Využívanie sociálnych médií v prospech Ruskej federácie, úlohy, metódy a vykonávatelia vo vzťahu k paramilitárnym organizáciám na území SR

Radovan Bránik / Seminár: Quo vadis, Democracy? / Panel 2: What is the role of Russian propaganda in social media in V4 region?

Motto: "Keď už je to vidno, je už zvyčajne neskoro, priateľu."
Vladimír Suchodolinský, bývalý spravodajský dôstojník na teritóriu Spoločenstva Nezávislých Štátov a námestník VSS, v osobnom rozhovore dva mesiace pred smrťou na extrémne ojedinelý nádor, zvyčajne spôsobený ožiarením.

Ruská federácia realizuje presadzovanie svojich záujmov v krajinách V4 dvoma hlavnými spôsobmi. Jednak oficiálnou cestou za aktívneho zapojenia diplomatických pracovníkov a kultúrnych inštitútov, čiastočne aj subjektov tretieho sektora a miestnych sympatizantov, zároveň aktívne a systematicky pôsobí na území týchto krajín neoficiálne cestou nasadenia rozviednych služieb.

Vychádzajúc zo správ siedmich spravodajských služieb členských krajín EÚ z roku 2014 a 2015 sa považuje za preukázané, že zvyčajne **štvrtina, až tretina všetkých pracovníkov zastupiteľských úradov RF v krajinách EÚ** (vrátane technickohospodárskych) pracuje pod krycou diplomatickou legendou a v skutočnosti ide o príslušníkov, resp. spolupracovníkov niektorej z tajných služieb. V tomto bode dochádza k prekrývaniu oficiálnej a neoficiálnej formy pôsobenia v záujmovej krajine a podľa správ prebehlíkov má v prípade rozhodovania o ďalšom postupe v absolútnej väčšine prípadov hlavné slovo tajná služba. Nakoľko oficiálna činnosť orgánov RF na sociálnych sieťach je kvalitne monitorovaná a zdokumentovaná, budeme sa venovať hlavne činnosti, ktorá na našom území prebieha skrytou formou, často nelegálne, využívajúc miestnu vplyvovú agentúru, na ktorej tvorbe a údržbe sa aktívne podieľajú riadiaci dôstojníci dvoch zložiek. Popíšeme si, aká je aktuálna štruktúra a úlohy jednotlivých tajných služieb RF.

V auguste roku 1991 došlo k aktívnej účasti KGB na neúspešnom pokuse o štátny prevrat, v nasledujúcich mesiacoch sa dostala následkom reorganizácie jej pôvodných kompetencií a štruktúry k stavu, v akom sa bez výraznejších zmien nachádza dodnes.

Pre potreby tohto príspevku sú z viacerých existujúcich zložiek dôležité dve: **Hlavná správa rozviedky generálneho štábu ozbrojených síl RF** a **Služba vonkajšej rozviedky RF**. Tieto dve organizačné zložky majú na starosti aktívne pôsobenie na území nepriateľa, **Federálna služba bezpečnosti RF** a **Federálna služba ochrany RF** pôsobia prevažne na území Ruska v oblasti boja proti vnútornému nepriateľovi a ich spravodajská činnosť na území iných krajín je vykonávaná ad hoc, zvyčajne bez vyslovene nepriateľských úmyslov a iba vo vzťahu k problematike vnútornej bezpečnosti. To isté sa týka aj **Federálnej služby RF pre boj proti narkotikám**, ktorá často spolupracuje s partnerskými službami v jednotlivých krajinách a až na výnimky nepôsobí nepriateľsky voči záujmovej krajine. V Rusku existuje tiež niekoľko menších špecializovaných služieb určených na vykonávanie konkrétnych ofenzívnych operácií vyžadujúcich si nasadenie fyzického násilia, atentátov, vrážd, a vykonávanie inej nelegálnej, resp. trestnej

činnosti. Ich vplyv na sociálne siete je prakticky bezvýznamný a na území EÚ sú nasadzované ojedinele.

Hlavná správa rozviedky generálneho štábu ozbrojených síl RF je zo svojej podstaty ofenzívnou službou výrazne vojenského charakteru, jej príslušníkmi sú napríklad členovia oddielov Spetznaz v minimálnom odhadovanom počte 17 400 osôb. Títo sú využívaní na plnenie rôznych špeciálnych úloh, často v konfliktných zónach, kde Ruská federácia buď vedie regulérnu vojnu, alebo vykonáva vojenské operácie bez oficiálneho vyhlásenia vojny, prípadne poskytuje inštruktorské služby pre miestnych bojovníkov a partizánov. Príslušníci Spetznaz tiež zabezpečujú prípravu terénu, logistického zázemia a fyzickej bezpečnosti špecialistov GRU na HUMINT, SIGINT a CYBINT operujúcich na misiách na nepriateľskom území, vrátane zabezpečenia evakuačných plánov v prípade rizika prezradenia. Predpokladá sa, že sekcia SIGINT je personálne najsilnejšou zložkou GRU, pričom väčšia časť jej činnosti prebieha z ruského územia, resp. prostredníctvom monitorovacích satelitov používajúcich optický prieskum, odposluch rádiovej, telefónnej a internetovej komunikácie. Menšia časť príslušníkov však vykonáva v zahraničí nevyhnutné činnosti spojené s **inštaláciou, prevádzkou a servisom zariadení zvyčajne umiestnených v objektoch veľvyslanectiev, ktoré neslúžia na legálne nezávislé krátkovlnné a strednovlnné spojenie s Ruskom, ale zabezpečujú funkčnosť systémov pracujúcich vo veľmi krátkych vlnách a UKV, ktorých jediným cieľom môže byť vzhľadom na obmedzený dosah zabezpečovanie nelegálneho vysielania a príjmu signálu súvisiace s rozviednou, alebo špionážnou službou**, zabezpečujú tiež nelegálny prienik do systémov mobilných operátorov s cieľom zabezpečiť odpočúvanie konkrétnych telefónnych čísel a monitoring pohybu záujmových osôb, **vrátane prevádzky niekoľkých falošných mobilných BTS** v prípadoch, že ich krátkodobé využitie vyhodnotí ako nevyhnutné.

Na území V4 sa tiež služby špecialistov Spetznaz využívajú v inštruktorskej činnosti bojovo orientovaných klubov, ktoré vedú osoby tvoriace súčasť ruskej vplyvovej agentúry. **GRU má najväčšiu vlastnú nezávislú sieť zahraničných agentov**, predpokladaný počet jej príslušníkov **šesť, až osemnásobne** presahuje počet príslušníkov siete Služby vonkajšej rozviedky. GRU využíva na koncovú komunikáciu s príslušníkmi vplyvovej agentúry a šírenie dezinformácií rôzne sociálne siete a zabezpečuje tiež plynulé spojenie medzi nimi a zdrojmi z teritória RF, na ktoré má priamy ideologický a mocenský vplyv. **Ciele záujmu GRU sú prevažne vojenskej povahy**, orientuje sa tiež na získavanie informácií rôzneho stupňa utajenia z NATO a ovplyvňovanie paramilitárnych organizácií a ich lídrov smerom k podpore ruského naratívu.

Vzhľadom na technologický rozvoj v ostatných rokoch a nadkritické zvýšenie dostupnosti internetu pre široké masy získali ruské tajné služby nečakane k dispozícii kanál, bez ktorého by ich činnosť nedosahovala ani zlomok dnešného účinku. Došlo tak k paradoxnej situácii, keď **produkt pôvodne budovaný pre potreby americkej armády po uvoľnení pre civilné využitie zásadne zvýšil šance rozviednych služieb Ruskej federácie ovplyvňovať medzinárodnú situáciu vo svoj prospech**. V kombinácii s tým, že v krajinách V4 nedošlo nikdy k efektívnemu rozkrytiu siete spolupracovníkov KGB a Štátnej bezpečnosti z čias Sovietskeho Zväzu, sú tieto krajiny v súčasnosti extrémne zraniteľné. Primárnym cieľom je nadkritická penetrácia Ozbrojených síl SR, resp. organizácií “tretieho sektora” združujúcich dôstojníkov, z ktorých mnohí buď nikdy nenadobudli dôveru voči novému štátnemu zriadeniu po roku 1989 a absolovovali výcvik ešte pod sovietskym vedením, alebo kombináciou rôznych vplyvov ich lojalita voči štátu, alebo NATO

významne poklesla, alebo úplne vymizla. **Časť z kedysi lojálnych dôstojníkov sa dokonca otvorene stavia proti platnej bezpečnostnej stratégii SR**. Situácia dospela do štádia, v ktorom značná časť ruskej vplyvovej agentúry už niekoľko rokov vystupuje úplne otvorene v prospech cudzej mocnosti a prejavuje otvorene nepriateľské postoje voči existujúcej vláde a proti našim spojeneckým záväzkom voči NATO a EÚ. (Útok na vedenie MOSR zo strany Asociácie Slovenských Vojakov)

V nezverejnenom špecializovanom prieskume vypracovanom analytickým oddelením jednej zo slovenských tajných služieb bol **zreteľne preukázaný kauzálny súvis medzi rýchlosťou rastu penetrácie bežného obyvateľstva dostupným vysokorýchlostným internetom, rastom počtu užívateľov sociálnych sietí a nárastom sympatií voči agende webov preukázateľne patriacich do sféry vplyvu GRU** medzi obyvateľstvom SR. Tento vývoj tiež opakovane nepriamo naznačujú aj verejne dostupné prieskumy rôznych agentúr, hoci žiaden z nich sa primárne nezameriaval na preukázanie tejto kauzality. Kombináciu výsledkov na sebe nezávislých prieskumov sa však podarilo hypotézu potvrdiť s pravdepodobnosťou hraničiacou s istotou.

Služba vonkajšej rozviedky RF je veľkosťou, zameraním a prevažne civilnou orientáciou porovnateľná s CIA. Ide teda o výrazne špecializovanú výzvednú službu, ktorej hlavnou úlohou je orientácia na **získavanie spolupracovníkov a informácií z prostredia politiky a jej ovplyvňovanie v prospech ruských záujmov**. Disponuje vlastnou nezávislou sieťou agentov a spolupracovníkov, odhadovaný počet aktívnych riadiacich dôstojníkov na území SR nepresahuje 100 osôb, ich úlohou je vytipovávať rôzne záujmové osoby a získavať ich pre vedomú spoluprácu, alebo nevedomú podporu kombináciou rôznych motivátorov, pričom sa vyznačuje kvalitnou a vysoko efektívnou HUMINT stratégiou. Podľa všetkého nie je pre väčšinu spolupracovníkov a členov vplyvovej agentúry Služby vonkajšej rozviedky RF rozhodujúcim motivátorom zvyčajne finančný, ani majetkový prospech: špecialisti pripravujúci verbovanie spolupracovníka uprednostňujú kombináciu vystavenia nádejného kandidáta nejakej dlhodobej ťažkej životnej situácii, prirodzene vzniknutej, alebo vyvolanej umelo nejakou formou provokácie, tzv. biodegradáciou (narušenie vzťahu falošnou komunikáciou s “milenkou” na fcb) s tým, že poskytnú “nezištnú” pomoc pri jej riešení. Prostredníctvom svojej siete potom pre budúceho spolupracovníka zabezpečia lepšie spoločenské postavenie, nápravu “havárie” a postupne mu umožnia opäť sa etablovať v lepšej spoločnosti. Viditeľným prejavom tejto stratégie je zdanlivo nepochopiteľná účasť bývalých nezmieriteľných ideových nepriateľov na spoločných akciách smerujúcich k mäkkej podpore ruského záujmu. V priebehu troch, až štyroch rokov je takto získaná osoba pod plným vplyvom svojich nových “priateľov”. Ak je to nevyhnutné, motivujú riadici dôstojníci záujmovú osobu aj majetkovo, a finančne, zvlášť v prípade, že z dôvodu časovej tiesne nie je možné použiť vyšie uvedenú metódu. Prakticky vždy však ekonomicky motivovaných spolupracovníkov považujú za menej spoľahlivých.

Internet je v tomto čase základným komunikačným protokolom, hoci **RF nikdy neupustila od využívania “klasických” rádiových frekvencií** a tak GRU, ako aj Služba vonkajšej rozviedky naďalej využíva aj pomerne zastaralú analógovú kódovanú komunikáciu, prakticky výhradne však iba pre vnútornú potrebu. V prípade, že dochádza ku komunikácii so sieťou spolupracovníkov obe služby používajú kombináciu verejných služieb typu gmail, yahoo, ale aj lokálnych poskytovateľov mailových a webových služieb s tým, že prakticky vždy pri odovzdávaní strategicky dôležitých informácií, alebo komunikácie, ktorá by mohla viesť k prezradeniu aj doplnkové šifrovanie (AES

Crypto, Xabber, Callgram, nepotvrdeny ostáva Signal). Až pri distribúcii (dez)informácií konečnému užívateľovi sú potom využívané tzv. klasické sociálne siete, teda facebook, twitter, vkontakte a podobne vzhľadom na ich schopnosť lavínovite a prakticky nekontrolovateľne šíriť toxický obsah. Dojem, že tajné služby Ruskej federácie využívajú ku komunikácii hlavne sociálne siete je teda iba sčasti pravdivý: v skutočnosti sú tieto služby využívané iba v okamihu, keď sa z pôvodne tajnej informácie určenej pre úzky okruh ľudí má stať vec verejná. Tento fakt dáva v konfrontácii s rozšírenou predstavou, že útokom na verejnú mienku zo strany RF sa nedá zabrániť vzhľadom na nekontrolovateľnú podobu sociálnych sietí nádej, že možno nájsť slabé miesto v ruskej stratégii ich zneužívania. Príležitosť pre bielch hackerov sa ukrýva práve na rozhraní medzi tajným a verejným.