Operačný program
Efektívna
verejná správa

Európska únia
Európsky sociálny fond

HYBRIDNÉ HROZBY NA SLOVENSKU

Energetická bezpečnosť

Analýza legislatívy, štruktúr a procesov

Tento projekt je podporený z Európskeho sociálneho fondu.

GLOBSEC
IDEAS SHAPING THE WORLD

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

AUTOR

Mgr. Matúš Mišík, PhD. je odborným asistentom na Katedre politológie Univerzity Komenského v Bratislave, špecializuje sa na energetickú politiku a vzťahy členských štátov v rámci Európskej únie.

Informácie v tejto publikácii sú aktuálne k 12. marcu 2019.

Text neprešiel jazykovou korektúrou.

METODOLÓGIA

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

GLOBSEC, Bratislava, marec 2019

GLOBSEC

Vajnorská 100/B

831 04 Bratislava

www.globsec.org

Táto analýza je súčasťou publikácie “HYBRIDNÉ HROZBY NA SLOVENSKU: Analýza legislatívy, štruktúr a procesov v šiestich tematických oblastiach”, ktorá je publikovaná na linke https://www.globsec.org/publications/hybridne-hrozby-na-slovensku-analyza-legislativy-struktur-a-procesov-v-siestich-tematickych-oblastiach/ a bola vydaná v rámci projektu „Zvyšovanie pripravenosti a kapacít verejnej správy na hybridné hrozby“, ktorý sa realizuje vďaka Operačnému programu Efektívna verejná správa a podpore z Európskeho sociálneho fondu.

OBSAH

I. ÚVOD

V oblasti energetiky pomenúva *Koncepcia pre boj SR proti hybridným hrozbám*,[1] schválená vládou SR v júli 2018, závislosť SR na dovoze energetických surovín z krajín mimo EÚ za možnú hybridnú hrozbu. Táto analytická správa však argumentuje, že uskutočnená diverzifikácia zdrojov a trás prepravy energetických nosičov, a predovšetkým zemného plynu, výrazne zvýšila bezpečnosť dodávok vytvorením významných alternatívnych možností dovozu zemného plynu zo zahraničia.

Navyše, energetická bezpečnosť v tradičnom ponímaní zabezpečenia dostatočného množstva energetických surovín a prevencie výpadkov v dodávkach spôsobených zneužívaním tzv. energetickej zbrane (*energy weapon*), je dlhodobo riešená orgánmi štátnej správy, najmä Ministerstvom hospodárstva (MH SR) a Ministerstvom zahraničných vecí (MZVEZ SR) Slovenskej republiky.

Na druhej strane predstavujú novšie typy hybridných ohrození energetickej bezpečnosti v spojení s kybernetickými útokmi na energetickú infraštruktúru novú oblasť pre orgány štátnej správy. To neznamená, že bezpečnosť dodávok energetických surovín nie je stále významnou témou pre štátnu správu – existujú však novšie a menej preskúmané hrozby v podobe kybernetických útokov, ktoré predstavujú v súčasnosti ešte väčšiu výzvu pre štátnu správu z pohľadu hybridných hrozieb. A to aj z toho dôvodu, že dnes ešte nie je vytvorený mechanizmus na ich zvládanie na rozdiel od „tradičných“ hrozieb. Tento text preto považuje kybernetické útoky na energetickú infraštruktúru za hlavný typ hybridných hrozieb v oblasti energetickej bezpečnosti.

Energetická politika sa vyznačuje komplexnosťou a veľkým počtom aktérov, ktorí sú do nej zahrnutí. Slovensko dováža veľkú väčšinu energetických surovín zo zahraničia – skoro všetok zemný plyn a ropu, veľkú väčšinu uhlia a všetko jadrové palivo. Po plynovej kríze v roku 2009 sa pozornosť štátnej správy upriamila predovšetkým na energetickú bezpečnosť a diverzifikáciu zdrojov dodávok, hlavne zemného plynu.

Dodávky energetických surovín, a teda aj energetickú bezpečnosť, však priamo nezabezpečuje štát, ktorý vytvára najmä právne a regulačné rámce v tejto oblasti a má do istej miery priamu kontrolu len nad niektorými hráčmi na slovenskom energetickom trhu, nakoľko vlastní podiely v niekoľkých spoločnostiach fungujúcich na tomto trhu.

Keďže sa táto analýza zameriava na štátnu správu, resp. štátnych aktérov, odporúčania z nej vyplývajúce sa sústreďujú na verejné politiky a na spoluprácu medzi štátnou správou a neštátnymi aktérmi. Väčšina konkrétnych opatrení v oblasti kybernetickej bezpečnosti je však vykonávaná na úrovni jednotlivých aktérov, obzvlášť výrobcov a prepravcov rôznych druhov energií, a preto je úlohou štátnej správy predovšetkým vytvoriť strategický rámec pre boj s kybernetickými hrozbami.

Hlavným zraniteľným miestom energetického sektora sú energetické siete, ktoré majú množstvo podobných znakov pri viacerých typoch energetických zdrojov. Najmä elektroenergetické, ropovodné a plynovodné siete sa vyznačujú komplexným systémom, ktorý je prepojený a založený na komunikácii cez počítačové systémy. Tematická analýza venujúca sa kybernetickej bezpečnosti predstavuje tieto hrozby z celkového pohľadu. Primárne zameranie tejto kapitoly o energetickej bezpečnosti však bude výhradne na kybernetické hrozby napojené na energetickú infraštruktúru.

Text ale predstaví aj všeobecné rámce kybernetických hrozieb a odpovedí štátnej správy na ne v podobne legislatívnych a iných nástrojov, a tým vytvorí ucelený prehľad o prostredí, v ktorom sa táto analýza pohybuje.

1 Vláda SR, Koncepcia pre boj SR proti hybridným hrozbám, schválená uznesením vlády SR č. 345/2018 dňa 11.7.2018, http://www.rokovania.sk/File.aspx/ViewDocumentHtml/Mater-Dokum-219866?prefixFile=m_

II. ZHRNUTIE ZISTENÍ A HLAVNÝCH ODPORÚČANÍ

Hlavným zistením tejto analýzy je, že vysoká závislosť Slovenskej republiky na dodávkach energetických surovín zo zahraničia nie je hlavnou hybridnou hrozbou tak, ako ju prezentuje *Koncepcia pre boj SR proti hybridným hrozbám*. V poslednom období totiž prišlo k výraznému posilneniu energetickej bezpečnosti SR proti prípadným výpadkom spôsobeným politickými rozhodnutiami (zapojenie tzv. *energy weapon*) posilnením diverzifikácie zdrojov a trás dodávok zemného plynu do SR.

Naopak, v oblasti kybernetickej bezpečnosti v súvislosti s kritickou infraštruktúrou nemá slovenská štátna správa doteraz bohaté skúsenosti. Koncepčné materiály v oblasti kybernetickej bezpečnosti boli prijaté len nedávno, a preto je nevyhnutné venovať sa tejto oblasti bližšie. Nemožno tvrdiť, že vysoká závislosť SR na dovoze energetických surovín nie je problém z pohľadu energetickej bezpečnosti, avšak v tejto oblasti existujú rôzne nástroje a prichádza k realizácii projektov, ktoré energetickú bezpečnosť podporujú, ako napríklad slovensko-poľské plynovodné prepojenie.

V oblasti ochrany kritickej energetickej infraštruktúry pred kybernetickými hrozbami však neexistujú v rámci SR jasne definované nástroje a postupy. Navyše, v rámci orgánov štátnej správy, ktoré majú energetickú bezpečnosť v primárnej agende, hlavne MH SR, ale aj MZVEZ SR, zatiaľ neboli vytvorené kapacity na riešenie týchto tém. Expertíza z oblasti energetickej bezpečnosti tak nie je prepojená s ďalšími aktérmi, ktorí majú v agende kybernetickú bezpečnosť (predovšetkým Národný bezpečnostný úrad).

Z týchto dôvodov analýza na základe detailného preskúmania situácie na Slovensku predstavuje aj súbor opatrení na zvýšenie odolnosti energetickej sústavy SR voči hybridným hrozbám. Najdôležitejším odporúčaním je presmerovať zameranie kľúčového strategického dokumentu v oblasti kybernetických hrozieb, ktorým je *Koncepcia pre boj SR proti hybridným hrozbám*, z dovozu energetických nosičov ako hlavnej hybridnej hrozby na kybernetické hrozby a ich možný vplyv na kritickú energetickú infraštruktúru. Medzi ďalšie odporúčania patrí zvýšená komunikácia medzi jednotlivými štátnymi inštitúciami, ktoré majú v agende energetickú bezpečnosť a kybernetické hrozby, hlavne NBÚ, MH SR a MZVEZ SR, alebo zahrnutie smart technológii do Koncepcie z dôvodu kľúčovej úlohy interkonektivity pre ich fungovanie.

III. POPIS PROSTREDIA A HROZIEB

Táto analýza sa zaoberá kybernetickými hrozbami v troch sektoroch energetiky – zemný plyn, elektrická energia a ropa. Najmä prvé dva typy energie sú z tohto pohľadu dôležité nielen pre ich vlastnosti, ale aj dôležitosť tranzitu pre Slovensko.

Tranzit ropy cez Slovensko je len minimálny (približne 6 miliónov ton ročne), a aj z pohľadu bezpečnosti má ropa lepšie postavenie vďaka svojim fyzickým vlastnostiam. Preto nepatrí medzi hlavné body záujmu v rámci energetickej bezpečnosti. Ropa sa môže prepravovať viacerými spôsobmi pri zachovaní približne rovnakej efektívnosti tranzitu, ľahšie sa skladuje a jej trh je globálny – preto je pri rope situácia ohľadom bezpečnosti na lepšej úrovni ako v oblasti zemného plynu.[2]

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

2 Slovensko má diverzifikované dodávky ropy. Takýto prístup sa ukázal ako kľúčový pre Českú republiku počas druhej polovice 90. rokov, ale aj neskôr, keď prestala prúdiť z Ruskej federácie polovica dohodnutého objemu ropy. V tom čase však už ČR dokončila ropovod IKL, a preto boli následky pre krajinu minimálne.

Slovensko patrí ku krajinám EÚ s najvyšším podielom jadrovej energie na elektrickom energetickom mixe, ktorý hovorí o zložení zdrojov, z ktorých sa elektrická energia vyrába. Z celkovej vyrobenej elektrickej energie na Slovensku – 27,1 TWh – pochádzalo v roku 2016 až 14,8 TWh z jadrovej energie,[3] čo je takmer 55%. Dva nové reaktory, ktoré majú byť dokončené v najbližšom období, Mochovce 3 a 4, prispejú do rozvodnej siete ďalšími približne 7 TWh elektrickej energie ročne. Následne sa zaradí Slovensko medzi čistých vývozcov energie,[4] čo bude mať následky aj pre existujúcu a práve sa rozvíjajúcu infraštruktúru.

Slovensko je významnou tranzitnou krajinou predovšetkým v oblasti zemného plynu. Eustream, slovenský operátor tranzitnej plynovodnej siete, má jednu z kapacitne najväčších prepravných sietí v Európe s kapacitou približne 100 mld. m^2 zemného plynu ročne na vstupnom bode z Ukrajiny. K nej je pripojená najväčšia kompresná stanica v strednej a východnej Európe s výkonom 300 MW, ktorá sa nachádza vo Veľkých Kapušanoch.

Slovensko je v oblasti zemného plynu prepojené s Českou republikou a Rakúskom pomocou spätného chodu na plynovode Bratstvo, s Ukrajinou tzv. malým reverzom cez Budince a s Maďarskom cez vstupný bod Veľké Zlievce. Vďaka týmto prepojeniam majú účastníci slovenského energetického trhu v súčasnosti kapacitné možnosti priviesť zemný plyn nielen z východného smeru cez Ukrajinu z Ruskej federácie, ale aj zo západnej Európy priamo zo zdrojov (napríklad Holandsko alebo Nórsko) alebo zo spotových trhov, predovšetkým tých v Nemecku. Mnohé obchodné toky už v súčasnosti prebiehajú zo západných smerov, keďže účastníci trhu nakupujú v západnej Európe, avšak podľa dostupných údajov fyzické toky stále prichádzajú aj z východu cez Ukrajinu.

Prepojenie s Poľskom sa v súčasnosti buduje aj s pomocou finančnej podpory zo strany EÚ[5] a bude mať veľmi pozitívny dosah na energetickú bezpečnosť SR, keďže umožní napojenie na poľský terminál na skvapalnený zemný plyn (LNG), ktorého trh je globálny, a predstavuje preto veľmi významné zvýšenie energetickej bezpečnosti. Navyše je v októbri 2022 plánované dokončenie nového plynovodu *Baltic Pipe,* ktorý zabezpečí dodatočné dodávky do Poľska z Nórska. Poľsko sa tak od roku 2022 chce stať úplne nezávislé od dodávok ruského zemného plynu.

Slovenský prepravca zemného plynu Eustream plánuje plynovod *Eastring*, ktorý má zabezpečiť napojenie na plánovaný plynovodný *hub* v Turecku, ktorý vznikne po dostavbe plynovodov *Turk Stream 2*[6] a *Trans-Anatolian Gas Pipeline (TANAP)*. Rovnako má tento plynovod reagovať aj na zmeny, ktoré s najväčšou pravdepodobnosťou nastanú po roku 2019 v preprave plynu cez Ukrajinu.[7]

V súčasnosti prebiehajú rokovania medzi Gazpromom a Naftogaz Ukrajiny o pokračovaní tranzitnej zmluvy, pričom Európska komisia sa snaží v tomto procese hrať úlohu mediátora a navrhla 60 bcm ako ročný prepravný objem zemného plynu cez Ukrajinu. Rokovania v januári 2019 však viedli len k dohode, že príde k ďalším rokovaniam v máji 2019. Hoci je *Eastring* len v počiatočnom štádiu príprav, dostáva výraznú politickú podporu zo strany EÚ ako aj slovenskej vlády.

Prepravca zemného plynu v Českej republike, Net4Gas, a.s., sa už v roku 2017 začal pripravovať na zmeny prúdenia zemného plynu z východného smeru na západný smer, teda z Nemecka cez ČR ďalej na Slovensko a Rakúsko. Slovenský prepravca Eustream, a.s. už taktiež začal rokovania s Gazpromom ohľadom podobného vývoja, no zatiaľ neboli zverejnené konkrétne informácie o kapacitách a dĺžke trvania plánovaných kontraktov. Súčasný kontrakt medzi Gazpromom a Eustreamom ohľadom prepravy cez slovenskú časť plynovodu *Bratstva* vyprší až v roku 2028, avšak jeho budúcnosť nie je po roku 2019 jasná.

3 Európska komisia, Energy datasheets: EU28 countries, 2018, https://ec.europa.eu/energy/sites/ener/files/documents/countrydatasheets_august2018.xlsx
4 V súčasnosti Slovensko dováža časť elektrickej energie zo zahraničia, avšak hlavne z toho dôvodu, že je to výhodnejšie, než ju produkovať v existujúcich elektrárňach.
5 Plynovodné prepojenie s Poľskom bolo zaradené na zoznam Projects of Common Interest a podporené z Connecting Europe Facility.
6 Turk Stream 1, ktorý je momentálne vo výstavbe, má slúžiť tureckým domácim potrebám.
7 Súčasná prepravná zmluva medzi Gazpromom a Naftogaz Ukrajiny končí 31. decembra 2019, pričom Gazprom už dlhodobejšie znižuje prepravované objemy plynu do Európy cez Ukrajinu, čo mu umožňuje plynovod Nord Stream. S vybudovaním plynovodu Nord Stream 2 a Turk Stream (ktorého prvé dve potrubia sú už vo výstavbe) bude môcť Gazprom úplne prerušiť alebo výrazne obmedziť tranzit plynu cez Ukrajinu. Viac v Pirani, S., Yafimava, K., Russian Gas Transit Across Ukraine Post-2019: pipeline scenarios, gas flow consequences, and regulatory constraints, The Oxford Institute for Energy Studies, 2016. Aj najnovšie analýzy potvrdzujú možnosť takéhoto scenára, resp. veľmi výrazného zníženia dodávok, na úroveň pod 10% celkovej kapacity: Sharples, J., Ukrainian Gas Transit: Still Vital for Russian Gas Supplies to Europe as Other Routes Reach Full Capacity, The Oxford Institute for Energy Studies, 2018.

V oblasti elektrickej energie je významné najmä prepojenie s Českou republikou, ktoré bolo vybudované počas obdobia federácie ako súčasť celorepublikovej sústavy. V súčasnosti sa buduje prepojenie s Maďarskom nielen na zvýšenie energetickej bezpečnosti, ale aj ako možný smer vývozu prebytkovej elektrickej energie po dobudovaní jadrovej elektrárne Mochovce 3 a 4. Toto prepojenie taktiež umožní slovenskému správcovi elektrizačnej sústavy, ktorým je Slovenská elektrizačná prenosová sústava, a.s., znížiť následky tzv. tranzitných tokov[8] na slovenskú sústavu odstránením úzkeho miesta (tzv. *bottleneck*) na slovensko-maďarskej hranici.

Slovensko má aj v oblasti ropy tranzitnú a rafinérsku kapacitu – Slovnaft, a.s. – hoci je rozsahovo menšia. Všetky tieto súčasti energetickej infraštruktúry môžu byť napadnuté kybernetickými hrozbami, ktoré môžu mať významné dopady nielen na energetickú bezpečnosť, ale aj na oblasť *hard security*.

Na Slovensku prišlo v minulosti k digitalizácii riadenia výroby elektrickej energie. Napríklad systém hydroelektrární na rieke Váh je plne automatizovaný s centrálnym riadením celého systému z Trenčína, kde sa nachádza Hydroenergetický dispečing. Všetky vodné elektrárne v pôsobnosti Slovenských elektrární, a.s., okrem PVE Čierny Váh, prešli do bezobslužného režimu od 1. januára 2009.[9]

IV. ANALÝZA LEGISLATÍVNEHO PROSTREDIA

Keďže tento text identifikuje kybernetické hrozby ako hlavný typ hybridných hrozieb v oblasti energetickej bezpečnosti, pri tomto prehľade legislatívneho prostredia bude vychádzať predovšetkým z existujúceho právneho prostredia v tejto oblasti v rámci SR ako aj EÚ, pretože právne predpisy v SR v tejto oblasti vychádzajú práve z právnych predpisov prijatých na úrovni EÚ.

Európska únia zahŕňa energetiku medzi oblasti, ktorých sa týkajú hybridné hrozby, najmä v súvislosti s ochranou strategickej infraštruktúry. V hlavnom strategickom dokumente tvrdí, že najlepší spôsob, ako reagovať na hybridné hrozby v oblasti energetickej bezpečnosti, je diverzifikácia v prípade energetických sietí a vytváranie najvyšších možných štandardov bezpečnosti v jadrovej energetike.[10] Tento dokument taktiež identifikuje budovanie *smart* technológií ako možnú rizikovú oblasť v rámci energetiky. *Európska energetická bezpečnostná stratégia* sa sústreďuje predovšetkým na tradičné hrozby, hoci spomína taktiež potrebu "*zvýšenej pozornosti*" bezpečnosti IT v oblasti strategickej infraštruktúry.[11]

Európska únia kritizovala členské štáty za nezaradenie nových hrozieb, mimo iných aj kybernetický útok, do scenárov, podľa ktorých sa uskutočnili tzv. *stress* testy energetickej bezpečnosti v oblasti zemného plynu.[12] Veľkú pozornosť hybridným hrozbám v oblasti energetiky venuje aj Európska služba pre vonkajšiu činnosť (EEAS), ktorá taktiež navrhuje diverzifikáciu a budovanie bezpečnostných štandardov ako odpoveď na tieto hrozby.

Celkový pohľad na problematiku kybernetickej bezpečnosti v kontexte hybridných hrozieb je možné nájsť v tematickej analýze venujúcej sa kybernetickej bezpečnosti.

Pre oblasť energetiky neexistuje špecifická právna úprava kybernetickej bezpečnosti energetickej infraštruktúry, avšak je zahrnutá do všeobecnej legislatívy o kritickej infraštruktúre. Pre účely tejto kapitoly je dôležité spomenúť najmä *smernicu o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii* (tzv. *NIS smernica*), ktorá bola prijatá v roku 2016, pričom členské štáty mali čas na transpozíciu tejto smernice do svojich právnych poriadkov do 9. mája 2018.[13] Smernica zavádza

8 Tie sú spôsobené nerovnováhou vo výrobe elektrickej energie v Nemecku zapríčinenou odstavením prvých 8 blokov jadrových elektrární po spustení procesu Atomausstieg, ktorý má do konca roku 2022 úplne odstrániť jadrovú energiu z nemeckého energetického mixu. Zvýšená produkcia elektrickej energie z obnoviteľných zdrojov spôsobila preťaženie domácich elektrických sietí a presmerovanie vnútroštátnych tokov do okolitých krajín (kruhové toky), ale aj export prebytočnej energie cez ďalšie krajiny vrátane Slovenska.

9 Slovenské elektrárne, Vodné elektrárne, 2010, https://www.seas.sk/data/contentlink/cfakepathhydro-power-plants-slovakia-2010-sk.pdf

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

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

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

13 Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii, 2016, https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:32016L1148&from=EN

koncept prevádzkovateľa základných služieb, kde sa v prílohe uvádza zoznam takýchto prevádzkovateľov. V článku 5, oddiel 1 sa pre členské štáty zaviedol cieľový dátum 8. november 2018 na identifikáciu takýchto prevádzkovateľov vo všetkých odvetviach a pododvetviach, ktoré smernica uvádza vo svojej prílohe č. 2.

Podľa článku 5, oddielu 2 smernice sú kritériá na identifikáciu prevádzkovateľov základných služieb nasledovné:

- Subjekt poskytuje službu, ktorá má zásadný význam z hľadiska zachovania kľúčových spoločenských a/alebo hospodárskych činností;
- poskytovanie tejto služby je závislé od sietí a informačných systémov a
- incident by mal závažný rušivý vplyv na poskytovanie uvedenej služby.

Príloha smernice pomenúva energetiku ako prvú zo siedmich identifikovaných skupín prevádzkovateľov základných služieb. Zemný plyn, elektrická energia a ropa sú tri identifikované energetické zdroje, pričom v rámci každého zdroja sú ďalej identifikovaní výrobcovia, prepravcovia, spracovatelia či distribučné spoločnosti ako prevádzkovatelia základných služieb.

Smernica 2016/1148 bola transponovaná do slovenského právneho poriadku *zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti*,[14] ktorý v § 4 pís. 2 určuje Ministerstvo hospodárstva Slovenskej republiky ako jeden z úradov pôsobiacich v oblasti kybernetickej bezpečnosti. *Zákon č. 69/2018* identifikuje v § 17 základnú službu a prevádzkovateľa základnej služby, ktorých zoznam je uvedený v prílohe 1. Tá uvádza energetiku ako piatu skupinu prevádzkovateľov a rozširuje zoznam o baníctvo (ktoré je tiež v gescii MH SR, ktoré je identifikované ako ústredný orgán pre danú skupiny prevádzkovateľov) a tepelnú energiu.

Do poslednej skupiny sú zaradení výrobcovia a dodávatelia tepla podľa *zákona č. 657/2004 Z. z. o tepelnej energetike.*[15] Medzi prevádzkovateľov základných služieb sú *zákonom č. 69/2018* zahrnuté aj prvky kritickej infraštruktúry podľa *zákona č. 45/2011 Z. z. o kritickej infraštruktúre,*[16] ktorý zaraďuje energetickú infraštruktúru do tejto skupiny. Tento zákon bol transpozíciou *smernice 2008/114/ES*, ktorá sa venovala európskej kritickej infraštruktúre.[17]

V. ANALÝZA ŠTRUKTÚR A PROCESOV

Slovensko sa v oblasti energetickej bezpečnosti sústredilo predovšetkým na otázku bezpečnosti dodávok energetických surovín (*energy security*), kým téma bezpečnosti prevádzky energetických zariadení a infraštruktúry (*safety*) sa zameriavala skôr na oblasť jadrovej energetiky. V iných sektoroch energetiky bola safety priraďovaná pozornosť hlavne v súvislosti s údržbou plynovodov a ropovodov.

Na Slovensku sa na úrovni ministerstiev zodpovedných za tému energetickej bezpečnosti – a energetickej politiky ako takej – ktorými sú MH SR a MZVEZ SR, doteraz systémovo neriešila otázka hybridných hrozieb v tomto sektore. Ako vyplynulo z rozhovoru so zástupcom MH SR, na tomto rezorte v súčasnosti prebieha diskusia o vytvorení pozície, ktorá by bola zameraná na hybridné, predovšetkým kybernetické, hrozby v oblasti energetiky. Momentálne však centrálna štátna správa nemá kapacity na analýzu kybernetických, resp. iných hybridných hrozieb v oblasti energetickej bezpečnosti.

Energetická bezpečnosť je do veľkej miery v rukách energetických spoločností, ktoré sú vo väčšine prípadov vo vlastníctve súkromných investorov, a štát má preto na ňu dosah najmä cez tvorbu verejných politík a regulačných rámcov. Niektoré kľúčové energetické spoločnosti ako SPP, a.s. a SEPS, a.s. sú stále v rukách

14 Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
15 Zákon č. 657/2004 Z. z. o tepelnej energetike
16 Zákon č. 45/2011 Z. z. o kritickej infraštruktúre
17 Smernica Rady EÚ 2008/114/ES z 8. decembra 2008 o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu, https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:32008L0114&from=EN. Táto smernica identifikuje zoznam sektorov, v ktorých sa nachádzajú takéto infraštruktúry v prílohe 1, pričom energetika je prvým sektorom a doprava druhým. V energetike identifikuje tri podsektory - elektrickú energiu, ropu a plyn, pričom v poslednej podskupine menovito hovorí o termináloch na skvapalnený plyn.

štátu úplne alebo do istej miery, ako napr. SPP Distribúcia, a.s., Eustream, a.s. alebo Slovenské elektrárne, a.s. Veľké množstvo hráčov na energetickom trhu je však čisto v súkromných rukách.

VI. ANALÝZA VEREJNÝCH POLITÍK

Podľa *Koncepcie pre boj SR proti hybridným hrozbám*[18] je závislosť slovenskej ekonomiky *„na dovoze strategických surovín, najmä energonosičov, od jedného externého dodávateľa“* problémová a označuje sa za možný druh hybridnej hrozby. Podľa Koncepcie diverzifikácia importu nepriniesla zmeny v energetickej bezpečnosti a existujúca energetická závislosť *„je zneužiteľná na vytváranie nátlaku zo strany dodávateľa a prípadná hrozba zastavenia dodávok surovín je potenciálne efektívnym nástrojom na vyvolávanie politického tlaku na SR alebo nespokojnosti medzi populáciou postihnutou sociálnym dosahom nedostatku energií“.* Energetickú politiku a infraštruktúru zaraďuje Koncepcia k dvom typom hybridných hrozieb:

- ekonomický alebo energetický nátlak ako rozšírenie politického nátlaku;
- rozsiahle sabotáže proti kľúčovej infraštruktúre.[19]

S takýmto nastavením hybridných hrozieb v oblasti energetickej bezpečnosti sa však dá polemizovať. Diverzifikácia trás a zdrojov zemného plynu, ktorá prebehla po plynovej kríze v roku 2009, výrazne zvýšila energetickú bezpečnosť v tomto sektore a zároveň výrazne znížila možnosť opakovania krízovej situácie do budúcnosti. Fyzická infraštruktúra umožňuje už v súčasnosti pokryť celkovú spotrebu Slovenska z alternatívnych zdrojov, pričom nové plynovodné prepojenie s Poľskom umožní prístup k zdrojom kvapalného zemného plynu.

Táto analýza preto považuje za omnoho významnejšiu hybridnú hrozbu kybernetické útoky na energetickú infraštruktúru. V roku 2015 schválila vláda *Koncepciu kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020*,[20] ktorá nadväzovala na predchádzajúce dokumenty v oblasti kybernetickej bezpečnosti. Stratégia sa venuje predovšetkým vytvoreniu uceleného rámca pre témy kybernetickej bezpečnosti na Slovensku, pričom jej hlavným cieľom je *„vybudovanie dôvery v spoľahlivosť a bezpečnosť najmä kritickej informačnej a komunikačnej infraštruktúry, ako aj istoty, že táto bude plniť svoje funkcie a slúžiť národným záujmom aj v prípade kybernetického útoku.”*[21]

Energetickú infraštruktúru označuje dokument za kritickú infraštruktúru vychádzajúc zo *zákona č. 45/2011 Z. z. o kritickej infraštruktúre*. Konkrétnym politikám alebo návrhom sa však koncepcia nevenuje. Detailnejšiu predstavu o jej aplikácii prináša až *Akčný plán realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020* prijatý v roku 2016.[22] Ten sa zmieňuje o kritickej infraštruktúre, avšak len vo všeobecnej rovine. Navyše MH SR ani nie je zaradené k subjektom podieľajúcim sa na príprave opatrení v tejto oblasti.

Stratégia energetickej bezpečnosti Slovenskej republiky z roku 2008[23] a *Energetická politika SR*[24] sa tiež však explicitne, ale ani implicitne, nevenujú téme kybernetických hrozieb. Hlavný dôraz kladú tieto dokumenty na bezpečnosť dodávok a budovanie alternatívnych prepojení. Ani každoročne uverejňované správy o výsledkoch monitorovania bezpečnosti dodávok plynu a elektriny neprinášajú informácie o takýchto hrozbách.

18 Vláda SR, Koncepcia pre boj SR proti hybridným hrozbám, schválená uznesením vlády SR č. 345/2018 dňa 11.7.2018, http://www.rokovania.sk/File.aspx/ViewDocumentHtml/Mater-Dokum-219866?prefixFile=m_
19 Ibid.
20 NBÚ, Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020, 2015, http://www.nbusr.sk/wp-content/uploads/kybernetickabezpecnost/Koncepcia-kybernetickej-bezpecnosti-SR-na-roky-2015-2020-A4.pdf
21 Ibid., str. 10.
22 NBÚ, Akčný plán realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020, 2016, http://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Akcny-plan-realizacie-Koncepcie-kybernetickej-bezpecnosti-SR-na-roky-2015-2020.pdf
23 Ministerstvo hospodárstva SR, Stratégia energetickej bezpečnosti SR, 2008, http://www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=14372
24 Energetická politika SR, 2015, http://www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=23993

VII. ODPORÚČANIA

V rámci slovenskej diskusie o energetickej politike a energetickej bezpečnosti sa téme kybernetických hrozieb nevenuje takmer žiadna pozornosť. Rozhovory s predstaviteľmi Ministerstva hospodárstva SR ako aj s členom parlamentu, ktorý sa venuje téme energetickej bezpečnosti, poukázali na to, že existuje istá diskusia v medzi MH SR, Národným bezpečnostným úradom a Ministerstvom vnútra SR ohľadom kybernetických hrozieb v oblasti energetiky. Z tejto analýzy však vyplýva, že strategické dokumenty jednotlivých aktérov v oblasti energetickej politiky sa zameriavajú na odlišné aspekty kybernetickej bezpečnosti, a preto je otázne, nakoľko prichádza ku synergii v rámci týchto diskusií.

Podľa rozhovoru so zástupcom Ministerstva zahraničných vecí ČR sa v Českej republike pre účely zvýšenia ochrany energetickej infraštruktúry pred kybernetickými útokmi rozhodli pre postupné zníženie množstva automatizovaných operácií riadených počítačom v rámci sieťových prvkov, ktoré sú najviac náchylné na kybernetické útoky, ako napr. elektrické rozvodne. Tie majú byť nahradené fyzickými procesmi, pri ktorých bude nevyhnutné zapojenie operátorov. Týmto opatrením má prísť k zníženiu zraniteľnosti infraštruktúry, a hoci ani takéto riešenie neznamená úplné odstránenie všetkých bezpečnostných hrozieb, keďže stále ostane zachovaná možnosť korupcie, vydierania a pod., očakáva sa od neho zvýšenie celkovej bezpečnosti systému.

Na Slovensku je energetická infraštruktúra zaradená medzi kritickú infraštruktúru, a tak sa k nej pristupuje aj v rámci diskusie o kybernetických hrozbách. Hrozby v oblasti energetickej infraštruktúry môžu mať dopad nielen na energetickú bezpečnosť v zmysle prerušenia dodávok energetických zdrojov a nenaplnenia potrieb koncových užívateľov, ale aj na oblasť *hard security* pri kybernetických útokoch na elektrárne, predovšetkým na jadrové, a tiež pri útokoch na infraštruktúru. Vzhľadom na dôležitosť jadrovej energetiky ako aj prepravnej infraštruktúry, najmä plynovodnej, pre Slovenskú republiku by mali témy spojené s kybernetickými ohrozeniami získať dominantnejšie miesto v rámci bezpečnostného diskurzu.

ODPORÚČANIA PRE TVORBU VEREJNÝCH POLITÍK

- Presmerovať zameranie kľúčového strategického dokumentu v oblasti hybridných hrozieb (Koncepcia pre boj SR proti hybridným hrozbám) z dovozu energetických nosičov ako hlavnej hybridnej hrozby na kybernetické hrozby a ich možný vplyv na kritickú energetickú infraštruktúru.
- Zintenzívniť komunikáciu medzi jednotlivými štátnymi inštitúciami, ktoré majú v agende energetickú bezpečnosť a kybernetické hrozby – predovšetkým Národný bezpečnostný úrad, Ministerstvo hospodárstva a Ministerstvo zahraničných vecí a európskych záležitostí.
- Klásť väčší dôraz na špecifiká energetického sektora, ktorý je odlišný od iných oblastí kritickej infraštruktúry, pretože hybridné hrozby v tejto oblasti majú dôsledky nielen pre energetickú bezpečnosť, ale aj pre hard security.
- Zahrnúť smart technológie do diskusie o možných hybridných hrozbách v oblasti energetickej bezpečnosti.

VIII. ZÁVER

Slovensko je nielen významnou tranzitnou krajinou, ale zároveň aj štátom, ktorý dováža veľkú väčšinu energetických surovín zo zahraničia. Aj preto boli po plynovej kríze v roku 2009 prijaté opatrenia, ktoré sa zamerali na zlepšenie energetickej bezpečnosti a diverzifikáciu zdrojov dodávok, hlavne čo sa týka zemného plynu.

Vďaka tomu je Slovenská republika omnoho lepšie pripravená na „tradičné“ hrozby, ktoré sa s energetickou bezpečnosťou spájajú. Aj z toho dôvodu nie je potrebné, aby boli tieto „tradičné“ hrozby opätovne uvádzané v *Koncepcii pre boj SR proti hybridným hrozbám*. Naopak, tento dokument by sa mal zamerať na kybernetickú zložku ohrozenia energetickej bezpečnosti, ktorá v našej legislatíve ani dokumentoch nie je dostatočne reflektovaná.

NÁVRH NA OPATRENIE ZAMERANÉ NA ZEFEKTÍVNENIE VEREJNEJ SPRÁVY

ZAHRNÚŤ KYBERNETICKÉ HROZBY A ICH MOŽNÝ VPLYV NA KRITICKÚ ENERGETICKÚ INFRAŠTRUKTÚRU DO KONCEPCIE PRE BOJ SR PROTI HYBRIDNÝM HROZBÁM

SUBJEKT, KTORÉMU JE ADRESOVANÉ

Národný bezpečnostný úrad SR

CIEĽ OPATRENIA

V súčasnosti sa hlavná pozornosť Koncepcie v oblasti energetiky venuje „tradičným“ témam energetickej bezpečnosti ako prerušenie dodávok alebo všeobecné problémy so zásobovaním SR energiami z tretích krajín. Týmito témami sa však intenzívne zaoberá Ministerstvo hospodárstva aj Ministerstvo zahraničných vecí a európskych záležitostí. Taktiež sa situácia na Slovensku výrazne zmenila následkom plynovej krízy v roku 2009, ktorá zapôsobila ako katalyzátor diverzifikácie a posilnenia energetickej bezpečnosti Slovenskej republiky.

Takéto „tradičné“ témy energetickej bezpečnosti preto nemožno považovať za primárne typy hybridných hrozieb a pozornosť je potrebné presmerovať k témam spojeným so zraniteľnosťou kritickej infraštruktúry, akou sú plynovody/ropovody, zásobníky plynu/ropy, kompresorové stanice, jadrové elektrárne a pod. Väčšia pozornosť v rámci Koncepcie by mala byť zameraná predovšetkým na kybernetické hrozby spojené s kritickou infraštruktúrou, ktoré nie sú pokryté v existujúcich strategických dokumentoch a v rámci orgánov štátnej správy sa im v súčasnosti ešte len začína venovať viac pozornosti. Koncepcia sa navyše zaoberá kybernetickými hrozbami vo všeobecnosti, čo z nej robí veľmi dobrý priestor na zahrnutie tém spojených s kritickou infraštruktúrou v energetike.

Hoci existuje istá diskusia medzi Ministerstvom hospodárstva SR, NBÚ a Ministerstvom vnútra SR ohľadom kybernetických hrozieb v oblasti energetiky, strategické dokumenty jednotlivých aktérov v tejto oblasti sa zameriavajú na odlišné aspekty kybernetickej bezpečnosti v oblasti energetickej politiky. Preto je otázne, nakoľko prichádza k synergii v rámci tejto diskusie. Zahrnutie kybernetických hrozieb do Koncepcie by podporilo premostenie tejto témy medzi jednotlivými zložkami štátnej správy, keďže by vytvorilo jasnejší prienik agend medzi NBÚ, MH SR, MV SR a MZVEZ.

SPÔSOB REALIZÁCIE OPATRENIA

Zahrnúť tému kybernetických hrozieb voči kritickej energetickej infraštruktúre do Koncepcie pre boj SR proti hybridným hrozbám a zaradiť túto oblasť k ďalším témam kybernetických hrozieb. To posilní možnosti aktivity v tejto oblasti a zvýši synergiu medzi jednotlivými témami ochrany kritickej infraštruktúry – nielen energetickej – voči kybernetickým hrozbám.

FINÁLNY STAV A DOPADY OPATRENIA

Kybernetická bezpečnosť kritickej infraštruktúry v oblasti energetiky bude zahrnutá do Koncepcie pre boj SR proti hybridným hrozbám, čo vytvorí strategický rámec pre ďalšie aktivity štátnej správy v oblasti ochrany energetickej infraštruktúry pred kybernetickými hrozbami. Tým bude doplnený súčasný stav, kedy existujú strategické dokumenty v oblasti energetickej bezpečnosti, predovšetkým Energetická politika SR.

TERMÍN REALIZÁCIE

Najbližšia aktualizácia Koncepcie pre boj SR proti hybridným hrozbám ponúkne vhodný priestor pre zahrnutie kybernetických hrozieb v oblasti energetiky do tohto strategického dokumentu.