu z dominantných úloh v procese, bez jej participácie je snaha zbytočná. Trojica rezortov/orgánov má dominantné postavenie v téme hybridné hrozby: ministerstvo vnútra - SIS - ministerstvo obrany (Vojenské spravodajstvo), v tejto kompozícii treba hľadať odpovede, ako čeliť hybridným hrozbám.

Odporúčania:

1. Nominovať kontaktnú osobu (POC) za Slovenskú republiku pre EU Fusion Cell;
2. Identifikovať kritické oblasti náchylné na zlyhanie pod vplyvom hybridných hrozieb v SR (na základe odporúčaní NATO);
3. Na základe výsledkov zvážiť prijatie celoštátnej stratégie voči hybridným hrozbám;
4. Konsolidovať bezpečnostný systém SR s vytvorením centra na boj proti hybridným hrozbám;
5. Zdokonaľovať systémy zdieľania kritických informácií, osobitne v utajovanom režime;
6. Zakomponovať elementy hybridných aktivít do scenárov cvičení krízového manažmentu a pravidelne ich vyhodnocovať;
7. Vytvoriť jednotnú komunikačnú stratégiu Slovenskej republiky;
8. Zakomponovať prvky bezpečnostného povedomia do vyučovacieho procesu na školách.

## **P. Draxler: Vplyv dostupnosti šifrovania na bezpečnosť občanov a štátu**

***Pavol Draxler** (1980) – Štúdium medzinárodných vzťahov na Linköping University vo Švédsku absolvoval v období 2006-2008. Predtým pracoval na Ministerstve vnútra SR, kde zastával post predsedu komisie na koordináciu postupu proti extrémizmu. Pôsobil tiež ako bezpečnostný špecialista vo viacerých medzinárodných organizáciách; poskytoval aj bezpečnostnú asistenciu novinárom v Kosove a v Bosne. V roku 2007 sa podieľal na činnosti Delegácie Európskej komisie v Moskve. Od roku 2011 je nezávislým expertom Európskej komisie v otázkach extrémizmu a radikalizmu. Aktuálne vedie súkromnú spoločnosť, ktorá sa venuje ochrane pred kybernetickými hrozbami.*

Nové technológie znamenajú markantnú zmenu v živote spoločnosti, preniesli nás za posledných 20 rokov do novej, digitálnej éry. Do virtuálneho sveta sa presúva stále viac aktivít z bežného života, čo platí aj pre tie nelegálne. S tým súvisí potreba zvyšovať ochranu prenášaných a uchovávaných dát. Odtiaľ plynú aj nové výzvy pre bezpečnostný sektor a štátne zložky, ktoré sa majú venovať ochrane obyvateľstva.

### **Kryptoanarchizmus – šifrovanie pre každého**

Zvyšovanie bezpečnosti súkromia s rozvojom kryptografie je vhodné spojiť s rokom 1988, keď Timothy C. May prvýkrát publikoval svoju víziu kryptoanarchizmu. Definoval nové usporiadanie spoločnosti cez sprístupnenie technológií a šifrovania. Malo to priniesť slobodu jednotlivcovi a štát - ako ho poznáme - mal zastarať. Vo svojom manifeste deklaroval oblasti, v ktorých dôjde k radikálnej zmene a odpútaniu od štátu. V prvom rade išlo o prístup k bezpečnej a diskkrétnej komunikácii medzi ľuďmi. Ďalšie oblasti predstavovali slobodné obchodovanie, virtuálnu decentralizovanú platobnú menu a v poslednom štádiu je spoločnosť založená na decentralizovanej obchodnej interakcii medzi ľuďmi bez akéhokoľvek zásahu štátu. V konečnom dôsledku má dôjsť k vytvoreniu dátového neba, kde ľudia budú môcť slobodne komunikovať, intereagovať a obchodovať bez akéhokoľvek zásahu centrálnej autority.

Akokoľvek sa zdal v roku 1988 manifest utopistický, postupne sa k nemu prihlásilo viacero výrazných osobností z oblasti kryptografie a inovatívnych riešení a dochádzalo k napĺňaniu jeho vízií. Ako prvé bolo sprístupnenie šifrovacích protokolov a programov, ktorých tvorcovia sa často hlásili k myšlienkam kryptoanarchizmu alebo cypherpunku. Zoznam lídrov, ktorí prispeli k kryptografickým inováciám dnes ovplyvňujúcim každodenné používanie internetu a technológií, je pomerne prekvapivo krátky. Obsahuje približne 70 často prepojených osôb. Z tých výraznejších môžeme spomenúť napríklad Juliana Assangea, zakladateľa Wikileaks, ktorý začal komunikovať s cypher punk komunitou v roku 1993. Ďalej to je Jacob Applebaum, vývojár anonymizačnej decentralizovanej siete TOR. Philip Zimmermann vytvoril a voľne sprístupnil v roku 1991 šifrovací protokol PGP a výrazne prispel k zabezpečeniu protokolu VoIP, prenosu hlasových služieb cez internet. Momentálne sa venuje vývoju bezpečných telefonických prístrojov v spoločnosti Silent Circle. Patrí sem aj Ben Laurie - tvorca knižnice open ssl, ktorá sa masovo využíva v ochrane prenosu webových stránok a ktorý bol zároveň aj v rade Wikileaks.

### **Virtuálna decentralizovaná platobná mena**

K naplneniu vízie slobodného decentralizovaného obchodovania prišlo len nedávno v roku 2009 zriadením prvej decentralizovanej virtuálnej meny Bitcoin, založenej na kryptografii dodnes neznámym autorom, vystupujúcim pod pseudonymom Satoshi Nakamoto. Decentralizované riešenie znamená, že neexistuje žiadna centrálna autorita alebo server, ktorý by mohol jednoducho ovplyvniť alebo regulovať dané riešenie. Každý používateľ je súčasťou celej siete, kde sa distribuovane uchovávajú všetky dáta. Preto ovládnutie tohto systému je značne nerealistické. Samotný bitcoin sa teší čoraz väčšej obľube a stáva sa čoraz viac akceptovanejším platidlom na lokálnej, ale aj medzinárodnej úrovni. Dnes nie je problém poslať SEPA platbu v Bitcoinoch, objednať si jedlo cez internet, alebo zaplatiť v sieti rýchleho občerstvenia Subway na Slovensku alebo v Čechách.

### **Slobodné obchodovanie**

K prvým pokusom o sprístupnenie slobodného obchodovania došlo po uvedení Bitcoinu. Priekopnícku úlohu zohral anonymný portál Silk Road, fungujúci v anonymizačnej decentralizovanej sieti TOR, ktorý vznikol v začiatkom roka 2012. Prostredníctvom portálu Bitcoin platieb mohli ľudia predávať a nakupovať akýkoľvek tovar s ohľadom na diskretnosť a súkromie. Najväčšou slabinou bola jeho centralizovanosť. To znamená, že i keď Silk Road fungoval v sieti TOR, portál bežal na konkrétnych serveroch, administrovaný konkrétnym administrátorom Rossom Ulbrichtom, ktorý bol odhalený koncom roka 2013. Za tú dobu dosahoval Silk Road obrat rádovo v stovkách miliónov dolárov. V zapätí vzniklo niekoľko nasledovníkov na rovnakom princípe. Evolúcia však priniesla nové decentralizované riešenie Open Bazar, ktoré je momentálne do veľkej miery regulované autormi. Je ale iba otázkou času, kedy vznikne decentralizovaný a neregulovaný produkt.

### **Slobodný prístup k tovaru**

Osobitnou časťou liberalizácie produkcie predmetov je dostupnosť 3D tlačiarňí, keď akékoľvek produkty možno vytlačiť v pohodlí domova. Momentálne je najrozšírenejšia tlač z tvrdeného plastu. Lacnejšie prístroje na 3D tlač sa dajú kúpiť už od 400 eur a veľmi kvalitné stoja 800 eur a viac. Tlačiarne sú schopné vytlačiť napríklad použiteľné súčiastky, šperky, súčasti nábytku, ale aj funkčné auto. Užívateľ si jednoducho stiahne niektorú z tisícov šablón produktov podľa potreby a pokojne doma vytlačí objekt. Rozruch vyvolalo sprístupnenie šablóny funkčnej strelnej zbrane liberátor. Rozšíreniu metalických tlačiarní bráni momentálne ich cena radovo v tisícoch eur, ale i tu sa očakáva zníženie ceny alebo sprístupnenie zariadení prostredníctvom „share fundingu“, komunitného zdieľania.



Liberator, 3D vytlačená zbraň kalibru .22.

### Slobodný „decentralizovaný“ občan

Estónsko je dlhodobo lídrom v digitalizácii štátnej správy a inováciách v tejto oblasti. Komplexný portál štátnych služieb bol sprístupnený občanom v roku 2005. Prostredníctvom neho sa minimalizoval počet úradníkov a návštev občanov na úradoch. Estónsko inovácie v tejto oblasti dynamicky rozvíja naďalej a ako prvá krajina sprístupnila koncept digitálneho obyvateľa E-residency už koncom roka 2014. Občania Európskej únie majú možnosť zažiadať o digitálne podpísanú rezidenčnú kartu, cez ktorú môžu komunikovať s úradmi v Estónsku, zakladať spoločnosti alebo bankové účty. Tým sa začína vytrácať priamy vzťah pravidiel a jurisdikcie na fyzický priestor, kde sa práve osoby nachádzajú.



Digitálna identifikačná karta Estónska

Estónsko inovatívne odhadlo, že funkcie štátu nemusia byť nevyhnutne závislé na fyzickom priestore. Ak by sme túto teóriu rozvinuli, občania si možno v budúcnosti budú môcť vybrať pravidlá, podľa ktorých budú chcieť žiť nezávislé na ich prítomnosti v konkrétnej krajine. Momentálne s podobným nápadom prišiel aj vyjednávač pre podmienky vystúpenia Veľkej Británie z Európskej únie, keď načrtnol možnosť, že Briti budú môcť ostať ako občania a využívať výhody EÚ ako jednotlivci na základe

svojho rozhodnutia a po zaplatení ročného poplatku. Týmto aktivitami sa začínajú stierať hranice národných štátov a politických systémov v ich vnútorných hraniciach. Estónsko sa na túto možnosť pripravuje aj zavedením konceptu „Digital Embassy“. Estónsko so svojou značne digitalizovanou štátnou správou sa rozhodlo uložiť tieto dáta a aplikácie do datacentier na svojich veľvyslanectvách v tretích krajinách. Tým si zabezpečia fungovanie estónskeho štátu aj v prípade, že prídu o svoje terajšie fyzické územie.

Momentálne začínajú v tejto oblasti aj neštátne aktivity, ako napríklad BitNation, čo je rozvinutý portál, ktorý ponúka neštátne digitálne občianstvo každému záujemcovi a služby k nemu na základe dobrovoľnosti.

## **Rozšírenie a dostupnosť šifrovacích nástrojov**

Presun bežného života do digitálneho sveta samozrejme znamenal aj presun kriminálnych činností tým istým smerom. Štát to vníma predovšetkým cez problematiku bežnej komunikácie záujmových osôb, ale začína reflektovať aj nové formy nelegálnych činností spojených s presunom do digitálneho sveta, ako sú krádeže údajov, ransomware\* a podobne.

V súčasnosti je k dispozícii množstvo riešení na šifrovanie dát a komunikácie. Takmer každý operačný systém ponúka šifrovanie disku a dát už v základnom nastavení. V najnevyhnutnejšom prípade prenosu súborov možno použiť jednoduchý program na komprimáciu súborov ZIP, ktorý už dávno ponúka solídne šifrovanie AES-256.

Na zasielanie e-mailov je voľne dostupný open source program GnuPG. Jeho nevýhoda je, že v prípade kompromitácie privátneho kľúča je útočník schopný prečítať všetku dovtedy zaslanú poštu v rámci platnosti získaného kľúča. Obavy okolo programov, zabezpečujúcich šifrovanú komunikáciu, vystali predovšetkým so stúpajúcou popularitou u teroristických organizácií. Aktuálne zarezonovala aplikácia Telegram, ktorú údajne využívali páchatelia teroristických útokov v Paríži v roku 2015. Od roku 2009 islamistické teroristické organizácie vyvíjali aj vlastné riešenia šifrovanej komunikácie, ako napríklad Mujahedeen secrets, ktoré bolo založené na PGP. Ďalšie veľmi populárne aplikácie sú Surespot, Threema a Signal. Pričom Signal poskytuje aj možnosť šifrovaného prenosu hlasu, ktoré možno rovnako jednoducho použiť, ako bežný telefonický hovor.

Osobitne robustné riešenie je zakrývanie aktivity na internete cez anonymizačné služby, z ktorých najznámejšia je The Onion Router alebo jednoducho TOR. Je to decentralizovaná sieť, do ktorej sa pristupuje prostredníctvom jednoducho stiahnuteľného programu. Prístup do siete je šifrovaný a komunikácia sa „stráca“ šifrovaným presunom medzi viacerými uzlami vo vnútri siete TOR. TOR možno využiť na anonymizovanie prístupu späť do internetu alebo pre služby tzv. Dark Web, prípadne Deep Web servisov vo vnútri TOR siete. Samotný TOR projekt, ktorý vznikol v roku 2002, finančne podporila americká vláda. Jeho cieľom bolo dať opozícií v diktátorských krajinách k dispozícii nástroj na bezpečnú komunikáciu.

---

\* Ransomware je druh malwaru, zabráňujúceho prístup k počítaču, ktorý je infikovaný; obvykle vyžaduje zaplatenie výkupného.

Z rovnakého dôvodu vznikla aj *live distribúcia* linuxu Tails, ktorá kombinuje všetky v nej prednastavené potrebné anonymizačné nástroje na ochranu súkromia.

So zvyšujúcou popularitou *hidden services* sa začali transformovať do deep webu aj nelegálne služby, ako napríklad predaj falošných dokumentov, bankoviek alebo zbraní.

**DEEPWEB GUNS STORE**

Market | Wallet (0.23120633 BTC) | Cart | Info | Support | Log out

**AK47 Black Laminate** Price: 1.137 BTC

**TSS Custom AK 47 AKMS** Price: 2.925 BTC

**Remington Defense XM110** Price: 7.115 BTC

Predaj zbraní vo vnútri siete TOR.

## Výzvy právo presadzujúcim a bezpečnostným zložkám

Štát je v tejto oblasti vždy retroaktívny, a teda pár krokov pozadu. Doménou, ale aj veľmi atraktívnym lákadlom sa stala možnosť využiť dostupnosť technológií na získanie prístupu ku komunikácii občanov a kontrole nad ňou. Ešte pred 15 rokmi boli informácie, prenášané cez sieť a následne ukladané, takmer výlučne voľne prístupné a nešifrované. Postupným presunom aktivít do digitálneho sveta tieto informácie nadobúdali na hodnote, a preto sa začali implementovať prvky na ich ochranu ako šifrovanie, anonymizácia a autentifikácia.

Štáty sa momentálne zameriavajú na dáta v dátovom úložisku a na prenášané dáta, inak povedané na dáta v mobile, počítači, serveri a cloude alebo na dáta počas ich prenosu po sieti.

**Základné stratégie, ktorými sa bezpečnostné zložky uberajú, sú:**

1. Regulácia šifrovacích programov
2. Masový zber dát, metadát a komunikácie
3. Cieľový útok na jednotlivca

### 1. Regulácia šifrovacích programov

Regulácia môže mať rôzne formy. Od obskúrnych zákazov užívania silnejších šifrov - aké je štát schopný zlomiť - až po nanútené implementovanie back dooru



(zadných vrátok) do šifrovacieho programu. Obe tieto stratégie so sebou prinášajú rovnaké riziko. Obe vytvárajú vedomú zraniteľnosť, ktorú v každom momente hľadajú a sú prichytené zneužiť tisíce kriminálnikov alebo nepriateľské služby a štáty. Relatívne akceptovateľný prístup pre centralizované riešenia je mať možnosť na základe solídnych kontrol vypnúť šifrovanie na strane klienta a takýmto spôsobom si sprístupniť komunikáciu. Takéto riešenie by však bolo rýchlo odhalené a sofistikovanejší páchateľ by preto veľmi pravdepodobne prestal takúto službu používať a zvolil inú formu konšpirácie.

## **2. Masový zber dát, metadát a komunikácie**

Najviac diskutovaná stratégia je masový zber metadát alebo v horšom prípade čistých dát. Tento prístup má svoje opodstatnenie v krajinách, kde je značná časť obyvateľstva nepriateľsky naladená, ako napríklad Izrael, alebo Donbas. Špecifická situácia je v krajinách, kde sa diktátorské režimy snažia kontrolovať opozične naladené obyvateľstvo.

Pre krajiny v západnom svete, kde treba hľadať nebezpečných jednotlivcov, ale do veľkej miery ide o placebo pre bezpečnostné zložky. Tento prístup dáva bezpečnostným zložkám pocit kontroly, ale viacero štúdií ukazuje, že ide o veľmi nákladný domnelý pocit s minimálnym vplyvom na prevenciu. Napríklad analýza využívania efektívnosti zberu metadát v USA ukazuje, že jediný prípad úspešnej profilizácie na základe metadát bol prípad Basaalu Moalina, taxikára zo San Diega, ktorý v rokoch 2007 a 2008 venoval \$8,500 teroristickej organizácii al-Shabaab, súčasť Al-Kaidy v Somálsku. Na druhej strane nie je známy prípad, keď analýza metadát dokázala zabrániť teroristickému útoku v USA. Vo väčšine prípadov k odhaleniu teroristického útoku došlo za použitia informátora alebo inak získaných operatívnych informácií.

Neefektivita v porovnaní s nákladmi má základ v profilácií „závadového“ správania vo veľkých dátach (big data). Úspešná profilácia správania potenciálneho páchateľa v miliónoch záznamov metadát je takmer na úrovni štatistickej náhody. Na druhej strane táto profilácia produkuje veľa „false positives“, teda hlásení, keď dáta zodpovedajú profilu „závadového“ správania, ale samotná osoba závadová nie je. Preverovanie týchto hlásení si vyžaduje značné ľudské a materiálne zdroje, čo vytvára ďalšie nároky na rozpočet zväčša so slabým výsledkom.

Prečo je teda masový zber dát taký populárny a presadzovaný bezpečnostnými zložkami? Je to z viacerých dôvodov. Najhlavnejšie sú tie, že je extrémne drahý, dáva dojem kontroly, ktorý sa veľmi dobre prezentuje, málokto politik si dovoľí prijať rozhodnutie, ktoré by vyvolalo dojem ohrozenia jeho občanov zrušením tohto nástroja a v neposlednom rade dáva bezpečnostným zložkám rýchly prístup na overenie podozrenia a prípadné následne odhalenie celej siete, na ktoré by za normálnej situácie bolo treba vypracovať a získať povolenia na vstup do súkromia. Posledný z bodov, rýchle potvrdenie informácie a získanie analýzy stykovej bázy záujmovej osoby môže byť prínosné pre bezpečnosť občanov. Otázne je, či toto zjednodušenie dostupnosti nemá vplyv na zníženie vyšetrovacích a operatívnych schopností bezpečnostných zložiek, keďže je lákavé skĺznuť k „hádaniu“ miesto overovania na základe kvalitne získaných informácií. Získanie rovnakých informácií o podozrivej osobe súdnym príkazom je síce pomalšie, ale

vedie operatívu k tomu, aby kvalitne vyšetrovala, je rádovo lacnejšie a výsledky sú rovnaké. Veľmi dôležitý argument je obava, nakoľko môžu byť tieto dáta zneužitie v prítomnosti, ale hlavne v budúcnosti.

### 3. Cielený útok na jednotlivca

Útok na konkrétne zariadenie vytipovanej osoby môže prebehnúť na viacerých úrovniach. Medzi legitímne postupy môžeme radiť kontrolovaný útok, využívajúci chybu dotyčného. Môže to byť napríklad získanie prístupu k zariadeniu sociálnym inžinierstvom, odpočutie komunikácie zo zariadenia, cielené získanie dát u poskytovateľov služieb, zadržanie zariadenia v zraniteľnom stave, kvalitná forenzná analýza zadržaného zariadenia, *brute force* legálne zadržaných zariadení, MITM útok, phishing, inštalácia keyloggeru a iné využitie chýb páchatel'ov.

Vo väčšine prípadov sú to rovnaké techniky, ako používajú kriminálne skupiny na napadnutie obete. Tieto techniky sú vo väčšine krajín podmienené súdnym príkazom, čo by malo zabezpečiť solídnu kontrolu nad procesom a ochranou súkromia.

Kontroverzné sa stali útoky cez tzv. *zero day exploits*, ktoré za slušnú finančnú odmenu poskytujú štátnym záujemcom niektoré privátne spoločnosti, ako Lench IT solutions, Gamma alebo Hacking Team. Problémom je využívanie *zero day* zraniteľností, teda zraniteľnosti, ktorá ešte nebola verejne odhalená a publikovaná, takže užívatelia ani poskytovateľ programu o nej nemajú vedomosť. Zodpovedný prístup je oznámiť túto zraniteľnosť autorovi kódu okamžite, aby mohol čo najskôr zabezpečiť nápravu v podobe záplaty. V opačnom prípade hrozí, že sa tieto *zero day* zraniteľnosti budú obchodovať a zneužívať kriminálnymi skupinami. Preto absencia informovania zo strany štátnych zložiek vedome vystavuje milióny zariadení občanov riziku útokov kriminálnych skupín.

### Záver

Je prirodzené, že každá inovácia, ktorá sa masovo rozšírila, vyvoláva aj pozornosť kriminálnych skupín. Neznamená to však, že inovácia je zlá ako celok. Ak by sme chceli poskytnúť príklad cez možno trochu prehnane prenesenú paralelu, *aj organizovaný zločin a teroristi využívajú papierové peniaze alebo internet na svoju činnosť. To samozrejme neznamená, že preto by sme ich mali zrušiť alebo kriminalizovať ako celok.* Dôležité sú kontroly týchto skupín, prevencia, ich odhaľovanie a nie plošné znižovanie bezpečnosti všetkých občanov. Bude veľmi zložitá a neefektívne zakazovať silnejšie šifry. Inými slovami táto možnosť je už málo realistická. Pre právo presadzujúce a bezpečnostné zložky nemá zmysel sa obávať programov so silným šifrovaním, ale programov, ktoré nedovoľujú užívateľom robiť chyby. Pretože väčšina páchatel'ov bola odhalená práve cez ne a kvalitným spojením operatívnej práce vo fyzickom svete a technickou akciou v tom digitálnom.

Ak nechceme opustiť naše hodnoty ochrany slobody a demokracie, pre právo presadzujúce a bezpečnostné zložky je rozumnejšie miesto nákladných a neefektívnych pokusov ovládnuť digitálny svet silou preniesť kvalitnú operatívnu prácu do vnútra digitálneho sveta a spojiť ju s kvalitnou prácou v tom fyzickom.

## **P. Zeman: Pokus o bilanci úspěchů a proher polistopadových českých a slovenských zpravodajských služeb**

***Petr Zeman** (1947) – Signatár Charty 77. Po novembri 1989 pôsobil na vedúcich postoch v kontrarozviedke. Bol tiež riaditeľom Úradu pro zahraniční styky a informace (1998-2001). Prednášal o spravodajských službách na Masarykovej univerzite v Brne. Podieľal sa aj na činnosti Ústavu strategických štúdií Univerzity obrany v Brne. Je autorom a hlavným koordinátorom spracovania publikácie Česká bezpečnostní terminologie. Významnou mierou zhrnul a rozpracoval poznatky z oblasti terminológie, fungovania a členenia spravodajských služieb. Venoval sa problematike transformácie spravodajských štruktúr v postkomunistických krajinách.*

Konstatuji, že úroveň bezpečnosti se v posledních třech až pěti letech významně zhoršila. Zejména zahraničně politický vývoj budí reálné obavy z příštího.

V nebezpečném světě vzrůstá potřeba kvalitních a kompetentních zpravodajských institucí. Pokusím se o bilanci úspěchů a proher polistopadových českých a slovenských zpravodajských služeb. Výhrad k nim mám spoustu, ale záměrně si nevšímám většiny tzv. afér. (Dozajista je mrzuté, že české a slovenské zpravodajské služby se nedokážou postavit čelem ke svým vlastním aférám, ať už je to slovenská Gorila nebo česká kauza Janoušek. Kazí si tak své vnímání veřejností.) V referátu se soustřeďuji jen na trendy, jež považuji za **zásadní** a **dlouhodobě určující**. Hodnocení je výlučně moje osobní, tedy chcete-li subjektivní.

Musím předem zdůraznit, že **vůbec nejzávažnějším** vybočením z dráhy slušné zpravodajské služby ve slušném státě bezpochyby bylo působení **Ivana Lexy a Jaroslava Svěchoty** v čele slovenské SIS za třetí Mečiarovy vlády. O této krajně smutné etapě, ba celonárodní prohře, byla na Slovensku napsána řada článků a knih; fakta všichni znáte, není tedy nutné je zde opakovat.

### **Neporozumění politiků**

Největším kamenem úrazu našich služeb byl vztah vedení státu, stručněji řečeno vztah politiků ke službám. Je to pravdaže problém i v jiných zemích, zejména v těch, jež po roce 1990 opustily komunismus. Zdá se mi však, a jistě chápete, že takovýto dojem stěžejí mohu dokázat, nebo dokonce kvantifikovat, že v disciplíně „nepochopení funkce zpravodajských služeb“ čeští a slovenští politici vyhrávají. Politiky přirozeně zajímá především to, co musejí řešit příští týden, a výsledek chtějí hned. Což není proveditelné. Mnozí z politiků nemohou překonat chuť tu či onu službu zneužít ve vlastním zájmu mezistranickém či vnitrostranickém. Jedinou zbraní proti tomu je profesionální pevnost a **občanská zmužilost** lidí ve vedení služeb. Jako pozitivní příklad tu uvádím postup Vladimíra Mitra a jeho náměstků ze SIS v roce 1995. Naproti tomu počínání šéfa českého Vojenského zpravodajství Ondřeje Páleníka s Janou Nagyovou v roce 2013, může posloužit jako krajně negativní příklad nezákonnosti, podbízení a trapnosti.

### **Právní bariéry**

Když po převratu roku 1989 nové zpravodajské služby vznikly, dalo se jim - v souladu s tehdy krajně rozšířenou „fobií z StB“ - do vínku jen pramálo **oprávnění**.

Služby byly začátkem 90. let co do kompetencí nastaveny na mírový stav ve vysněném bezpečném světě. Praxe později ukázala, že příslušná oprávnění je potřeba rozšířit. Náprava postupovala velmi pomalu. Koulí na noze byl - a je - navyklý **postup při úpravě zákonů** a organizačních opatření, týkajících se zpravodajských služeb. Projevuje se to několika způsoby. Převažuje pojetí, že v právním textu je potřeba všechny možné situace předem předjímat, vše dopodrobna definovat, a to nejlépe **taxativně** (touto slepou uličkou se s oblibou ubírají zejména legislativní návrhy slovenské).

Bezpochyby by bylo ideální zformulovat zákon, který upraví vše podstatné najednou a není nutné jej každý rok příštípkářsky doplňovat. To ale v českém právně parlamentním prostředí možné není. Podaří-li se navrhnout dílčí úpravu, ozvou se ihned hlasy, že je třeba tuhle něco přidat, tuhle něco ubrat, a vůbec - musíme zesílit kontrolu služeb. Jenže čím více požadavků, **tím snadněji každý z nich začne někomu vadit**. A tak uplyne volební období a legislativní úpravy se neuskuteční.

Příkladem budiž oprávnění služeb nahlížet do evidencí, které ostatní orgány státu pro různé účely vedou. Optimálním řešením by bylo, stručně shrnuto, asi toto: *zpravodajská služba je oprávněna požádat o nahlédnutí do evidencí, které pro své účely vedou orgány státu; tam, kde je to možné, nahlédnout do nich on-line; příslušné orgány státu jsou povinny jí vyhovět; každé nahlédnutí musí samo být do detailů zaznamenáno, aby mohlo posléze eventuálně být obhájeno. Samostatnou kategorií jsou explicitně vyjmenované evidence, jejichž vytěžení schvaluje soud.*

Praxe se ubírala jinou cestou. Po urputném vyjednávání byla přijata novelizace zákona, jež svolila nahlédnout – paroduji – do speciální evidence předních tramvajových vozů; po půldruhém roce nastala další novelizace pro zadní tramvajové vozy, a tak dále.

## Vnější kontrola

Plně souhlasím s tím, že vedle posílených oprávnění se současně musí řešit zlepšení civilní kontroly služeb. V České republice se návrhy na hlubší kontrolu prováděnou **neposlanci** poprvé objevily v roce 1996. Dvacet let (!) se návrh nedařilo prosadit. Právě v době konání tohoto sympózia je v české poslanecké sněmovně obdobný návrh, který možná bude schválen. Návrh nynějšího zákona o kontrole nicméně obsahuje taková vnitřní systémová omezení, že naplnit jej bude skoro nemožné a výsledek bude bohužel zcela neefektivní.

## Koordinace

Asi 18 let se v ČR volá po neresortním a nestraničském **koordinátorovi** služeb na úrovni státního tajemníka při úřadu vlády. Koordinátor je institut, který lze zřídit dohodou exekutivy, bez bitev v parlamentu. Vážně to navrhnout si dosud nikdo netroufnil. Domnívám se, že podobné situace prožíváte i na Slovensku.

## Otazníky nad vojenskými službami

Velmi stručně: Jak je tomu v zahraničí?

Americká střežová zpravodajská služba ministerstva obrany DIA (Defense Intelligence Agency) je vyjmenována mezi 16 dalšími tělesy zpravodajského zaměření, ale označena je výslovně jako resortní, americky *departmental*. Naproti tomu CIA je v kategorii *national*, tj. celostátní.

Ve Velké Británii zákon vyjmenovává tři zpravodajské služby: SIS, Security Service a GCHQ. Střežová služba ozbrojených sil DIS (Defence Intelligence Staff) takto označena *není*.

Pohledme na Nizozemí: Současný zákon z roku 2002 upravuje postavení dvou služeb – civilní AIVD (Algemene Inlichtingen- en Veiligheidsdienst) a vojenské MIVD (Militaire Inlichtingen- en Veiligheidsdienst). Obě slučují kontrarozvědné i výzvědné role. Postavení vojenské zpravodajské služby v Nizozemí je na první pohled oproti službě civilní zdánlivě zrcadlově symetrické. Není tomu tak. Článek 7 zákona **výslovně** MIVD zaměřuje na otázky **militární** (*matters with military relevance*). Jestliže MIVD chce aplikovat zpravodajské prostředky na prostory, které *nejsou* v držení ministerstva obrany, musí podle článku 20 **žádat o svolení** ministra vnitra nebo **šéfa civilní služby**.

Právní postavení a organizační uspořádání Vojenského zpravodajství (VZ) v ČR (a podobně i na Slovensku) považuji za chybné. V roce 1994 byla Zpravodajská služba generálního štábu přejmenována na Vojenskou zpravodajskou službu (VZS) a povýšena na úroveň **definovanou zákonem stejně jako BIS a ÚZSI**, česká vnitřní a česká vnější civilní služba.

Česká VZS podle zákona z roku 2005 splýnula s Vojenským obranným zpravodajstvím (VOZ) do tzv. jednotného VZ, snad aby se servilně vyhovělo nekvalifikovanému volání politiků, zda je potřeba mít „tolik služeb“. Sloučení kontrarozvědky a rozvědky do jedné instituce považuji z řady důvodů za nesprávné. Mimo jiné sloučení ztěžuje kontrolu služby, mísí dva odlišné právní režimy a tak posiluje možnost a pokušení službu zneužít.

Myslím, že selhání šéfů Vojenského zpravodajství v aféře Nagyová není náhodné a plyne z interní firemní kultury, jež v něm přetrvává. Předchůdce VZS, tedy ZS GŠ po roce 1989 hřešila na to, že nebyla přímou součástí represivního aparátu komunistického státu, takže údajně nebyla potřebná její personální obměna. Troufám si říci, že v této službě:

- absentovalo vnímání soudobé situace zpravodajských služeb (význam lidských práv, civilní kontrola ozbrojených složek, právní stát, etické kodexy, předkládání účtů veřejnosti);
- přetrvávalo sebepojetí namyšlené, bohorovně výlučné, s pocitem „nám je vše dovoleno“, jsme lidé výjimečného ražení;
- zůstalo ovlivnění postoji ruské GRU, mj. s jeho dědictvím neustálého soupeření s civilní výzvědnou službou.

Bonmotem říkávám, že pánové z vedení Vojenského zpravodajství se v roce 2013 žili mentálně spíše v roce 1913. Pozoroval jsem ale, že obdobné mentální sebepojetí a tendence zakořenily i v polských militárních zpravodajských službách. Jde asi o věčně zelené dědictví „tábora míru a socialismu.“

V České republice (dříve) VZS a (nyní) VZ po léta soupeří s civilním výzvědným zpravodajstvím ÚZSI – duplikuje o politické zpravodajství globálního dosahu a non-militárního obsahu, což enormně zesiluje rivalitu a škodí oběma službám. Do vývoje ve VZ nešťastně zasáhl v roce 2004-2006 tehdejší jeho šéf Miroslav Krejčík, který zbytečně a hlavně náhle a bez náhrady propustil bývalé důstojníky ZS ČG, v té době už 15 let sloužící novému režimu. (Aby bylo jasno, jsem výrazně pro personální změny, ale nikoli tímto způsobem. Podobně destruktivně si počínal v roce 2004 i ředitel Slovenskej informačnej služby Ladislav Pittner.) M. Krejčík se pokusil kriminalizovat předchozího ředitele Andora Šándora a dehonestoval ředitele VOZ z let 1991-93 Jana Duchka. VZ v pozdějších letech do značné míry sloužilo k neformální informační podpoře presidenta Klause, a někteří tvrdí, že i ODS.

Domnívám se, že jediná cesta k nápravě militárních služeb je návrat k výlučně **resortnímu zaměření služby**, podřízení VZ generálnímu štábu, a uvnitř organizace zřetelné oddělení vnitrostátního zpravodajství (VOZ) od zahraničního.

V mých očích ZS GŠ a VZS zaslouží jednu významnou **pochvalu**. Před zraky nekvalifikovaných reformátorů armády v letech 1990 až 2001 ve svých útrobách skryla tehdy přísně tajnou jednotku – 601. skupinu speciálních sil. Kdyby byla šestsetjednička v oněch letech pod „normální“ armádou, nepřežila by.

České VZ se nejnověji ujímá role tzv. **kybernetické obrany**. Otázka je, jak se zdaří kybernetickou obranu „ošetřit zákonem“, a zda veřejnost uvěří, že služba svá oprávnění ke vstupu do internetového prostoru nezneužije.

## **Česká rozvědka**

Česká civilní rozvědka neboli Úřad pro zahraniční styky a informace (ÚZSI) byl v roce 1994 „z rozpaků co s ním“ ponechán pod ministrem vnitra a pod přikrytím rozpočtem ministerstva vnitra. Vztah civilní rozvědky s ministrem vnitra se postupně rozvolňoval a navzdory této podivné právní úpravě se dalo říci, že ÚZSI de facto pracuje pro ministerstvo zahraničí a že postupně posiluje svou autonomii. Média před nedávnem ocenila ÚZSI v kauzách unesených osob.

Bohužel, autonomie rozvědky se po nástupu ministra vnitra Milana Chovance v roce 2013 vytrácí. Do vedení služby byli dosazeni lidé ministři osobně zavázaní, což je vždy na pováženu. Tento stav mne vede ke změně názoru na právní zakotvení rozvědky. Dnes dávám přednost tomu, aby **rozvědka podléhala Úřadu vlády** a o jejím šéfovi **rozhodovala vláda jako sbor**, tak jako je tomu od roku 1994 s BIS. Léta jsem si myslel, že když BIS má odpovídat vládě jako celku, tj. cca 15 lidem, v podstatě neodpovídá nikomu. Praxe ukázala, že v tomto právním postavení si BIS zachovala i v letech poměrně četných střídání vlád a premiérů (cca 2005 – 2016) jistou autonomii a přiměřenou nestrannost.

## **Česká služba s vnitřní působností**

Kontrarozvědná služba BIS (Bezpečnostní informační služba) si vydobyla postavení nezpochybnitelné instituce, na rozdíl od prvé polistopadové dekády nyní pozitivně citovanou médií. Je to důsledek krajní opatrnosti, s jakou si BIS posledních 10 let počínala. **Primárním zájmem** bylo a je **neudělat malér** a tak si nepřivolat problémy. Ve srovnání s kontrarozvědkami některých západoevropských států je BIS

příliš skoupá na informace podávané veřejnosti a rozhodně navenek nepřipouští žádná pochybení. Mám za to, že dosti tuhá disciplína ve službě vede mnohé pracovníky k práci do šuplíku, a většinu dalších k markýrování a k práci pouze „od do“.

BIS vznikla v letech 1990 až 1993 de facto jako jakási konfederace několika krystalizačních jader. Nebyla budována shora dolů a také neměla štěstí na uznávané a charismatické ředitele. Potřebná hierarchie se proto usazovala dosti obtížně. Už také proto, že ze všech dosud zmiňovaných služeb byli noví pracovníci BIS ve svém občanském životě před pádem komunismu výrazné individuality.

Vedení BIS před cca 10 lety sáhlo k výrazné centralizaci řídicích a informačních toků; prakticky vymizela schopnost vnímat sledované problematiky na teritoriu působnosti **v celku a ve vzájemných souvislostech**. Přehnaně řečeno, **vymizel územní dozor** a z dřívějších krajských úřadoven se staly pouhé opěrné body. Interpretuji to tak, že ústřednímu vedení se takto pohodlněji velelo.

### **Slovenské služby**

Pokud jde o slovenské služby, mohu jen málo říci o slovenském Vojenskom spravodajstve (VS). Mám ale podezření, že řada neduhů českého VZ je ve VS obdobná. Z médií se dovídáme o tunelování, také o pokusech kriminalizovat kritiky.

Slovenská civilní zpravodajská služba SIS má velmi komplikovanou historii. Poznamenaly ji výrazné **personální diskontinuity**, méně učeně řečeno, čistky a vyhazovy po každé změně vlády. (Za nezbytné přitom považuji jen změny, jež se odehrály na podzim 1998.) Těchto personálních proměn bylo násobně více než v českých civilních službách mezi lety 1993 a dneškem. Úbytek či nezralost zpravodajců **nenapraví** přijímání většího množství policistů (zejména ne těch starších); to je bohužel běžný omyl. Slovenské služby jsou **závislejší na výkyvech stranické politiky** než české. Celé bezpečnostní prostředí (policie, justice) je na Slovensku více klientelistické než v Česku. Tyto faktory brzdily a brzdí profesionální zrání organizace. O to víc jsem uvítal, když za ředitele Jána Valka zmíněný „kádrový trend“ mizel. Bohužel, zdá se, že v současné SIS dochází k jisté recidivě a snaze ochočit ji ve jménu jedné politické strany.

### **Závěr**

Mám za to, že kompetentnost českých a slovenských zpravodajských služeb v uplynulých letech se nezkvalitnila tak, jak bychom v nynějším rizikovějším světě potřebovali. Jistěže dosáhly určitých úspěchů, ale jsem si jist, že se mohlo podařit daleko více a řada příležitostí byla promarněna (to jsou ty prohry!). Viníky nehledejme ve vnějším prostředí, rozhodující roli totiž vždycky má vedení služeb.

## **J. Málík: Reflexia zmeneného operačného prostredia v spravodajskej činnosti polície**

*Jaroslav Málík (1973) – Plukovník Policajného zboru SR absolvoval magisterské štúdium (2003), ako aj rigorózne konanie (2009) na Akadémii PZ v Bratislave. V aktívnej službe je od roku 1992; prešiel viacerými funkciami. Od r. 2000 pôsobil na špecializovanom útvere Prezídia PZ - kriminálne spravodajstvo a riadenie agentov; v období 2012-2016 zastával post riaditeľa útvaru. Od 15. júna 2016 bol menovaný do funkcie 1. viceprezidenta Policajného zboru, podliehajú mu špecializované útvary PZ. Pôsobí tiež ako národný expert Stáleho výboru pre operačnú spoluprácu v oblasti vnútornej bezpečnosti a Slovenskú republiku zastupuje na pravidelných zasadnutiach v centrále Europolu. Venuje sa aj prednáškovým a vzdelávacím aktivitám.*

Keďže operačné prostredie sa mení a podoba hrozieb tiež podlieha zmenám, zákonodarca musí zabezpečiť, aby dosiahol rovnováhu medzi ochranou občianskych slobôd a možnosťami spravodajských služieb robiť si svoju prácu a ochraňovať tak spoločnosť v aktuálnych úlohách a problémoch reflektujúcich zmeny a obsah operačného prostredia, a to i v podmienkach Policajného zboru.

### **1. OPERAČNÉ PROSTREDIE A DETERMINANTY OVPLYVŇUJÚCE ZMENY V ŇOM A ICH VŠEOBECNÁ CHARAKTERISTIKA**

Slovenská republika (ďalej len „SR“) prostredníctvom svojej bezpečnostnej politiky chce flexibilne reagovať na meniace sa bezpečnostné hrozby a výzvy s cieľom obmedziť až eliminovať ich negatívny dosah na bezpečnosť občana a štátu. SR bude svoju bezpečnostnú politiku realizovať tak, aby bola zaručená bezpečnosť a základné podmienky pre život jednotlivca a jeho ochrana pred násilnými hrozbami namierenými voči jeho právam, bezpečnosti a životu.

Súčasnú bezpečnostnú prostredie SR je výrazne ovplyvnené zmenami v aktuálnom celosvetovom i euroatlantickom bezpečnostnom prostredí. Toto je dynamické, komplexné, viacvrstevné a premenlivé, pričom z dlhodobého hľadiska naň bude ešte výraznejšie vplývať rastúca rôznorodosť a stále zložitejšia a ťažšie identifikovateľná previazanosť v ňom pôsobiacich aktérov. Bezpečnostné hrozby a riziká, ako aj ich nositelia a zdroje sú často veľmi zložito lokalizovateľné a majú postupne výraznejší neštátny a nadnárodný charakter. Preto konkrétne aktivity ohrozujúce bezpečnosť SR alebo ich prípadné dôsledky sú ťažko predvídateľné, čo zreteľne prispieva k stieraniu rozdielov medzi vonkajšou a vnútornou bezpečnosťou štátu.

V euroatlantickom priestore v súčasnej dobe prevažujú nevojenské hrozby nad vojenskými. S prehlbujúcou sa globalizáciou sa kontinuálne posilňuje potenciál asymetrických hrozieb a keďže s nástupom a rozvojom globalizácie sa svet stáva čoraz menším, zvyšuje sa možnosť šírenia bezpečnostných hrozieb a rizík i z relatívne vzdialených oblastí, čo reálne znamená, že nie je možné vylúčiť nepriaznivý dopad miestnych a regionálnych konfliktov na bezpečnosť SR a aj jej spojencov v NATO a Európskej únii (ďalej len „EÚ“). I geograficky vzdialené udalosti a procesy totiž môžu ohroziť našu bezpečnosť - a to aj v prípade, keď samé o sebe nepredstavujú priamu hrozbu, ich dôsledky môžu zapríčiniť nestabilitu a prispieť ku



vzniku ďalších konfliktov či krízových situácií a zároveň tak k ďalšiemu šíreniu bezpečnostných hrozieb.

K najvýznamnejším procesom s rizikovým alebo konfliktným potenciálom radíme nárast moci a sily nových globálnych aktérov, slabé a zlyhávajúce štáty, posilňovanie a aktivity neštátnych aktérov, oslabovanie štátnych inštitúcií i mechanizmov medzinárodnej a regionálnej spolupráce, geograficky nevyvážený demografický vývoj, degradáciu životného prostredia a napokon vyčerpávanie prírodných zdrojov.

Medzi hlavné zdroje asymetrických bezpečnostných hrozieb patrí predovšetkým *politický radikalizmus, prehnaný nacionalizmus, ideologický a náboženský fundamentalizmus* a tiež *terorizmus*. V tejto súvislosti je potrebné zdôrazniť, že terorizmom v danom slova zmysle sa nemá na mysli terorizmus aký existoval na zemi po stáročia, ale terorizmus, ktorý môže v súčasnosti zasiahnuť kohokoľvek, kdekoľvek a kedykoľvek a ktorý je zameraný na masovú deštrukciu materiálnych hodnôt a masové zabíjanie nevinných civilistov.

Ako ďalšie hrozby môžeme označiť najmä *šírenie zbraní hromadného ničenia a ich nosičov, rastúcu dostupnosť a využiteľnosť civilných technológií pre útočné účely, kybernetické útoky na verejné i súkromné siete a organizovaný medzinárodný zločin*. Faktom zostane skutočnosť, že aj keď žiadna z týchto hrozieb nie je úplne nová, novú úroveň predstavuje predovšetkým vyššie štádium ich vzájomnej previazanosti a vyšší potenciál ich vzájomného posilňovania.

Je možné konštatovať, že členstvo v NATO a EÚ výrazne zmenilo nielen politické a ekonomické, ale aj bezpečnostné postavenie SR a vytvorilo tak kvalitatívne nové predpoklady na realizáciu jej bezpečnostných záujmov, vrátane zabezpečenia vnútornej bezpečnosti. Zmena postavenia však pre SR neznamená len posun od zabezpečenia individuálnej vnútornej bezpečnosti smerom ku „spoločnej“ európskej v rámci EÚ, ale zároveň aj skutočnosť, že bezpečnostné zložky ako základný prvok bezpečnosti SR sa stali partnerom v aliančných zväzkoch, a preto musia byť pripravené nielen na plnenie úloh bezpečnostného prostredia SR, ale rovnako na plnenie úloh v oveľa komplexnejšom strategickom a operačnom prostredí.

Súčasnú operačné prostredie je okrem iného aj vo vzťahu k aktuálnym úlohám a problémom spravodajských služieb determinované najmä:

- Doteraz pokračujúcou globalizáciou, ktorá spôsobuje prehĺbovanie neistoty a nepredvídateľnosti ďalšieho vývoja ľudstva, ako aj stále viac rastúcu závislosť štátov aliancie a únie od prírodných a energetických zdrojov, ktoré nemajú pod priamou kontrolou. Nestabilné oblasti zostanú v centre pozornosti, pričom komunikačné a informačné technológie a prostriedky pôsobiace v globálnom meradle môžu byť zneužitú teroristickými alebo extrémistickými skupinami na šírenie nepokojov cielene zameranými informačnými kampaňami a propagáciou násillia.
- Asymetrickými spôsobmi vedenia útokov a ozbrojených konfliktov, ktoré sa neustále zdokonaľujú. Liberalizácia a internetizácia spoločnosti, rozvoj

moderných technológií a ich dostupnosť postupne vytvárajú čoraz širšie možnosti ich zneužitia súčasnými alebo potenciálnymi nepriateľmi prostredníctvom nekonvenčných spôsobov násilia a ničenia.

- Nevyliešenými konfliktami, ktoré môžu jednak vytvárať živnú pôdu pre teroristické a extrémistické skupiny a organizácie a jednak byť hrozbou alebo možnou príčinou vzniku ďalších ozbrojených konfliktov.
- Prehľbujúcimi sa ekonomickými, sociálnymi a demografickými rozdielmi medzi vyspelými a rozvojovými krajinami, ktoré spolu s rastom populácie môžu byť príčinou rozsiahlej nelegálnej migrácie spojenej so zvyšovaním etnického napätia.
- Zlyhávajúcimi štátmi, ktoré v dôsledku ekonomických kolapsov, zrútenej infraštruktúry a zlého alebo nevyhovujúceho spôsobu vládnutia vytvárajú mocenské vákuum. Práve toto môže byť zneužitá neštátnymi činiteľmi, vrátane teroristov a zločincov. Za týchto podmienok môžu zlyhávajúce štáty poskytnúť útočisko medzinárodnému terorizmu a organizovanému zločinu.
- Ekologickými problémami súvisiacimi s rastúcimi požiadavkami na energetické zdroje, nerastné suroviny a potraviny a zároveň spojenými s devastáciou životného prostredia a vyčerpávaním zdrojov. Nedostatok zdrojov, surovín a potravín spolu s ich nespravodlivým prerozdeľovaním a využívaním rovnako predstavujú vhodné prostredie pre vznik konfliktov a organizovaný zločin.

Jedným zo základných predpokladov realizácie vyššie uvedených cieľov a operačných postupov je adekvátne politické, legislatívne, organizačné, ale najmä zdrojové zabezpečenie. Je zrejmé, že bez adekvátneho a stabilného financovania bezpečnosti a obrany SR, a tým aj vyčleňovania dostatočných ľudských, materiálnych a finančných zdrojov pre jej bezpečnostné zložky, tieto nebudú môcť vôbec alebo len s obmedzeniami plniť úlohy stanovené v oblasti nevojenských ohrození vládou SR alebo Ministerstvom vnútra SR.

Bezpečnostná stratégia Slovenskej republiky charakterizuje bezpečnostné hrozby a výzvy ako „*dynamické, vzájomne previazané a podliehajúce zmenám v závislosti od vnútorných, regionálnych a globálnych podmienok*“<sup>\*</sup>. Na zachovanie svojej bezpečnosti a na elimináciu týchto hrozieb a výziev používajú štáty a spoločenstvá štátov všetky dostupné prostriedky počnúc politickými cez ekonomické, informačné, psychologické až po vojenské.

Stratégia špecifikuje bezpečnostné hrozby, na ktoré musí SR reagovať a kategorizuje ich do nasledovných skupín:<sup>†</sup>

- hrozba veľkého konvenčného útoku proti územia NATO je nízka, i keď po udalostiach na Ukrajine sú prijímané opatrenia na posilňovanie síl a prostriedkov bližšie k hraniciam Ruskej federácie,
- hrozbu konvenčných zbraní nemožno ignorovať,

---

<sup>\*</sup> *Bezpečnostná stratégia Slovenskej republiky*. 2005. čl. 33.

<sup>†</sup> *Ibidem.*, čl. 17 – 32.

- šírenie jadrových zbraní a iných zbraní hromadného ničenia ako aj ich nosičov má potenciál stať sa hrozbou s nepredvídateľnými následkami pre globálnu stabilitu a prosperitu,
- terorizmus predstavuje priamu hrozbu pre bezpečnosť obyvateľov krajín NATO a v širšom meradle aj hrozbu pre medzinárodnú stabilitu a prosperitu,
- nestabilita alebo konflikt za hranicami NATO môže priamo ohroziť bezpečnosť aliancie,
- kybernetické útoky sú častejšie a lepšie organizované,
- všetky krajiny sú čoraz viac závislé na dôležitých komunikačných, transportných a tranzitných cestách, od ktorých závisí globálny obchod, energetická bezpečnosť a prosperita,
- obmedzenia v oblasti životného prostredia a zdrojov, klimatické zmeny, zdravotné riziká, nedostatok vody a zvyšujúce sa energetické potreby, budú ďalej formovať budúce bezpečnostné prostredie.

## 2. MIESTO A VÝZNAM SPRAVODAJSKÉJ ČINNOSTI V POLICAJNÝCH ČINNOSTIACH

Vykonávanie spravodajskej činnosti nie je len doménou spravodajských služieb. Uplatňuje sa aj v práci Policajného zboru. Spravodajskú činnosť považujeme za súčasť policajno-bezpečnostných činností, a preto má svoje opodstatnenie aj v činnostiach Policajného zboru.

Spravodajská činnosť v Policajnom zbore je nevyhnutná najmä pri rozkladaní a deštruovaní kriminálnych, zločineckých a teroristických skupín. Vo všeobecnosti je jej využívanie v Policajnom zbore potrebné vnímať ako podporu v boji proti organizovanej, latentnej a sofistikovanej trestnej činnosti a tiež v boji proti terorizmu. Opodstatnenosť začlenenia spravodajskej činnosti do policajných činností možno podporiť historickými súvislosťami, ale aj súčasnými potrebami boja proti organizovanému zločinu a terorizmu, ktoré potvrdzujú aj aktivity Europolu a EÚ, a to i v kontexte Európskeho modelu kriminálneho spravodajstva.

Pripomeniem, že cieľom Európskeho modelu kriminálneho spravodajstva je poznanie hrozieb v oblasti kriminality na strategickej, ako aj na operatívnej úrovni. Cieľom môže byť zmapovanie kriminálnych skupín, ktoré páchajú organizovanú trestnú činnosť alebo terorizmus, ale aj určenie väzieb a vzťahov medzi jej jednotlivými členmi, zistenie oficiálnych a neoficiálnych podnikateľských aktivít, zisťovanie režimu jednotlivých členov, hlavne v hierarchii riadenia organizovanej skupiny najvyššie postavených a pod.\* Takto stavené ciele v súčasnej dobe korešpondujú aj s činnosťou subjektov Policajného zboru, ktoré plnia úlohy na úseku kriminálneho spravodajstva.†

---

\* Zborník ABSD, In: *Skúsenosti s fungovaním spravodajských služieb v postkomunistických krajinách*. Poradca podnikateľa, spol. s. r.o. : Žilina, r. 2013, s. 49.

† Ibidem, s. 49.

Významným argumentom na začlenenie spravodajskej činnosti do policajných činností je súčasná bezpečnostná situácia v oblasti organizovaného zločinu a v oblasti terorizmu - o to viac, že vznikajú „nové“ hrozby a s tým súvisiace výzvy. Je potrebné si uvedomiť, že organizovaná kriminalita spolu s novými hrozbami a výzvami je fenoménom prospievajúcim k prehodnocovaniu doposiaľ „tradičných“ a „riešených“ hrozieb súčasného sveta, a teda i k „prirodzeným“ zmenám operačného prostredia.

Zmeny politického, ekonomického, ekologického a bezpečnostného charakteru, ktoré aktuálne prebiehajú v dnešnom svete ako na globálnej tak i na „regionálnej“ úrovni, ktorú je možné vnímať ako „európsku“ ale aj „národnú“, prirodzene generujú nové vážne doposiaľ nepoznané hrozby, s tým súvisiace výzvy a potrebu ich vzhľadom k procesom zmien riešiť s nebývalou dynamikou.

Spravodajská činnosť je súčasťou policajno-bezpečnostných činností, predstavuje ich samostatný podsystém tvorený jednotlivými prvkami:

1. Objekt a predmet spravodajskej činnosti.
2. Princípy, ciele a úlohy spravodajskej činnosti.
3. Spravodajský cyklus.
4. Subjekt spravodajskej činnosti, organizácia a riadenie spravodajskej činnosti.
5. Metódy, formy a prostriedky spravodajskej činnosti.

Okrem „tradičnej“ organizovanej kriminality existujú i nové formy súvisiace s registrovanými hrozbami, a to sa stáva „*nemocou (chorobou), patológiou spoločnosti - nepriateľom spoločnosti*“. Na každú chorobu však existuje liek. Základom úspešnej liečby je presná diagnostika choroby od príčin jej vzniku cez jej prejavy až po následky. Uvedené axiómy možno aplikovať aj pri boji proti organizovanej kriminalite ako novým hrozbám.

*„Primeraná odpoveď na sociálne, politické a ekonomické hrozby, ktoré predstavuje organizovaná kriminalita, vyžaduje dokonalé pochopenie jej koreňov, pováh a pravdepodobnosti úspechov zvláštnych typov protiopatrení“.* Politika, ktorá je vykonávaná bez takéhoto pochopenia, má chyby v samých základoch a je odsúdená na neúspech. Bez pochopenia vzťahov medzi jednotlivými faktormi nie je možné problémy nových hrozieb a výziev riešiť, a tak adekvátne reflektovať i na zmeny v operačnom pôsobení spravodajských služieb, policajný zbor nevynímajúc. Preto je potrebné analyzovať nebezpečenstvo, zákerné, mnohotvárne, vytvárajúce množstvo hrozieb, ktoré môžeme vo všeobecnosti charakterizovať ako:\*

- *Hrozba pre nezávislosť a suverenitu jednotlivých krajín.* Národné hranice, ktoré sú základným symbolom suverenity štátu, nie sú pre väčšinu medzinárodne organizovaných kriminálnych skupín prekážkou a v dnes značne globalizovanom svete ani pre väčšinu „nových hrozieb“ a ich aktuálnych výziev. Priechodnosť hraníc je tak veľká, že ohrozuje základný symbol „národného štátu“ - suverenitu. Ako „flagrantný“ príklad porušenia suverenity je možné vidieť napr. činnosť Islamského štátu a jeho ozbrojených

---

\* Zborník ABSD, In: *Spravodajské služby v demokratickej spoločnosti*. Poradca podnikateľa, spol. s. r. o. : Žilina, r. 2009, s. 45-47.

štruktúr bez väčších problémov na území Iraku, Sýrie, ktoré sú formálne pod kontrolou, nie sú však schopné zabezpečiť kontrolu nad takými formami činnosti a jej rozsahu organizovania a pôsobenia až konkurujúcich činnosti štátnych orgánov, čím spomenuté štáty de facto strácajú svoju suverenitu. Z doterajšieho vývoja je zrejmé, že podobným „hrozbám“ prameniaticim skôr a zatiaľ „len v sprievodných činnostiach a javoch spojených s napr. s existenciou Islamského štátu“ už dnes čelia viaceré krajiny ekonomicky vyspelého a politicky demokraticky usporiadaného „západného sveta“.

- *Hrozba pre spoločenskú štruktúru.* Expanzia kriminálnych skupín a ich nekontrolovaných aktivít spôsobuje spochybnenie základných právnych, politických a spoločenských hodnôt. Skupiny si vytvárajú svoje vlastné hodnoty, zastrašovaním a korupciou organizovaná kriminalita podkopáva základy legitímnych inštitúcií a potiera ich hodnotový základ, ktorý je „imanentnou súčasťou“ demokracie.
- *Hrozba pre stabilitu a riadenie štátu.* Organizovaná kriminalita pôsobí ako štát v štáte založený na fungovaní „tieňovej ekonomiky“, pričom získava výsadnejšie postavenie. Kriminálne skupiny si vytvárajú „silový monopol“, za pomoci násillia a zastrašovania zaisťujú disciplínu a pomocou korupcie prenikajú do vlád nielen na miestnej úrovni, ale aj na národnej úrovni. Organizovaná kriminalita svojou podstatou podkopáva stabilitu demokratickej a občianskej spoločnosti, do riadenia štátu vnáša nestabilitu, nepokoj a narúša normálne fungovanie vlády a zákona, čím si samozrejme generuje aj „vhodné prostredie pre svoj rast“.
- *Hrozba pre demokraciu.* Kriminálne skupiny sa pomocou korupcie snažia neutralizovať činnosť vlád v boji proti kriminalite a dosiahnuť, aby nepodnikali žiadne alebo len formálne kroky na jej potlačanie. V tomto prípade organizovaná kriminalita nenapáda štát otvorene, ale nečinnosť vlád a štátnych orgánov sa snaží dosiahnuť skrytou formou.
- *Hrozba pre národnú ekonomiku.* Organizovaná kriminalita tým, že vytvára tieňovú ekonomiku, spôsobuje znižovanie daňových príjmov a má negatívny vplyv na ekonomickú rovnováhu a ekonomický rozvoj na celospoločenskej úrovni.
- *Hrozba pre finančné inštitúcie.* Množstvo ziskov, ktoré sú produktom organizovanej kriminality a ktoré sú legalizované prostredníctvom legálnych finančných inštitúcií, má vážny a dlhodobý negatívny vplyv na dôveru vo finančný systém a legálne finančné inštitúcie.
- *Hrozba pre jednotlivca.* Organizovaná kriminalita používa násillie k ochrane svojho teritória a ziskov a násillie proti ľuďom a majetku. V tomto kontexte má silný sociálny vplyv a predstavuje veľké nebezpečenstvo pre jednotlivca, keďže bezpečnosť jednotlivca je nepriamo úmerná násilliu v spoločnosti podmienenému práve aktivitami organizovanej kriminality.\*

---

\* Zborník ABSD, In: *Spravodajské služby v demokratickej spoločnosti*. Poradca podnikateľa, spol. s.r.o.: Žilina, r. 2009, s. 45-47.

Získané poznanie, aj s využitím spravodajskej činnosti, je možné následne zúročiť pri realizácii krokov tak, aby došlo k prerušeniu aktivít organizovaných, zločineckých a teroristických skupín, ale aj k obmedzeniu ich ziskov. Akákoľvek spoločnosť, ktorá poznáva organizovanú kriminalitu, nesmie podceňovať schopnosť svojho protivníka na tomto poli, ak chce byť schopná mu porozumieť a poznať jeho silné a slabé stránky.\*

Tieto skutočnosti, kontext ich vzniku a dynamiky si uvedomuje aj Európska únia a Europol, ktorý vypracoval Európsky model kriminálneho spravodajstva (skratka – ECIM) a ktorý mieni zaviesť do policajnej praxe vo všetkých krajinách EÚ. V nadväznosti na tieto aktivity Europolu bolo v súlade s Haagskym programom uznesením vlády SR č. 63/2008 z 23. januára 2008 uložené Ministerstvu vnútra SR v termíne do 30. júna 2008 zaviesť do praxe zmienený model s cieľom jeho spustenia v roku 2008.

Európsky model kriminálneho spravodajstva je chápaný ako štandardizovaný systém práce s informáciami, zberom, spracovávaním, analyzovaním a následným postupovaním a využívaním týchto informácií. Jeho hlavným produktom je hodnotenie hrozieb organizovaného zločinu a zároveň je nástrojom na implementáciu spravodajského riadenia presadzovania práva, a teda aj spravodajského vedenia policajných jednotiek.

Je na mieste pripomenúť, že odporúčania Európskeho modelu kriminálneho spravodajstva nemajú záväzný charakter v zmysle ich striktnej a časovo vymedzenej implementácie, je na členských krajinách akým spôsobom jednotlivé odporúčania implementujú.

### **3. OBJEKT A PREDMET SPRAVODAJSKEJ ČINNOSTI POLICAJNÉHO ZBORU**

Vykonávaním spravodajskej činnosti v Policajnom zbore sa má zabezpečiť plnenie úloh Policajného zboru uvedených v § 2 zákona č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov, najmä úloh pri ochrane základných práv a slobôd, pri odhaľovaní daňových únikov, nezákonných finančných operácií a legalizácie príjmov z trestnej činnosti a pri boji proti terorizmu a organizovanému zločinu.

Objekt spravodajskej činnosti vykonávanej v rámci Policajného zboru môžeme chápať v dvoch rôznych podobách, a to ako objekt všeobecný a ako objekt konkrétny. *Všeobecným objektom*, ktorý spravodajskou činnosťou poznávame, teda predmetom jej záujmu v tom najširšom slova zmysle, je *kriminalita*.

Pojem kriminalita pochádza z latinského „crimen - zločin“ a vychádza z pojmu trestný čin vymedzený v platnom trestnom práve. Predstavuje súhrn sociálne škodlivých javov stanovených v trestných kódexoch, pričom je formou deviantného správania v rozpore s normami uvedenými v Trestnom zákone, ktorú tvorí súhrn

---

\* OSN, Hospodárska a sociálna rada: Problémy a nebezpečenstvá, ktoré predstavuje organizovaný medzinárodný zločin v rôznych oblastiach sveta, In.: *Základný dokument konferencie, Svetová ministerská konferencia o organizovanom transnacionálnom zločine, Neapol, 21. - 23.11. 1994*, s. 8.

trestných činov spáchaných v príslušnej spoločnosti, štáte či regióne.\* V súvislosti s uvedeným je potrebné si uvedomiť, že aj napriek existencii mnohých štatistík, ich štatistické ukazovatele nám neposkytujú obraz o skutočnej kriminalite. Zachytávajú len kriminalitu známu.

Z uvedenej charakteristiky objektu spravodajskej činnosti, t.j. spáchanej kriminality na území SR za príslušný rok, možno vidieť, že objekt nie je len dynamický, ale aj „mnohokomponentný“, a preto je jeho poznávanie potrebné zamerať len na niektoré jeho aspekty, ktoré *predstavujú predmet spravodajskej činnosti*. Ide o aspekt latencie a organizovanosti.

Väčšina odborníkov z oblasti kriminológie, kriminalistiky a trestného práva chápu *latentnú trestnú činnosť* ako trestnú činnosť, ktorá zostáva utajená a pre policajné orgány a orgány činné v trestnom konaní neznáma. Napriek tomu, že tieto o jej existencii vedomosť nemajú, dokonca o nej mnohokrát nemá vedomosť ani sám poškodený, reálne existuje, resp. bola spáchaná.

Rozhodujúcimi kritériami na rozlíšenie latentnej kriminality od kriminality známej, či už so známym alebo neznámym páchatelom, je existencia dvoch podmienok:

- určitého konania, ktoré sa prejavuje ako pre spoločnosť nebezpečný čin a ktorého znaky sú uvedené v Trestnom zákone,
- prekážky (vedomej alebo nevedomej), ktorá bráni poznaniu a zaregistrovaniu tohto konania políciou alebo orgánmi činnými v trestnom konaní (odhaleníu, oznámeniu).

Na základe vyššie formulovaných kritérií možno latentnú kriminalitu definovať ako reálne existujúcu trestnú činnosť, ktorá zostáva z rôznych dôvodov (nevedomosť, nejednoznačná kvalifikácia, neodhalenosť a pod.) pre orgány polície a orgány činné v trestnom konaní utajená a neznáma a nie je ani nikde štatisticky podchytená.

Existencia latentnej kriminality má negatívne vplyvy a dôsledky na znižovanie právneho vedomia jednotlivcov a celej spoločnosti. Je nesporné, že čím väčší je nepomer latentných trestných činov k počtu registrovaných trestných činov (odhalených, zistených), tým viac sa prehĺbuje rozpor vo všeobecnom záujme spoločnosti na ochrane občanov a ich majetku. Latentná kriminalita jednoznačne vytvára podmienky na recidívu, pretože neodhalenie trestnej činnosti páchatelov utvrdzuje v „neodhaliteľnosti“ nimi páchaných činov, čo v konečnom dôsledku spôsobuje ich pokračovanie v konkrétnej trestnej činnosti alebo páchanie ďalšej.

Existencia latentnej kriminality má negatívny vplyv aj na poznanie skutočného stavu kriminality, jej dynamiky, štruktúry, vývoja a príčin. Má za následok vytváranie nedôvery voči orgánom činným v trestnom konaní a polícii, čo v konečnom dôsledku vedie k ľahostajnosti, pasivite a k zmiereniu s negatívnou situáciou v bezpečnostnej oblasti. Nedôvera občanov v políciu spôsobuje, že spáchané trestné činy

---

\* ONDREJKOVIČ, P., BREZÁK, J., VLČKOVÁ, M.: *Sociálna patológia ako predmet pozornosti sociálnej práce, sociálnej pedagogiky a vychovávateľstva*, 1. vydanie, Bratislava: PF UK, 1999, ISBN 80-88868-47-5, s.60-61.

neoznamujú a nespolupracujú pri ich objasňovaní, čím sa miera objasnenosti kriminality znižuje. Nízka miera objasnenosti zapríčiňuje nedôveru občanov v políciu, negatívne pôsobí na efektívnosť jej práce, čo zase vytvára dôvody na neoznamovanie a slabú spoluprácu pri objasňovaní trestných činov. Tento „bludný kruh“ nemecký kriminológ H. J. Schneider nazýva „efektom spätnej väzby“. Uvedené skutočnosti potvrdzujú i výsledky získané niektorými výskumami v SR. Podľa prieskumu Odboru verejnej mienky Slovenského rozhlasu z mája 2004 Policajnému zboru dôveruje 40,6 % opýtaných občanov. V zisťovaní dôvery polícii komparatívnou metodikou dôvery rôznych inštitúcií má SR až o 20 % nižšiu dôveru oproti 61 % priemernej úrovne dôvery všetkých štátov Európskej únie.\*

Dôležitým aspektom determinujúcim predmet spravodajskej činnosti je organizovanosť. Je prirodzené, že spravodajská činnosť nebude zameraná na jednoduchú pouličnú kriminalitu, prostú a známu kriminalitu a pod., ale práve na organizovaný zločin vo všetkých jeho podobách.

Ako už bolo spomenuté popri klasických formách kriminality sa do popredia dostávajú nové formy trestnej činnosti páchanej kriminálnymi skupinami (organizovanými, resp. zločineckými skupinami). Organizovaná kriminalita je tak neprehliadnuteľnou súčasťou dnešnej doby a v oblasti kriminality predstavuje „novú kvalitu“. Spoločenská nebezpečnosť trestných činov sa zvýšila, objavili sa nové formy najzávažnejších trestných činov a vzrástla agresivita kriminálnych skupín. Organizovaná trestná činnosť je páchaná plánovane, dlhodobo s orientáciou na vysoký zisk, pričom sa zároveň realizujú aj opatrenia proti jej odhaleniu a trestnému postihu. Hlavným cieľom organizovanej kriminality je teda dosiahnutie maximálneho finančného zisku bez ohľadu na použité prostriedky a oblasť podnikania. Práve zisk je jej hnacím motorom, jej súčasťou a cieľom. Jednou z hlavných úloh a snáh kriminálnych skupín je zlegalizovať príjmy z trestnej činnosti tak, aby vzbudzovali dojem zákonnosti a legálnosti.

Členovia kriminálnych skupín sa z týchto dôvodov snažia zaviesť zisky z trestnej činnosti do legálneho finančného systému, t.j. „preprať ich“. Legalizácia príjmov z trestnej činnosti - častokrát označovaná aj ako „pranie špinavých peňazí“ - je sprievodným znakom organizovanej kriminality a zároveň jej integrálnou súčasťou. Z uvedeného dôvodu je nevyhnutné zo strany štátu a spoločnosti prijímať adekvátne opatrenia na zamedzenie akýchkoľvek možností legalizovať príjmy nadobudnuté trestnou činnosťou. Internacionalizácia a intelektualizácia kriminality bude posilňovaná zdokonaľovaním jej organizovaných foriem a bude stavať vlády aj tých najvyspelejších a najbohatších krajín sveta do takmer bezvýchodiskového postavenia, keď nebudú schopné spoľahlivo ochrániť pred zločinom svojich občanov a možno ani seba.

Všeobecný predmet spravodajskej činnosti v Policajnom zbore predstavuje najmä latentná organizovaná kriminalita a terorizmus vo všetkých ich podobách. *Konkrétny objekt* spravodajskej činnosti v Policajnom zbore predstavuje *konkrétna trestná činnosť, trestná udalosť, osoba páchatela. Konkrétny predmet tvorí organizované, resp. teroristické skupiny, vrátane ich členov, legálnych a nelegálnych aktivít.*

---

\* Prezentované údaje boli publikované v rámci signálnej správy z výskumu verejnej mienky k vedeckej úlohe „Vývoj dôveryhodnosti PZ a analýzy faktorov, ktoré ju ovplyvňujú“.



Na účely Trestného zákona\* sa *organizovanou skupinou* rozumie spoločenie najmenej troch osôb na účel spáchania trestného činu s určitou del'bou určených úloh medzi jednotlivými členmi skupiny, ktorej činnosť sa v dôsledku toho vyznačuje plánovitosťou a koordinovanosťou, čo zvyšuje pravdepodobnosť úspešného spáchania trestného činu.

*Zločineckou skupinou* sa na účely tohto zákona rozumie štruktúrovaná skupina najmenej troch osôb, ktorá existuje počas určitého časového obdobia a koná koordinovane s cieľom spáchať jeden alebo viacej zločinov, trestný čin legalizácie príjmu z trestnej činnosti podľa § 233 Trestného zákona alebo niektorý z trestných činov korupcie podľa ôsmej hlavy tretieho dielu osobitnej časti zákona na účely priameho alebo nepriameho získania finančnej alebo inej výhody.

*Teroristickou skupinou* sa na účely Trestného zákona rozumie štruktúrovaná skupina najmenej troch osôb existujúca počas určitého časového obdobia na účely spáchania trestného činu teroru alebo trestného činu terorizmu.

Trestnou je aj *činnosť pre zločineckú alebo teroristickú skupinu a ich podpora*. Činnosťou pre zločineckú alebo teroristickú skupinu sa rozumie úmyselná účasť v takej skupine alebo iné úmyselné konanie na účel zachovania existencie takej skupiny alebo spáchania vyššie zmienených trestných činov takou skupinou.

Podpora zločineckej alebo teroristickej skupiny predstavuje úmyselné konanie spočívajúce v poskytnutí prostriedkov, služieb, súčinnosti alebo vytváranie iných podmienok na účel založenia alebo zachovania existencie takej skupiny či spáchania vyššie uvedených trestných činov takou skupinou.

Konkrétny predmet spravodajskej činnosti sa bude neustále meniť, a to v závislosti na prijatej spravodajskej stratégii, kedy sa spravodajská pozornosť bude venovať konkrétnej organizovanej alebo teroristickej skupine, t.j. jej nelegálnym, ale aj legálnym aktivitám, zloženiu, vzájomnej komunikácii medzi členmi, možnostiam preniknutia do takejto skupiny s cieľom deštruovať jej logistické zabezpečenie, zisťovať spáchanú trestnú činnosť, ktorá je latentná, jej plánované nezákonné akcie a podobne.

#### **4. CIEĽ A ÚLOHY SPRAVODAJSKEJ ČINNOSTI V POLICAJNOM ZBORE**

*Cieľom je poskytovať spravodajské informácie oprávneným konkrétnym užívateľom k rozhodovaciemu procesu na prijímanie opatrení v oblasti kontroly kriminality.* Obsah spravodajských informácií je tvorený v závislosti od objektu a predmetu spravodajskej činnosti.

Ak je objekt a predmet všeobecný, t.j. kriminalita, resp. organizovaný zločin alebo terorizmus, tak aj cieľ spravodajskej činnosti bude formulovaný ako všeobecný a bude zameraný na elimináciu kriminality, organizovanej trestnej činnosti alebo terorizmu. Ak bude objekt a predmet spravodajskej činnosti individuálny, t.j. konkrétna zločinecká organizácia alebo teroristická skupina, tak potom cieľom bude

---

\* Zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov, § 129.

eliminácia nezákonných aktivít konkrétnej organizovanej alebo teroristickej skupiny, organizácie.

Cieľ spravodajskej činnosti je teda podmienený objektom a predmetom poznávania. V prípade všeobecného cieľa budú úlohy smerovať k eliminácii kriminality ako takej alebo k eliminácii organizovaného zločinu a terorizmu. Ak bude cieľom konkrétna organizovaná alebo teroristická skupina, tak úlohy budú prijímané na elimináciu jej nelegálnej činnosti.

Tak ako bolo uvedené vyššie, ak je objekt a predmet spravodajskej činnosti všeobecný, potom aj cieľ spravodajskej činnosti je všeobecný, t.j. poznávanie organizovaného zločinu a terorizmu vo všetkých jeho podobách. Cieľ spravodajskej činnosti je de facto strategický, a preto sa takáto spravodajská činnosť označuje tiež ako *strategické spravodajstvo*. Na zabezpečenie *všeobecného cieľa* strategickej spravodajskej činnosti v Policajnom zbore sú prijímané úlohy na kontrolu kriminality, najmä v oblasti:

- legislatívy,
- organizácie a riadenia Policajného zboru,
- taktiky a metodiky.

*Úlohy v oblasti legislatívy* predstavujú prijímanie konkrétnych zákonov a iných všeobecne záväzných právnych predpisov, ktorých cieľom je eliminácia nelegálnych činností, vrátane trestnej činnosti, najmä jej najzávažnejších foriem (organizovaný zločin, pranie špinavých peňazí, terorizmus a pod.) na úsekoch prevencie alebo represie. Prijímané zákony „zužujú priestor“ na páchanie trestnej činnosti a vytvárajú podmienky na efektívnejší boj proti konkrétnemu druhu kriminality. Samozrejme dávajú aj možnosť a priestor na sankcionovanie, vrátane trestného postihu konkrétnych subjektov.

*Úlohy v oblasti organizácie a riadenia Policajného zboru* sú prijímané v prípadoch, keď na základe spravodajských informácií možno spozorovať nárast určitého druhu kriminality (napr. drogovej, finančnej a pod.) na celom území alebo v niektorom jej teritóriu (kraj, okrese). Obdobne aj v prípade zaznamenania nových druhov kriminality (karuselové podvody a pod.) bude prirodzene Policajný zbor reagovať prijímaním opatrení v oblasti organizácie a riadenia.

Ako príklad je možné použiť vznik Úradu boja proti korupcii, pretože korupcia začala v SR spôsobovať vážne celospoločenské problémy. Obdobne to bolo pri vytvorení služby finančnej polície pri enormnom náraste finančnej kriminality a prania špinavých peňazí.

*Úlohy v oblasti taktiky a metodiky* spočívajú najmä v spracovávaní taktických a metodických pomôcok, rôznych nariadení ministra vnútra SR, ktoré majú zefektívniť boj proti jednotlivým druhom trestnej činnosti.

Je potrebné znovu zdôrazniť, že organizované skupiny utajujú svoju trestnú činnosť, prijímajú opatrenia na zabránenie jej odhalenia, vrátane získavania vplyvu v polícii prostredníctvom korupcie a pod., čo zákonite musí viesť k tomu, aby Policajný zbor na tieto skutočnosti reagoval adekvátne aj v oblasti taktických a metodických postupov polície.

Medzi ďalšie úlohy prijímané na zabezpečenie všeobecného strategického cieľa možno zaradiť:

- mapovanie jednotlivých druhov kriminality, ich výskyt a rozloženie na území SR,
- mapovanie množstva a rozmiestnenie zločineckých a teroristických skupín na území SR,
- mapovanie vzťahov medzi jednotlivými organizovanými alebo teroristickými skupinami (vzájomná spolupráca alebo konkurencia, rozdelenie vplyvu a pod.),
- zisťovanie nových foriem páchanej kriminality a pod.

V prípade plnenia individuálneho, *konkrétneho*, cieľa je predmetom poznávania konkrétna organizovaná alebo teroristická skupina a tento cieľ je možné označiť ako operatívny alebo taktický (pojem používaný v západnej Európe). Výkon spravodajskej činnosti sa preto tiež nazýva taktickým alebo operatívnym spravodajstvom.

*Operatívnym spravodajstvom* sú prijímané rôzne úlohy, ktoré vedú k odhaľovaniu a predchádzaniu páchania konkrétnej trestnej činnosti. Hlavné úlohy sú zamerané na :

- identifikáciu členov konkrétnej kriminálnej alebo teroristickej skupiny,
- mapovanie ich pohybu,
- mapovanie ich kriminálnych aktivít,
- mapovanie ich legálnych podnikateľských aktivít,
- rozkladanie kriminálnej alebo teroristickej skupiny zvnútra (aj za použitia legalizanta),
- narúšanie logistiky kriminálnej alebo teroristickej skupiny (napr. narúšanie vzájomnej komunikácie medzi členmi kriminálnej skupiny),
- zabránenie investovania príjmov z trestnej činnosti do legálnej ekonomiky,
- dočasné zaisťovanie ziskov získaných z trestnej činnosti a iné.

Všetky tieto úlohy musia byť integrované do jedného komplexného systému a musia zahrňovať aj spoluprácu v oblasti boja proti legalizácii výnosov z trestnej činnosti kriminálnych skupín, v oblasti boja proti terorizmu a aj prejavom zavražďovania, ako aj v oblasti boja proti korupcii.

## **5. OBSAH SPRAVODAJSKEJ ČINNOSTI V POLICAJNOM ZBORE**

Vychádzajúc zo spomínaného spravodajskú činnosť vykonávanú Policajným zborom možno chápať ako cieľavedomú, systematickú poznávaciu činnosť, ktorou kompetentní pracovníci Policajného zboru využívaním špecifických metód, prostriedkov a foriem utajene, plánovito získavajú, spracovávajú informácie a vytvárajú spravodajské informácie pre konkrétnych užívateľov (adresátov) za účelom zvýšenia úrovne kontroly kriminality. Spravodajská činnosť má povahu poznávacej činnosti (poznávacieho procesu), kde sa zo štádia neznalosti postupuje ku konkrétnemu poznaniu.

Z pohľadu obsahu je podstatou spravodajskej činnosti práca s *informáciami*, teda ich získavanie, spracovávanie (hodnotenie, triedenie, ukladanie a analyzovanie) a ich interpretácia. Zmienené potvrdzuje aj názor amerických kriminalistov D.

Herberta a H. Tritta, ktorí konštatujú, že „*cieľom a prostriedkom akejkoľvek efektívnej reakcie na hrozbu organizovaného zločinu je informácia*“. Citovaný názor jasne odzrkadľuje podstatu prístupu zainteresovaných subjektov (polície, tajných služieb a pod.) v rozvinutých štátoch k hrozbe organizovaného zločinu. V praktickej rovine sa najväčší dôraz kladie na zber, vyhodnotenie a spracovanie informácií o zločineckých a teroristických organizáciách. „*Kvalitná informácia predstavuje kľúč k spoľahlivej politike a stratégii kontroly organizovaného zločinu*“, tvrdia J. Dintino a F. Martens.

V podstate tohto prístupu tkvie jasné chápanie toho, že hlavný objekt pôsobenia bezpečnostných zložiek v danej sfére (zločinecké organizácie) predstavuje jednotný celok. „*Naším dnešným hlavným cieľom nie je boj proti individuálnym malým zlodejom, ale likvidácia veľkých zločineckých organizácií*“, zdôraznil riaditeľ amerického Federálneho úradu pre vyšetrovanie William S. Sessions. „*Prostredníctvom metódy vyriešenia konkrétneho prípadu možno usvedčiť len individuálne osoby, ktoré budú bez problémov nahradené v rámci zločineckej skupiny...*“, tvrdia švajčiarski kriminalisti.

Ak chcú orgány činné v trestnom konaní seriózne bojovať proti organizovanému zločinu, musia zadefinovať hlavný cieľ. Tým je likvidácia organizácie prostredníctvom usvedčenia maximálneho počtu jej členov, v prvom rade jej lídrov. Na tento účel je potrebné precízne preskúmať celý „organizmus“ zločineckej formácie.

Výsledkom a konečným produktom spravodajskej činnosti je spravodajská informácia. Spravodajská činnosť nie je jednorazovým aktom či jednorazovou činnosťou, ale predstavuje súbor činností vykonávaných v určitej postupnej následnosti. V zásade je procesom, ktorý má - tak, ako aj iné poznávacie činnosti - svoje etapy, resp. fázy, ktoré spolu tvoria tzv. spravodajský cyklus.

Spravodajský cyklus má nasledovné etapy:

1. Zadanie požiadavky a definovanie problému.
2. Zber informácií.
3. Spracovanie informácií (triedenie, ukladanie, hodnotenie a analýza).
4. Interpretácia spravodajskej informácie (logického záveru).
5. Vyhodnotenie spravodajského cyklu.

V spravodajskom cykle sa pracuje s informáciami, a to od ich zberu cez zhromažďovanie, hodnotenie, porovnávanie, analyzovanie, distribúciu a plánovanie. Na spravodajský cyklus môžeme nazerať buď z pohľadu organizácie ako celku alebo z cez optiku určitej spravodajskej úlohy, či už strategickej alebo operatívnej.

Informácia alebo pochopenie problému sa rozpracovávajú vo viacerých kolách. Významnú úlohu tu zohráva neustála spätná väzba. Po zhromaždení, porovnaní a analýze informácií sa objavia ďalšie potreby, na ktoré sa je potrebné zamerať a ktoré na začiatku zrejme neboli. To znamená nové zhromažďovanie - avšak viac špecifické - a cyklus sa znova opakuje. Výsledná analýza je už podrobnejšia a stručnejšia, ako tá na predchádzajúcom stupni. Z praktického hľadiska je teda možné skôr hovoriť o spravodajskej špirále než o cykle.

Spravodajský cyklus sa tradične popisuje ako postupná metóda, ale v praxi ide o dynamický proces reagujúci na zmeny situácie a operatívne potreby.

Žiadna jeho etapa nie je dôležitejšia než iné, pretože všetky navzájom súvisia.

## **6. SUBJEKT SPRAVODAJSKÉJ ČINNOSTI V POLICAJNOM ZBORE A ŠPECIFICKÉ PROSTRIEDKY**

Opätovne zdôrazňujem, že spravodajská činnosť ako špecifická poznávacía činnosť so všetkými jej prvkami nie je vykonávaná len spravodajskými službami, ale spravodajské činnosti ako také sú aj súčasťou policajno-bezpečnostných činností a v činnostiach Policajného zboru majú svoje opodstatnenie.

Pri zabezpečovaní úloh spravodajskej činnosti v Policajnom zbore, ale najmä pri rozkladaní a deštruovaní kriminálnych skupín je vytvorené špecializované pracovisko, odbor špecializovaných služieb Prezídia Policajného zboru,<sup>†</sup> ktoré pripravuje najmä podmienky a možnosť nasadenia legalizanta a agenta do záujmového prostredia. Spravodajská činnosť ako podpora v boji proti kriminalite je aplikovaná aj operatívnymi službami Policajného zboru (služba kriminálnej polície, služba finančnej polície), ktoré pôsobia na úseku boja proti organizovanej trestnej činnosti, korupcii, terorizmu a pod.

Do 31. decembra 2012 bol relevantným subjektom plniacim úlohy kriminálneho spravodajstva odbor zvláštnych operatívnych činností - od 1. januára 2013 je to odbor špecializovaných služieb Prezídia Policajného zboru, ktorý je výkonným spravodajským pracoviskom s celorepublikovou pôsobnosťou vykonávajúci úlohy v oblasti kriminálneho spravodajstva, zabezpečovania plnenia úloh agenta podľa podmienok upravených zákonom. Odbor ďalej centrálné zabezpečuje nasadenie legalizanta Policajného zboru, vedie databázu legalizantov a koordinuje ich nasadenie v jednotlivých prípadoch podľa osobitného predpisu, pričom otázky osobitostí služobného pomeru a výkon služby podliehajú v zmysle osobitného predpisu zvláštnemu režimu.

V prípade vykonávania spravodajskej činnosti pracovníkmi spravodajského pracoviska alebo útvaru Policajného zboru vykonávajúceho spravodajskú činnosť, títo môžu v súlade s platnými zákonnými normami využívať:

- prostriedky operatívno-pátracej činnosti,
- informačno-technické prostriedky.<sup>‡</sup>

Prostriedky operatívno-pátracej činnosti sú najmä :

- sledovanie osôb a vecí,
- monitorovanie osôb a dopravných prostriedkov,
- kontrolovaná dodávka,
- kriminálne spravodajstvo, legalizant a agent,
- používanie krycích dokladov,
- nástrahová a zabezpečovacia technika,
- osoby konajúce v prospech Policajného zboru,

---

\* Bližšie pozri STIERANKA, J., *Základy spravodajskej činnosti*, Bratislava 2008, Akadémia PZ v Bratislave, ISBN 978-80-8054-443-0, s. 7-13

<sup>†</sup> Pozn.: v minulosti, do 31. 12. 2012 tiež známy pod názvom: „Odbor zvláštnych operatívnych činností PPZ SR“.

<sup>‡</sup> Zákon č. 171/1993 Z. z. o policajnom zbore v znení neskorších predpisov, § 39 a.

- objekty a miesta používané pod legendou,
- predstieraný prevod veci.\*

Vzhľadom na to, že používanie niektorých prostriedkov operatívno-pátracej činnosti je upravené v interných normách Ministerstva vnútra SR, ktoré majú charakter utajovaných skutočností, rozoberať v tomto referáte je možné len tie, ktoré sú verejne prístupné, resp. definované v zákonoch, a nie sú utajovanými skutočnosťami. V kontexte tejto skutočnosti a z dôvodu praktických skúseností rozoberiem najmä nasledovný prostriedok.

*Kriminálnym spravodajstvom* sa rozumie činnosť, ktorou sa utajeným spôsobom získavajú, sústreďujú a vyhodnocujú informácie o trestných činoch a ich páchateloch a vytvárajú sa podmienky na použitie agenta. Na plnenie úloh na úseku kriminálneho spravodajstva možno použiť policajta-legalizanta, ktorý koná pod trvalou legendou alebo dočasnou legendou. Policajt, ktorý koná pod trvalou legendou alebo dočasnou legendou, môže byť pri plnení úloh na úseku kriminálneho spravodajstva, za podmienok ustanovených v osobitnom predpise, použitý ako agent.<sup>†</sup>

Organizovaný zločin je vážnou hrozbou predovšetkým kvôli skutočnosti, že je rezistentným voči tradičným spôsobom vyšetrovania, kde existuje miesto činu a dôkazný materiál na jednom mieste. Práve kriminálne spravodajstvo sa ukázalo ako jedna z najúčinnějších zbraní proti nemu. Prepracované spravodajstvo a úspešná infiltrácia informátorov alebo agentov do kriminálneho prostredia pôsobí ako metóda, ktorá prináša výsledky. Úloha kriminálneho spravodajstva je o to závažnejšia, že políciu môže upozorniť na ešte latentné kriminálnej činnosti.

Aj napriek zjavnej dôležitosti kriminálneho spravodajstva, neexistuje v SR rozšírejší výskum, ktorý by rozkrýval jeho mechanizmy, rozoberal jednotlivé prostriedky, ktorými policajné útvary v rámci kriminálneho spravodajstva disponujú a načrtával metódy ich použitia v praxi, prípadne, ktorý by analyzoval a sumarizoval slabiny súčasného systému a navrhol možnosti ich riešenia, a tak flexibilne v kontexte zmien operačného prostredia spravodajských služieb prispôbil celý koncept kriminálneho spravodajstva aktuálnym úlohám a problémom s jasným odlíšením od práce a poslania spravodajských služieb.

## **7. AKTUÁLNE ÚLOHY A PROBLÉMY DETERMINUJÚCE SÚČASNÉ OPERAČNÉ PÔSOBENIE V PROSTREDÍ POLICAJNÉHO ZBORU**

V súvislosti s evidovaním informačnej produkcie zo strany napríklad Slovenskej informačnej služby (ďalej „SIS“) za rok 2015 v rámci spolupráce s Ministerstvom vnútra SR a Policajným zborom možno konštatovať, že táto sa týkala najmä bezpečnostnej a ekonomickej oblasti, kedy v oblastiach Strategického zamerania SIS v roku 2015 pre externých príjemcov, vrátane Ministerstva vnútra SR a Policajného zboru, vypracovala 352 spravodajských produktov, z toho 212 (60 %) v bezpečnostnej (pre Ministerstvo vnútra SR: 194, pre prezidenta Policajného zboru: 181), 78 (22 %) v ekonomickej (pre Ministerstvo vnútra SR: 54, pre prezidenta

\* Zákon č. 171/1993 Z. z. o policajnom zbore v znení neskorších predpisov, § 39.

† Zákon č. 171/1993 Z. z., § 39a.

Policajného zboru: 48) a 62 (18 %) v zahranično-politickej oblasti.\*

Boj proti medzinárodnému terorizmu je zásadne založený na spolupráci, intenzívnej výmene informácií a na dôvere medzi spravodajskými službami a ďalšími bezpečnostnými orgánmi demokratického sveta, a to na národnej i medzinárodnej úrovni. Spolupráca v tejto oblasti je vysoko efektívna a účinná, predsa však niektoré nešťastne formulované vyhlásenia môžu vytvárať podivnú predstavu o spolupráci samotnej, o jej kvalite a výsledkoch ani nehovoriac. Cieľom bezpečnostných orgánov, a teda aj Policajného zboru, je formou informačnej výmeny a zapojenia sa do procesov preverovania fyzických aj právnických osôb pre projekty v gescii iných orgánov štátu (napr. Ministerstva vnútra SR, Ministerstva zahraničných vecí a európskych záležitostí SR) maximálne podporiť štát a jeho prácu na ochrane záujmov SR a jej občanov, a tak prispieť k obmedzovaniu bezpečnostných rizík či k ich úplnému odstráneniu.

Dramatický vývoj udalostí v roku 2015 sa negatívne premietol do zhoršenia bezpečnostnej situácie členských štátov EÚ v schengenskom priestore, vrátane SR. Hlavnými udalosťami roka boli teroristické útoky v Paríži, ktoré sa spolu so všetkými súvisiacimi okolnosťami stali hlavným impulzom pre prácu všetkých spolupracujúcich spravodajských služieb. Policajný zbor sa spoločne s ostatnými podieľal na mapovaní pohybu potvrdených, podozrivých i potenciálnych útočníkov. Preverovanie tisícov mien radikálov viedlo k zisteniu, že v roku 2015 niektorí z nich SR využívali ako jednu z tranzitných krajín na ceste medzi Blízkym východom a západnou Európou. V kontexte ďalších informácií je zrejmé, že aj na území SR existuje potenciálna hrozba teroristického útoku islamistických džihádov napojených na tzv. Islamský štát (ďalej len „IS“), príp. na skupinu Džabha an Nusrat (sýrska odnož al Qá'idy). Napriek mnohým územným a personálnym stratám dokázal IS v roku 2015 vykonať niekoľko teroristických útokov nielen v Európe, ale aj na Blízkom východe (napr. v Libanone, Turecku, Egypte). V nadväznosti na to zintenzívnil svoju propagandu, ktorej primárnym cieľom je radikalizácia a nábor ďalších dobrovoľníkov pridávajúcich sa k jeho ozbrojeným zločkom.

S ohľadom na tento fakt Policajný zbor sústredil svoje kapacity, vrátane spravodajských, na dve skupiny rizikových osôb. Prvú skupinu tvorili osoby, ktoré prejavili sympatie k ideológii a činom IS alebo k niektorému z jemu podobných zoskupení. V rámci cieľovej skupiny, na ktorú sa IS zameriava (mladšie generácie moslimov a konvertitov), slovenské bezpečnostné zložky zaznamenali na Slovensku iba niekoľko sympatizantov. U väčšiny z nich boli prezentované názory prejavom psychickej labilita, frustrácie či priamo choroby. Žiadny z nich nedisponoval väzbami na islamistické zoskupenia a často ani na žiadnu miestnu moslimskú komunitu. Moslimovia žijúci v SR, až na niekoľko výnimiek, aktivity IS verejne odsúdili. Druhá skupina sa skladala z osôb, ku ktorým bezpečnostné zložky SR, vrátane Policajného zboru, zisťovali informácie o ich odchodoch zo SR so zámerom pripojiť sa k teroristickým organizáciám v Sýrii, najmä k IS. Išlo o osoby pôvodom z islamského sveta, resp. s väzbami naň (rodina, pôvod), ktoré sa krátkodobu zdržiavali v SR. Návrat týchto osôb do EÚ by predstavoval vážnu bezpečnostnú hrozbu z hľadiska účasti na teroristických útokoch. Získané informácie sú zdieľané v rámci domácej i zahraničnej bezpečnostnej komunity.

---

\* Zdroj: Správa o činnosti SIS za rok 2016, jún 2016, tabuľka a diagram „Prehľad spravodajskej produkcie SIS v období od 01. 01. 2015 do 31. 12. 2015.“

Keďže SR patrí k menej významným tranzitným a cieľovým krajinám, najzávažnejšie migračné hrozby tak bezprostredne nesúviseli s prebiehajúcou migračnou vlnou, ale s jej strednodobými a dlhodobými dôsledkami v celoeurópskom rámci. Ide predovšetkým o hrozby, ktoré vyplývajú z toho, že je fakticky nemožné organizovane integrovať veľké množstvo cudzincov z kultúrne odlišného prostredia do európskej spoločnosti. Následne dochádza k vzniku uzavretých komunit, ktoré môžu byť voči európskemu kultúrnemu prostrediu nepriateľské. Tieto komunity môžu následne vytvárať ideové či logistické zázemie pre kriminálne aktivity rozličného charakteru.

Z tohto aspektu došlo k významnej zmene operačného pôsobenia spravodajských služieb v SR, Policajný zbor nevyvímajúc, zahŕňajúcej všeobecne prioritné zameranie spravodajskej pozornosti na monitorovanie a vyhodnocovanie teroristických rizík pre EÚ v kontexte výrazného nárastu teroristických útokov a teroristických hrozieb voči „Západu“ zo strany islamistických radikálov, najmä džihádistickej organizácie Daesh (tzv. Islamský štát). V súvislosti s uvedenými skutočnosťami boli analyzované možné teroristické riziká pre SR a reakcie rizikovej časti cudzineckej komunity žijúcej v SR na ne.

Možno konštatovať, že väčšina z úspešne realizovaných útokov v západných krajinách bola inšpirovaná militantnými úspechmi Daesh a jeho intenzívnou mediálnou propagandou, ktorá našla odozvu vo forme násilných aktivít u svojich sympatizantov v západnom svete. Aj preto boli priebežne získavané informácie v uvedenej súvislosti a v intenciách spolupráce s ďalšími štátnymi orgánmi boli prijaté a realizované opatrenia s akcentom na trendy mediálnej propagandy Daesh a jej dosahu na rizikovú komunitu cudzincov žijúcich SR.

V polovici roku 2015 prudko vzrástli počty nelegálnych migrantov v hlavných nárazníkových krajinách EÚ (predovšetkým Grécko, Maďarsko a Taliansko). Masívny prílev migrantov do EÚ pokračoval najmä tzv. balkánskou migračnou trasou aj v nasledujúcich mesiacoch roka 2015. Rozsah migračnej vlny a potenciálne bezpečnostné riziká s ňou súvisiace sa v druhom polroku 2015 premietli aj do spravodajskej činnosti bezpečnostných orgánov SR, vrátane polície a plnenia úloh na úseku kriminálneho spravodajstva. V rámci monitorovania nelegálnej migrácie bola pozornosť i koncipovanie opatrení sústredené najmä na posudzovanie bezpečnostných rizík spojených s príchodom nelegálnych migrantov na územie EÚ, primárne riziká možnej infiltrácie migračnej vlny osobami sympatizujúcimi s radikálnymi a teroristickými islamistickými organizáciami, veteránmi z bojov v konfliktných zónach a osobami, ktoré sa mohli v týchto zónach dopustiť zločinov proti ľudskosti.

V kontexte migračnej krízy boli (sú) súčasne priebežne vyhodnocované reakcie pravicových a ľavicových extrémistických zoskupení (v SR, ale aj v rámci EÚ) na masívny prílev migrantov, ďalej sú monitorované skupiny organizovaného zločinu profitujúce na prevádzachstve a v intenciách nastavenej spolupráce je priebežne sledovaná aj bezpečnostná situácia v severnej Afrike a na Blízkom východe.

V priebehu roka 2015 nedošlo k zmene migračných trás tak, aby nové cesty zasiahli územie SR. Následkom toho, že orgány štátu dôsledne vykonávali kontrolné



a registračné procedúry a dodržiavali zásadu, že utečenci, ktorí nežiadajú v SR o azyl, sú nelegálnymi migrantmi, došlo k razantnému zníženiu počtu tranzitujúcich cudzincov.

Kontrolné procedúry však narážajú na faktickú nemožnosť vykonávať ich dôsledne. Príčinou tohto stavu je okrem iného skutočnosť, že mnoho migrantov má alebo veľmi pravdepodobne môže mať cestovné doklady vydané síce oficiálne, avšak na území ovládanom v zdrojových krajinách migrácie extrémistickými silami, prípadne sa preukazujú cestovnými dokladmi odcudzenými či pozmenenými. Na druhej strane (v zdrojových krajinách) potom nemajú slovenské bezpečnostné zložky spoľahlivého oficiálneho partnera, ktorý by bol schopný na overovaní pravdivosti údajov o migrantoch a ich cestovných dokladoch spolupracovať a poskytovať dôveryhodné a relevantné informácie.

*K už spomínaným bezpečnostným rizikám je tak nutné pripočítať aj riziko prenášania problémov a konfliktov zo zdrojových krajín do krajín cieľových aj tranzitných, ktorých sa migračná vlna dotýka.*

V súvislosti s uvedeným boli v kontexte odstúpených informácií o aktivitách zločineckých skupín podozrivých z organizovania nelegálnej migrácie osôb pôvodom najmä zo Sýrie, Afganistanu a Pakistanu na ukrajinsko-slovenskej hranici ako aj na trase vedúcej z územia Maďarska do SR prijímané bezpečnostné opatrenia i opatrenia spravodajského charakteru,.

Keďže reálnym problémom sa javí zneužívanie všeobecného strachu z cudzincov, ktorý vyvolával nepokoj a ďalšie obavy v spoločnosti, v atmosfére neistoty, či sú ostatné štáty schopné vysporiadať sa s problémami migrácie, profilovali sa extrémistické a populistické politické subjekty, radikalizovalo sa politické prostredie a narástla popularita extrémistických strán.

Aj z toto dôvodu bola zaregistrovaná významná odozva migračnej krízy a dokonaných teroristických útokov na teritóriu Európy v roku 2015 aj v agende slovenských pravicových extrémistov (PEX), ktorí začali prezentovať protiimigračné / protiislamské postoje a boj proti multikulturalizmu oveľa intenzívnejšie ako v minulosti. Výrazným spôsobom sa v tejto súvislosti dostala do popredia aj kritika EÚ a NATO. Tradičná téma slovenských PEX – protirómska rétorika – sa pod týmto vplyvom stala pre PEX najmä v druhej polovici roka 2015 sekundárnou. Vo vzťahu k ľavicovému extrémizmu (LEX) neboli v porovnaní s PEX zaregistrované významnejšie odozvy, nebolo zaregistrované posilnenie členskej základne sympatizantov ľavicového extrémizmu, verejné aktivity zostali skôr nevýrazné, relatívne „aktívni“ boli len vo virtuálnom prostredí.

Značná pozornosť bola venovaná situácii v Turecku v súvislosti s parlamentnými voľbami a úlohou, ktorú krajina zohrávala v sýrskej a migračnej kríze. Ťažiskami spravodajských požiadaviek bolo zabezpečenie informačnej produkcie charakterizujúcej bezpečnostnú situáciu pozdĺž turecko-sýrskej hranice, operácie Daesh v jej blízkosti a tolerovanie prítomnosti niektorých skupín sýrskych džihádistov a ich aktivít na tureckom území tamojšími úradmi. Získaná spravodajská produkcia poukazovala na významnú úlohu zohrávanú aj korupciou v radoch hraničnej polície v Turecku, ktorá v niektorých prípadoch s prevádzачmi úzko spolupracovala.

Obdobné opatrenia ako v prípade Turecka, boli zamerané aj na Líbyu, kde získané informácie signalizovali vzrastajúce tendencie komplikovaného vývoja vnútropolitickej, bezpečnostnej a ekonomickej situácie, najmä značnej fragmentácie spoločnosti a politickej scény zabraňujúcej dosiahnuť široký konsenzus v otázke politického riešenia krízy. Prioritou ozbrojených skupín v Líbyi bolo udržanie moci a vplyvu na nimi ovládaných územiach, keď ekonomika krajiny je po výraznom poklese príjmov z exportu ropy vo vážnej kríze. Kriminálne a pašerácke aktivity, ako aj výnosy z ilegálnej migrácie sa stali lukratívnym zdrojom príjmov a líbyjská odnož Daesh sa po čiastočnom zatlačení do defenzívy sústredila na udržanie a upevnenie moci na územiach, ktoré získala pod kontrolu.

V naznačených súvislostiach boli v rámci kompetencií a úloh primerane v spolupráci s ďalšími štátnymi orgánmi reflektované získané informácie charakterizujúce nestabilitu a občianske vojny v niektorých štátoch regiónu majúce priamy dosah na bezpečnosť SR a EÚ v podobe masívnej migračnej vlny spojenej s rizikom jej infiltrácie osobami, ktoré majú prepojenie na teroristické skupiny.

Hlavnými zdrojmi príjmov organizovaného zločinu v SR z nelegálnych aktivít je dlhodobá najmä ekonomická a drogová trestná činnosť, pričom hospodárska kriminalita zahŕňa najmä pašovanie tovarov, nelegálnu výrobu a predaj vysokozdaniteľných tovarov a podvody s nadmernými odpočtami dane z pridanej hodnoty. V rámci boja proti medzinárodnému drogovému organizovanému zločinu sú monitorované predovšetkým skupiny, ktorých členovia majú zázemie, resp. pochádzajú z juhovýchodnej a východnej Európy. Pretrváva záujem niektorých vysokopostavených členov medzinárodného organizovaného zločinu o vytvorenie zázemia aj na našom území získaním povolenia na pobyt v SR. Za týmto účelom si také osoby v SR zakladajú firmy.

Je možné tiež uviesť poznatok, že naďalej narastá význam *pašovania drog do Európy po tzv. „Balkánskej ceste“*, v rámci ktorej časť trás vedie cez SR a ďalej sa rozvetvuje do cieľových krajín západnej Európy ku koncovým odberateľom. SR je však zväčša len tranzitnou krajinou, prípadne dočasným skladiskom pre medzinárodných obchodníkov s drogami. Významnú úlohu v transporte drog, predovšetkým heroínu, po Balkánskej ceste začal zohrávať aj ukrajinský prístav Odesa, a to vďaka vysokej miere miestnej korupcie a možnosti prekladať tam drogy z Južnej Ameriky a západnej Afriky spolu s tovarom pre EÚ a prepraviť ich do Bulharska a Rumunska, odkiaľ drogy putujú ďalej do Európy.

V súvislosti s pôsobením organizovaného zločinu je možné ako významný a pretrvávajúci faktor výrazne svojou dynamikou a tendenciami ovplyvňujúci zmenu operačného pôsobenia spravodajských služieb, trvalo pôsobiaci na potrebu flexibility v oblasti aktualizácie úloh a vzniknutých problémov, označiť dysfunkciu výkonu verejnej správy, ktorá je z významnej časti výsledkom „moderného“ pôsobenia organizovaného zločinu. Priebežne sú získavané informácie ku konaniam a prípadom dysfunkcie na centrálnej i regionálnej úrovni.

K dysfunkcii vo verejnej správe najčastejšie dochádza preto, že štátni úradníci a osoby, ktoré vykonávajú verejné funkcie, nemajú dostatočnú zodpovednosť za dôsledky vlastných rozhodnutí. V niektorých prípadoch táto zodpovednosť úplne

chýba, často sú uzatvárané nevýhodné zmluvy a verejné obstarávania boli zverované spoločnostiam s nejasnou vlastníckou štruktúrou alebo boli zadávané bez výberového konania. Výsledkom je „zlé hospodárenie“ so zvereným majetkom, keď však nedochádza k trestným činom a preukazovanie miery zavinenia je veľmi ťažké. Zodpovednosť konkrétnych osôb sa mnohokrát počas schvaľovacieho procesu - pri ktorom sa prenáša z jednej osoby na druhú bez toho, aby bol presne vymedzený podiel a úloha každej zo zúčastnených osôb na výslednom rozhodnutí - vytráca.

Možno tvrdiť, že za dysfunkciou verejnej správy, ktorá vedie k poškodzovaniu záujmov SR, prípadne záujmov EÚ, však často nestojí nielen nedbanlivosť, ale aj zámerné konanie niektorých osôb pôsobiacich v štátnej správe alebo samosprávach motivované partikulárnymi, zväčša zištnými záujmami, ktorých presadzovanie „spravidla“ sprevádza nelegitímny lobing alebo také motivovanie predstaviteľov verejnej správy, ktoré hraničí so sofistickou korupciou. K zaväzovaniu si úradníkov sú využívané nielen finančné odmeny ale aj iné spôsoby.

Medzi časté prejavy dysfunkcie verejného sektora patrí aj neúčelné vynakladanie verejných prostriedkov, ktoré je navonok legitimizované ako napĺňanie verejného záujmu. V niekoľkých prípadoch bol verejný záujem v zmysle všeobecnej spoločenskej prospešnosti použitý ako zámienka k extenzívnemu výkladu alebo dokonca k oslabeniu pevne nastavených pravidiel pre zodpovedné nakladanie s verejnými rozpočtami.

Následkom tejto praxe je „odvádzanie“ (transfer) verejných peňazí prostredníctvom právnických osôb s netransparentnými personálnymi a vlastníckymi vzťahmi do súkromných rúk. Dôsledkom teda nie sú iba nezanedbateľné ekonomické dopady na verejné rozpočty ale aj oslabovanie efektívnosti a dôveryhodnosti výkonu verejnej správy. Osobne zastávam názor, že v prípade formálneho i obsahového dodržania platných noriem by k tomuto javu vôbec nedošlo alebo ak, tak len na akceptovateľnej úrovni.

V súvislosti so spravodajským monitorovaním potenciálnych *kybernetických hrozieb*, ktorých zneužitie by predstavovalo zvýšené bezpečnostné riziko v rámci kybernetickej bezpečnosti SR, boli realizované opatrenia v rámci spolupráce s inými štátnymi orgánmi ako i s Jednotkou pre riešenie počítačových incidentov (CSIRT.SK), kedy sa riešila infiltrácia škodlivým softvérom niektorých klientskych staníc zastupiteľských úradov SR v zahraničí.

Boli analyzované zachytené signály odhaľujúce pokusy o obchádzanie registračných procedúr v informačných systémoch prevádzkovaných a používaných v organizačných štruktúrach v gescii Ministerstva zahraničných vecí a európskych záležitostí SR. Už v minulosti boli získané informácie, že tento systém je dlhodobou cieľom takýchto pokusov. Automatizované prekonávanie jednotlivých krokov v registračnej procedúre cielene zaisťujú jednotlivci alebo skupiny osôb so zámerom získať predajom zablokovaných termínov pre pohovory vlastný ekonomický prospech. Uvedené aktivity majú zásadný vplyv na dobré meno ministerstva i štátu.

Prípady domnelých DDoS útokov vedených proti informačným systémom v gescii zmieneneho ministerstva boli preverované. V spolupráci zainteresovaných subjektov pri previerkach bolo zistené, že IP adresy, ktoré mali byť k týmto útokom využívané, sa používajú k automatickému vykonávaniu zápisov registráciou do tohto

systemu.

V súvislosti s rizikami v oblasti kybernetickej bezpečnosti SR možno vnímať aj potencionálne zneužitie zraniteľnosti webových aplikácií a cloudových služieb týkajúcich sa systémov, pri ktorých je na jednom serveri prevádzkovaných niekoľko rôznych webových aplikácií a prístupov, ktoré sú limitované prihlasovacími údajmi. Rovnaká zraniteľnosť sa týka tiež cloudových služieb, pri ktorých bežne nastáva obdobná situácia, t.j. na jednom serveri bežia paralelne rôzne služby či aplikácie, pričom aj v SR existuje množstvo takto zraniteľných aplikácií. Vzhľadom na to, že štátne inštitúcie zdieľané hostingy pre prevádzku webových aplikácií zvyčajne nevyužívajú, možno predpokladať, že sa táto zraniteľnosť dotýka predovšetkým komerčných subjektov. Nie je možné však vylúčiť, že štátne orgány, ktoré takto riešené služby užívajú, môžu čeliť riziku napadnutia používateľských účtov.

Cieľom elektronických útokov sa môžu stať desiatky malých spoločností, ktoré si nemôžu dovoliť prevádzkovať vlastný server pre ľubovoľnú vlastnú webovú aplikáciu (napr. väčšina e-shopov). Môže dochádzať k odcudzeniu údajov o klientoch, vytváraniu podvodných objednávok, poškodzovaniu funkčnosti jednotlivých aplikácií, nekalému konkurenčnému boju a pod. Rôzne subjekty sa tiež môžu stať cieľom elektronických útokov v podstate „omylom“ - len preto, že používajú rovnaký hosting alebo cloudovú službu ako útočníkom zamýšľaná obeť. Zásadne podceňované je v tejto oblasti riziko špionáže, mnohé slovenské firmy si ho neuvedomujú a nemajú dostatočné povedomie o hrozbách, ktorým môžu reálne čeliť.

Dlhodobé kyberšpionážne kampane sponzorované štátmi a vykonávané buď priamo štátnymi aktérmi (určitými zložkami štátu) alebo aktérmi štátom platenými prebiehajú takmer po celom svete. Je veľmi pravdepodobné, že s rastúcou digitalizáciou verejnej sféry bude využívanie týchto kampaní stále intenzívnejšie. Aj v podmienkach Policajného zboru bol už tento trend zaznamenaný ako z vlastných šetrení, tak aj z informácii získaných v rámci zahraničnej spolupráce.

Cieľom spomínaných kampaní je predovšetkým získavanie informácií z politickej oblasti, z oblasti vojenstva a diplomacie, z vedecko-technickej oblasti a z oblasti priemyslu a energetiky. Odcudzené údaje a informácie môžu byť využívané na vlastné účely, či už na politické alebo vedecko-priemyselné, na dehonestáciu určitých osôb či priamo štátov, na dezinformácie, prípadne vydieranie.

Kyberšpionážne útoky však nie sú zamerané len na dáta ako také alebo na utajované skutočnosti, ale zameriavajú sa skôr na krádeže osobných údajov a prihlasovacích údajov do informačných a komunikačných systémov a krádeže obsahu elektronickej komunikácie politicky či inak významných osôb. Tieto údaje a informácie potom ďalej slúžia na sofistikované útoky, ktoré využívajú metódy sociálneho inžinierstva. Hlavný smer, ktorým boli zaznamenané útoky vedené, predstavovalo najmä rozosielanie spearphishingových emailov, a to s využitím sociálneho inžinierstva a prípadne tzv. „*watering hole attacks*“.

## ZÁVER

Analyzované aspekty bezpečnostného prostredia SR v kontexte činnosti Policajného zboru v aktuálnych potrebách a možnostiach reflektujú obsah a kontext zmien v operačnom prostredí.

V mnohom iniciujú prijímanie opatrení a zásadne ovplyvňujú iniciatívy a činnosti, ktoré sú každodenným obsahom plnenia aktuálnych úloh, ako aj riešenia problémov zmien v operačnom prostredí, a to aj v kontexte rozoberanej spravodajskej činnosti v Policajnom zbore, jej miestu a významu v aktuálnych kontúrach spoločenského, politického a ekonomického vývoja SR.

Privítam iniciatívy, námietky, pripomienky k spracovanej téme s cieľom zefektívniť a „zobsažniť“ komunikáciu na jednej strane medzi štátnymi orgánmi navzájom a na strane druhej aj s odbornou verejnosťou, a tak prispieť k flexibilitě zainteresovaných subjektov v spravodajskej činnosti v rámci SR a reflektovať na zmeny v operačnom pôsobení spravodajských služieb.

### Literatúra a pramene

- [1.] HOLCR, K.: *Logika, metodológia a metódy vedeckého poznania*, Bratislava : Akadémia Policajného zboru, 1996. ISBN 80-88751-91-8.
- [2.] HOLOMEK, J., ŠIMANOVSKÁ, T.: *Úvod do metodológie praktických vied : Policajné vedy ako vedy praktické*, Bratislava 2002, Akadémia PZ v Bratislave, ISBN 80-8054-249-X.
- [3.] FILÁK, A., PORADA, V.: *Pojem, obsah a hlavní organizačně taktické formy policejné bezpečnostní činnosti* In: *Policajná teória a prax*, Bratislava 2006/4, : Akadémia policajného zboru v Bratislave.
- [4.] KOSTÍK, C.: *Prognóza vývoja kriminality v SR do roku 2010*, Akadémia PZ v Bratislave, 2007. ISBN 978-80-8054-423-2, EAN 9788080544232.
- [5.] KOHUTIAR, J.: *Spravodajská etika*. In: [www.absd.sk](http://www.absd.sk).
- [6.] KOUBOVÁ, E.: *Latentní kriminalita a její výzkumy na světě (Victim Surveys)*, In: *Československá kriminalita* č. 4/199.
- [7.] LÁTAL, I.: *Příznaková analýza a možnosti jejího užití v policejní praxi*. In: *Kriminalistika*, 1996, roč. XXIX, č. 1.
- [8.] LIŠIŇ, M.: *Charakteristika operatívno-pátracej činnosti a spravodajskej činnosti*, In: *Policajná teória a prax* č. 1/2008.
- [9.] NESNÍDAL, J.: *Neodvratnost trestního postihu a operativně pátrací činnost*, Praha, 1989 : Kriminalistický ústav VB.

- [10.] PORADA, V., STRAUS, J.: *Kriminalistická stopa*, In.: Kriminalistika č. 3/1999.
- [11.] PJEŠČAK, J. a kol.: *Základy kriminalistiky*, Praha: Naše vojsko, 1976.
- [12.] Správa o činnosti SIS za rok 2016.
- [13.] STIERANKA, J.: *Odhaľovanie latentnej kriminality a zisťovanie jej páchatel'ov*  
In: *Právne aspekty činnosti polície v boji proti kriminalite v európskej dimenzii : zborník príspevkov z celoštátneho seminára s medzinárodnou účasťou, ktorý sa konal dňa 16. mája 2005*. Akadémia Policajného zboru v Bratislave, 2005. ISBN 80-8054-352-6.
- [14.] STIERANKA, J.: *Odhaľovanie latentnej kriminality - súčasť operatívnych a spravodajských činností*  
In: *Stav a možnosti rozvoja operatívnych činností v Policajnom zbore : zborník z medzinárodného teoreticko-praktického seminára konaného dňa 8. decembra 2005 na Akadémii Policajného zboru v Bratislave*, Katedra kriminálnej polície Akadémie PZ, 2005. ISBN 80-8054-370-4.
- [15.] STIERANKA, J.: *Základy spravodajskej činnosti*, Bratislava : Akadémia PZ v Bratislave, 2008. ISBN 978-80-8054-443-0.
- [16.] ZRUN, M., RĚHOŘOVÁ, L.: *Úvod do spravodajství*. Praha : Policejní akademie ČR, 2007. ISBN 978-80-7251-252-2.
- [17.] Zákon č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov.

## **I.Cibula: Ženy v štruktúrach spravodajských služieb**

**Igor Cibula (1942)** – *Publicista, expert v oblasti spravodajských služieb. Ako spravodajský dôstojník začínal na 1.správe FMV (1968-1970). Po rehabilitácii v roku 1990 pokračoval v spravodajskej kariére na Úrade pro zahraničné styky a informace. V období 1993-1995 bol riaditeľom rozviedky SIS. V rokoch 2006-2007 prednášal na Fakulte politických vied a medzinárodných vzťahov Univerzity Mateja Bela v Banskej Bystrici o spravodajských službách. Od roku 2008 na túto tému prednáša na Fakulte práva Paneurópskej vysokej školy. V roku 2006 inicioval založenie Asociácie bývalých spravodajských dôstojníkov na Slovensku. Špecializuje sa na Rusko a Ukrajinu.*

*Dame Stella Rimington – „prvá dáma špionáže“*

K úvahám o postavení a poslaní žien v štruktúrach spravodajských služieb ma do určitej miery inšpiroval rozhovor v britskom denníku The Guardian, kde šéf kontrarozviedky MI5 Andrew Parker hovoril o úlohách tejto bezpečnostnej služby na obdobie najbližších piatich rokov a medzi inými spomenul predsavzatie dosiahnuť v náboře rovnováhu pohlaví 50 na 50. Uvedenej téme som venoval pozornosť už skôr, ale keď som to spomenul mojim profesionálnym kolegom zo spravodajskej komunity, zdalo sa im, že ženy v spravodajských službách si skôr zaslúžia pozornosť ako námet pre popkultúru, než aby sa osobitne rozoberal ich význam a prínos pre efektívne fungovanie rozviedky alebo kontrarozviedky. Vieme však, že ani v popkultúre nedominujú ženy, ale hrdinovia typu Jamesa Bonda a ženám sa dostávajú skôr periférne úlohy. Ba dokonca možno považovať za ironicky príznačné, že spisovateľ Ian Fleming podľa literárnych historikov opísal Bondovu šéfkou - pani „M“ – na základe charakteristík, ktoré sa vzťahovali na vedúce postavy britskej spravodajskej komunity mužského pohlavia, ako boli admirál John Godfrey, William Melville, Claude Dansey alebo Maxwell Knight. Až neskôr prišla v roku 1992 do čela britskej MI5 prvá žena – Dame Stella Rimingtonová, ktorú BBC nazvala „prvou dámou špionáže.“ Ďalšou ženou na poste generálneho riaditeľa MI5 bola barónka Eliza Manningham Buller (2002-2007); spravodajská dôstojníčka z aristokratickej rodiny osvedčila sa ako šéfka sekcie boja proti írskemu terorizmu a vo funkcii riaditeľky MI5 viac priblížila službu britskej verejnosti – a to tým, že zriadila webovské stránky na internete a zaviedla nábor agentov prostredníctvom inzerátov v novinách.

### *Zastúpenie žien v britskej spravodajskej komunite*

Podľa najnovších údajov spravodajského a bezpečnostného výboru britskej Dolnej snemovne ženy na vedúcich pozíciách v bezpečnostnej službe MI5 predstavujú 27 %, v rozviedke MI6 pätinu z celkového stavu riadiaceho manažmentu a v štruktúrach britskej rádiorozviedky - Government Communications Headquarters (GCHQ) toto číslo činí iba 18 %. Kvôli úplnosti štatistického prehľadu o spravodajských bezpečnostných štruktúrach vo Veľkej Británii ešte spomeniem Úrad pre bezpečnosť a boj proti terorizmu (OSCT) – vznikol v roku 2007 – kde na vedúcich pozíciách pôsobí iba 16 % žien. Britská parlamentná komisia označila uvedené čísla za kritický stav a niektorí poslanci naliehali, aby sa pri náboře žien hľadali nové a inovatívne spôsoby, ktoré poskytnutú príležitosť pre talentované ženy nielen v operatívnej činnosti, ale aj útvaroch spravodajskej analýzy a SIGINT-u, ktorý

v aktuálnom operačnom prostredí plní niekedy nenahraditeľnú funkciu. V tomto rámci nábor žien pre britské spravodajské agentúry sa orientuje hlavne na ženy v „strednom veku“ s ustáleným sociálnym a rodinným zázemím. Flexibilné pracovné prostredie v spravodajskej službe kladie totiž na ženy - v porovnaní s mužmi – zvýšené nároky, čo si vyžaduje od žien emocionálnu stabilitu a určitú životnú zrelosť.

### *Kariéra žien v CIA*

Postavením žien a otázkami ich profesionálno-kariérneho postupu v spravodajských službách sa zaoberajú nielen vo Veľkej Británii, ale osobitnú pozornosť venujú tejto téme aj v Spojených štátoch, kde v apríli 2012 vtedajší riaditeľ CIA generál David H. Petraeus zriadil osobitnú poradnú skupinu pre ženy vo vedení. Jej poslaním bolo hľadať spôsoby, ako zlepšiť kariérny postup žien v CIA. Na čelo tejto expertnej skupiny pozval generál Petraeus bývalú ministerku zahraničných vecí Madeleine K. Albrightovú so zreteľom na jej životné skúsenosti kariérnej diplomatky i jej rešpektovanú spoločenskú autoritu. V tíme externe spolupracovali aj piati bývalí významní armádni, bezpečnostní a spravodajskí činitelia, ktorí dôverne poznali vnútorné podmienky fungovania bezpečnostných a spravodajských štruktúr USA. Záverečná správa skupiny s odporúčaniami bola dokončená vo februári 2013 a je k dispozícii na internetovej stránke CIA. Dokument konštatuje, že ženy tvoria 46 % personálu CIA, čo v porovnaní s rokom 1980 predstavuje nárast o 8 %. Dôležitý je údaj, že za obdobie od roku 1980 sa zvýšilo zastúpenie žien v riadiacich funkciách z 9 % až na 44 percent. Výsledkom analýzy expertnej skupiny sú viaceré systémové odporúčania, ktoré by mali zmeniť kultúru personálnej práce v agentúre. Medzi zaujímavé výsledky personálnej analýzy patrí zistenie, že ženy by častejšie ako muži v určitých obdobiach svojej kariéry využili flexibilné možnosti práce – napríklad možnosť pracovať na čiastočný úväzok - keby to nemalo negatívny dopad na vývoj ich ďalšej kariéry v službe.

### *Problémy diskriminácie žien v spravodajskej komunite USA*

Problematikou postavenia žien v spravodajskej službe a otázkami ich služobného postupu sa začali zaoberať v CIA už v roku 1991, keď vznikla štúdia, ktorá odhalila kariérnu diskrimináciu žien v spravodajskej službe, favorizovanie mužov pri obsadzovaní vedúcich pozícií a dokonca oficiálne tolerovanú prax sexuálneho obťažovania žien. Podľa údajov tejto štúdie ženy vtedy tvorili štyridsať percent príslušníkov CIA, ale iba 17 % boli dôstojníčky operatívy a len 9 % žien sa dostalo do riadiacich funkcií. V roku 1992 cca 250 žien podalo skupinovú žalobu kvôli profesionálnej diskriminácii a obťažovaniu; súd ich žalobe vyhovel. Proces reformy prístupu k uplatneniu žien v americkej spravodajskej komunite nebol však jednoduchý a až v roku 2010 sa stala žena najvyššou šéfkou významnej spravodajskej agentúry USA. Na post riaditeľky National Geospatial-Intelligence Agency (NGA) nastúpila v roku 2010 Letitia Longová, ktorá túto zodpovednú funkciu zastávala až do roku 2014. Predtým štyri roky pôsobila ako námestníčka riaditeľa Vojenskej spravodajskej služby (DIA). Podotýkam, že táto dáma nie je jediná žena, ktorá sa prepracovala až do najvyšších poschodí americkej spravodajskej komunity.

### *Utajené údaje o ženách v SIS*



Dovolil som si stručný torzovitý exkurz do problémov, súvisiacich s postavením žien v štruktúrach spravodajskej komunity vo Veľkej Británii a v USA. Na porovnanie som získal informáciu o štruktúre žien, ktoré sú v služobnom pomere v Slovenskej informačnej službe. Ženy predstavujú v SIS 39,89 % celkového personálneho stavu služby; na operatívnych útvaroch pôsobí 14,95 % a na logistických útvaroch 80,05 %. Vysokoškolské vzdelanie všetkých stupňov má 65,27 % príslušníčok spravodajskej služby. Na riadiacich funkciách je zaradených 24,78 %, z toho pozície na úrovni manažmentu zastáva 14,28 percenta žien. Jediný verejne prístupný údaj poskytuje internetová stránka Slovenskej informačnej služby, kde sa v správe o činnosti SIS v roku 2015 uvádza, že „mužov pôsobí v službe 60 % a žien 40 %“. Z mojich zdrojov je mi známe, že na spravodajsky významnej pozícii pôsobí iba jediná žena. Ale aj na iných riadiacich postoch v službe boli alebo sú ženy, ako to uvádzajú predchádzajúce údaje. Na rozdiel od britských poslancov výboru pre spravodajské a bezpečnostné služby Dolnej snemovne členovia Osobitného kontrolného výboru Národnej rady SR na kontrolu činnosti SIS ani členovia Osobitného kontrolného výboru Národnej rady SR na kontrolu činnosti Vojenského spravodajstva nepovažujú postavenie a poslanie žien v spravodajskej komunite za tak závažnú otázku, aby jej venovali náležitý záujem. Zastávam názor, že téma si zaslúži systematickú pozornosť, a preto by mala SIS vypracovať systém flexibilného využívania žien v špeciálnych profesiách a zaviesť opatrenia, ktoré by rozšírili uplatnenie žien v službe a rozšírili podmienky pre ich kariérny postup.

### *Ženy sú v spravodajskej službe nenahraditeľné*

Bývalý riaditeľ Mossadu Tamir Pardo v rozhovore pre izraelský časopis *Lady Globes* uviedol charakteristiku ženských vlastností, ktoré tzv. nežné pohlavie predurčujú na to, aby v tajnej vojne spravodajských služieb boli nenahraditeľné. A nemal na mysli ani tak ich sexuálny pôvab, ale predovšetkým schopnosť „multitaskingu“, teda vykonávať viac vecí naraz. Podľa bývalého šéfa izraelskej rozvedky „ženy majú dar rozlúštiť situáciu. Na rozdiel od stereotypov, ženy prekonávajú mužov, pokiaľ ide o vnímanie terénu, čítanie situácií a priestorové vnímanie. Keď sú dobré, sú veľmi dobré.“ Vyzdvihol tiež, že ženy dokážu „lepšie hrať svoju rolu“ než muži, pretože dokážu potlačiť svoje ego, aby dosiahli cieľ. Ženám pomáha aj fakt, že sú vnímané ako slabšie pohlavie a špionáž je mužská práca – čo robí ženy ideálne pre špionáž. K výhodám žien patrí schopnosť spriatelíť sa, ľahko čítať v ľuďoch, zistiť ich motivácie i zraniteľnosť.

### *Prekonaná teória rodových stereotypov*

Pozitívne vyjadrenie Tamira Pardo vyvracia – a zároveň potvrdzuje – teóriu rodových stereotypov, tradičných predsudkov, ktoré sa týkajú mužskosti a ženskosti a považujú sa za dané, prakticky nemenné. Pre rodový stereotyp je typické nediferencované paušálne prisudzovanie určitých vlastností všetkým príslušníkom daného pohlavia. Podľa sociálnych psychológov je charakteristický emocionálnosťou a iracionalitou, zjednodušeným výkladom javov. Napríklad o mužoch sa stereotypne predpokladá, že neplačú. Ženám sa zase pripisuje citlivosť, submisívnosť, poriadkumilovnosť a iné vlastnosti, ktoré sa v prevažujúcej miere nevyskytujú u mužov. Pre rodové stereotypy je charakteristická značná zotrvačnosť a proces ich zmien viac-menej zaostáva za deklarovanými spoločenskými princípmi občianskej rovnoprávnosti a rovnosti. Je skutočnosťou, že ani v civilizačne najvyspelejších

krajinách neboli úplne prekonané rodové stereotypy, podporujúce hierarchický – nerovný vzťah medzi ženami a mužmi. V takomto kontexte slová bývalého šéfa Mossadu o kvalitách žien majú osobitný význam a zavážia ako argument, aby sme k verbovaniu žien do spravodajských služieb pristupovali bez predsudkov a nekládli ich kariérnemu postupu prekážky.

### *Známy príklad agentky Mossad-u*

Tamir Pardo v rozhovore pre časopis Lady Globes uviedol, že v Mossade existuje rovnaký počet agentov mužského i ženského pohlavia. Jeden z najznámejších prípadov izraelskej ženskej agentky sa týka operácie, ktorej cieľom bolo vylákať informátora Mordechaia Vanunu z Londýna do Talianska, odkiaľ bol tajne unesený do Izraela (1985). Na základe zistenia psychológov Mossadu, že Vanunu sa cíti osamelý, bola na neho nasadená izraelská agentka Cheryl Haninová, vydávajúca sa za americkú turistku „Cindy.“ Dohovorili si spoločnú dovolenku v Ríme, kde namiesto „radovánok“ s Cindy ho čakalo komando Mossadu, ktoré ho omámeného zavlieklo na izraelskú loď, aby ho dopravila do Izraela, kde ho súd odsúdil na 18 rokov do väzenia za prezradenie izraelského tajného jadrového programu britským novinám Sunday Times. Cheryl Haninová bola americká Židovka, ktorá sa vydala v Izraeli za dôstojníka izraelskej spravodajskej služby a pred akciou proti jadrovému technikovi Vanunu absolvovala výcvik v Mossade.

### *Využitie Nikah al-mutah v špionáži*

Príklad využívania emocionálnej manipulácie mužov na ich kontrolu a spravodajské vyťažovanie v praxi Mossadu uviedol vo februári tohto roku arabský internetový portál Al Bawaba, ktorý má centrálu v Ammáne a pobočku v Dubaji. V článku od jordánskej agentúry SyndiGate sa zmieňuje o „ženskej špionážnej jednotke“ Mossadu, ktorá zahŕňa mnoho arabských žien, predovšetkým z Maroka. Agentúra sa odvoláva na informácie bližšie nešpecifikovaného Ould El Kabliho, že Mossad vytvoril v Maroku sieť „krásnych žien“, ktoré musia byť moslimského pôvodu od narodenia. Sieť sa údajne orientuje na aktiváciu tzv., teda „dočasných manželstiev“ – čo je vlastne podľa islamu nábožensky schválená určitá forma prostitúcie. Nevesty sa ponúkajú hlavne významným arabským osobnostiam, najmä z regiónu Perzského zálivu. Agentky z tejto štruktúry majú monitorovať cudzincov v Maroku, ktorí sú považovaní za hrozbu záujmom Izraela – alebo tiež osobnosti, významné pre vzťahy medzi Marokom a Izraelom. Okrem toho majú získavať aj informácie o Američanoch arabského pôvodu, pôsobiacich v americkej administratíve alebo v rozvojových mierových projektoch na Strednom východe. Zaujímajú ich Arabi i cudzinci, ktorí sú známi prejavmi protiizraelského cítenia. Nemožno vierohodne určiť mieru spoľahlivosti informácií portálu Al Bawaba, ale určite zrkadlia praktiky spravodajských služieb v regióne.

Dovolím si zdôrazniť, že môj referát nie je mienený ako argumentačná obhajoba pokryteckej a falošnej doktríny genderového rovnostárstva, ktorým zamorujú svet fanatickí vyznávači evanjelia tzv. politickej korektnosti. Skôr mi ide o to, že sa chcem podeliť o moje poznámky o nezastupiteľnej úlohe žien v efektívnom fungovaní spravodajských služieb. Zaiste niektorí z vás uvádzané konkrétne poznáte, ale napriek tomu som ich spomenul, aby som ilustroval význam

problematiky ženského fenoménu a akcentoval potrebu venovať mu pozornosť aj v súvislosti s aktuálnym operačným prostredím spravodajských služieb.

### *Významný podiel žien na zadržaní bin Ládina*

Pre ďalšie uvažovanie týmto smerom možno považovať za zaujímavú inšpiráciu štúdiu o zmene postavenia amerických žien a ich úlohe v spravodajskej komunite, ktorej autorkou je Amy J. Martin z katolíckej Marymount University v Arlingtone\*. Autorka ju prezentovala na 11. výročnej konferencii International Association for Intelligence Education (IAFIE). Okrem toho, že štúdia obsahuje historický prehľad niektorých prostriedkov spravodajskej činnosti žien, prezentuje tiež ich dispozície poskytovať pomoc a podporu, ako aj schopnosť viesť spravodajské operácie po celom svete. Ako príklad spomeniem významný podiel žien v analytickej skupine, ktorá rozhodujúcou mierou prispela k úspechu operácie na vypátranie a zadržania Usámu bin Ládina. Skupina analytičiek z tímu CIA – známeho pod kódovým označením „Alec Station“ – dokázala pracovať aj 18 hodín denne, aby spracovali obrovské množstvá dát a poznatky sprostredkovali kolegom. Jedna z nich – Susan Hasler – neskôr v rozhovore pre televíziu CNN povedala, že ženy sú dobrými protiteroristickými analytikmi, pretože ich vlastné ego im nekomplikuje plniť náročné úlohy; ženy na rozdiel od mužov dokážu pripustiť, že niečo nepoznajú, majú medzeru vo vedomostiach, a preto požiadajú o pomoc. Vzdelaná analytička CIA z farmárskej rodiny odišla po 21 rokoch zo služby a venuje sa písaniu románov z prostredia, kde pôsobila. Súhlasím s jej názorom, že „atribúty úspešných spravodajských dôstojníkov sú vytrvalosť, húževnatosť, trpezlivosť a oddanosť.“

### *Zápas s predsudkami ženy stimuluje*

Počas môjho pôsobenia v spravodajských štruktúrach som sa prakticky nestretol so ženami, ktorým by sa dali vytknúť závažné defekty po profesionálnej stránke. Uvedené konštatovanie sa však nevzťahuje na moje služobné skúsenosti so spravodajskými dôstojníkmi mužského pohlavia. Boli medzi nimi elitní profesionáli a odborníci spoľahlivých kvalít, potom ešte priemerní zamestnanci, ale aj takí, ktorí podľa mojich očakávaní nespĺňali náročné kritéria pre pôsobenie v spravodajskej službe. Nie som však idealista, pretože i ženy v spravodajských službách sú rovnako rôznorodé ako ostatná populácia. Avšak stereotypné predsudky sociálneho prostredia a z toho prameniace bariéry nedôvery – nielen akási vrodená ženská svedomitosť – ich nútia k tomu, aby k svojim služobným povinnostiam pristupovali s maximálnou zodpovednosťou a dokázali mužským kolegom, že sú ich rovnocennými partnermi. Zostáva pravdou, že ak sa chce žena presadiť v takomto prostredí, musí preukázať vyššiu úroveň svojho pracovného výkonu a profesionalitu, ako sa to očakáva od muža v rovnakom alebo podobnom služobnom zaradení. Zmienila sa o tom aj Letitia Longová - šéfkla spravodajskej agentúry NGA (National Geospatial-Intelligence Agency) – keď v denníku Washington Post hovorila o svojej spravodajskej kariére a spomínala, ako na poradách v období svojich profesionálnych začiatkov niektorí mužskí kolegovia sústredene a niekedy dokonca s neskrývanými pochybnosťami očakávali, čo povie k diskutovanej téme – a to len preto, že tam bola jediná žena.

---

\* Martin, Amy J.: America's Evolution of Women and Their Roles in the Intelligence Community. In: Journal of Strategic Security 8, no.5, 2015, ss.99-109.

## *L'udské zdroje sú nenahraditeľné*

Uviedol som niekoľko poznámok k postaveniu a poslaniu žien v štruktúrach bezpečnostných a spravodajských služieb, ktoré predovšetkým utajeným spôsobom získavajú informácie, potrebné pre riadenie štátu a ochranu spoločnosti pred aktuálnymi bezpečnostnými hrozbami. Viacerí kolegovia predtým hovorili o zmenách operačného prostredia, na ktoré musia tieto služby reagovať. Nazdávam sa, že jednou z týchto zmien je neregulovaná migrácia ľudí z iného kultúrno-civilizačného prostredia a s tým súvisiaci problém rozšírenia sociálneho priestoru pre medzinárodný terorizmus. Napriek nesporne efektívnemu rozsiahlemu prieniku informačných a elektronických technológií do spravodajskej činnosti využitie HUMINT-u, teda ľudských zdrojov v spravodajských službách, je nenahraditeľným prostriedkom účinného boja proti medzinárodnému terorizmu. Spravodajský prienik do kultúrno-civilizačne uzavretých a samo sa izolujúcich komunít v Európe si vyžaduje, aby spravodajské služby euroatlantického spoločenstva väčšou mierou využívali na kontakt so záujmovými osobami ženy.

Ženský faktor je však dôležitý nielen v HUMINT-e, ale aj v ostatných segmentoch spravodajskej aktivity. Ženy zohrali kľúčovú úlohu v operáciách elektronického monitorovania komunikácie (SIGINT) a preukázali svojej špičkové kvality aj v kryptológii a pri analýze spravodajských informácií. V USA, Izraeli i vo Veľkej Británii chápu významný príspevok žien pre zvyšovanie efektívnosti spravodajských služieb. Preto sa téme využívania predností ženských kvalít vo svojej činnosti systematicky venujú, vrátane otázok ich kariérneho postupu i flexibilného prístupu k ich pracovnému zaradeniu. Na Slovensku nie sú zatiaľ k dispozícii informácie o tom, že by vrcholní predstavitelia spravodajského spoločenstva venovali tejto téme pozornosť.

# Závery zo sympózia

## Spravodajské služby v zmenenom operačnom prostredí - aktuálne úlohy a problémy spravodajských služieb

1. Lektori sympózia zdôraznili zmenu v operačnom prostredí spravodajských služieb, ktoré charakterizuje neregulovaná migrácia, rozširovanie štruktúr medzinárodného terorizmu, hybridné vojny a radikálny prienik moderných informačných technológií do činnosti spravodajských služieb. Spoločenské očakávania od spravodajskej komunity si vyžadujú nové prístupy i kritický pohľad na doterajšie fungovanie spravodajských služieb.
2. Zborník príspevkov zo sympózia bude užitočnou štúdijskou pomôckou pre študentov problematiky spravodajských služieb a poskytne funkcionárom a expertom štátnych inštitúcií podnety, ako reagovať na aktuálne bezpečnostné výzvy.
3. Zborník príspevkov zo sympózia bude k dispozícii poslancom - členom výborov Národnej rady SR na kontrolu činnosti spravodajských služieb, aby mohli kompetentnejšie posudzovať efektívnosť fungovania spravodajských služieb Slovenskej republiky.
4. Uskutočnenie v poradí už 10. medzinárodného sympózia o spravodajských službách na pôde Fakulty práva Paneurópskej vysokej školy svedčí o tom, že sa podarilo založiť fungujúcu tradíciu, ktorá úspešne slúži nielen spravodajskej komunite a bezpečnostným expertom, ale pomáha aj poslucháčom Fakulty práva Paneurópskej vysokej školy, ktorí si zvolili študijný predmet venovaný spravodajským službám.
5. Uznanie za založenie a pravidelnú aktivitu tohto medzinárodného diskusného fóra si zaslúži Asociácia bývalých spravodajských dôstojníkov, Fakulta práva Paneurópskej vysokej školy a zahraniční lektori, ktorí nezištne prispievali k odbornej úrovni sympóziá.