STRATÉGIA KYBERNETICKEJ OBRANY SLOVENSKEJ REPUBLIKY

Bratislava 2022

ÚVOD

1. Jednou zo základných funkcií štátu je zabezpečovať vlastnú obranu. Tá predstavuje súhrn opatrení, ktorými sa zachováva mier, bezpečnosť, zvrchovanosť, územná celistvosť a nedotknuteľnosť hraníc, ako aj plnenie opatrení vyplývajúcich z medzinárodných zmlúv o spoločnej obrane proti napadnutiu a z ďalších medzinárodných zmlúv vojenskej povahy, ktorými je Slovenská republika viazaná. Kybernetický priestor je po pozemnom priestore, námornom priestore, vzdušnom priestore a kozmickom priestore ďalšou operačnou doménou, v rámci ktorej štát plní vyššie uvedenú úlohu.

2. Obrana štátu sa preto vykonáva aj v kybernetickom priestore prostredníctvom kybernetických operácií zameraných na riešenie závažných kybernetických bezpečnostných incidentov a na obranu prvkov kritickej infraštruktúry a objektov osobitnej dôležitosti, ďalších dôležitých objektov, ktoré sú určené na zabezpečenie obrany a obranyschopnosti štátu (ďalej len „kybernetická obrana“).

3. Technologický pokrok v oblasti informačných a komunikačných technológií predstavuje okrem nových príležitostí aj zdroj hrozieb, ktoré majú dopad na celkové zabezpečenie obrany štátu a použitie ozbrojených síl Slovenskej republiky (ďalej len „OS SR“). Rastie počet kybernetických útokov zo strany štátnych a neštátnych aktérov ako aj ich celková zložitosť. Kybernetické útoky sú uskutočňované takým spôsobom, aby boli ťažko identifikovateľné, prisúditeľné konkrétnemu aktérovi a nemohli byť považované za klasický konvenčný útok v zmysle medzinárodného práva. Potenciálnemu útočníkovi pomáha aj samotný charakter kybernetického priestoru, v rámci ktorého neexistujú časové alebo geografické obmedzenia. Na druhej strane kybernetický priestor predstavuje novú operačnú doménu, ktorej charakter a prepojenosť s ostatnými operačnými doménami vytvára priestor na synergiu a efektívne použitie vojenskej sily, ekonomizáciu vynakladaných nákladov a dosahovanie zámerov veliteľa v reálnom čase.

4. *Stratégia kybernetickej obrany Slovenskej republiky* (ďalej len „*Stratégia*“) určuje prístupy na zabezpečenie obrany národného kybernetického priestoru v stave bezpečnosti, v čase núdzového stavu, výnimočného stavu, vojnového stavu ako aj vojny, či obrany jednotiek OS SR použitých na plnenie úloh na území Slovenskej republiky a mimo územia Slovenskej republiky.

5. *Stratégia* vychádza z národných a medzinárodných strategických dokumentov, národnej legislatívy na úseku obrany štátu a kybernetickej bezpečnosti a medzinárodných záväzkov, ktorými je Slovenská republika viazaná.

6. *Stratégia* stanovuje svoj cieľ, stanovuje kľúčové princípy, popisuje aktuálne bezpečnostné prostredie v rámci kybernetického priestoru, identifikuje hrozby v kybernetickom priestore a navrhuje opatrenia na zaistenie kybernetickej obrany štátu.

7. Úspešným plnením opatrení navrhnutých v *Stratégii* sa Slovenská republika začlení medzi tie členské krajiny Organizácie Severoatlantickej zmluvy (ďalej len „NATO“) a Európskej únie (ďalej len „EÚ“), ktoré disponujú národnými kybernetickými spôsobilosťami

potrebnými na adekvátne zabezpečenie vlastnej obrany a zároveň prispievajú k posilňovaniu bezpečnosti euroatlantického priestoru.

I. CIEĽ STRATÉGIE

8. Cieľom *Stratégie* je určiť rámec pre budovanie národných kybernetických spôsobilostí potrebných pre zabezpečenie kybernetickej obrany Slovenskej republiky, rovnako ako aj informačnej a komunikačnej infraštruktúry OS SR a Vojenského spravodajstva nasadzovanej na území Slovenskej republiky, ako aj mimo územia Slovenskej republiky, ktoré umožnia vykonávanie obranných, útočných, podporných a spravodajských kybernetických operácii a plnenie medzinárodných záväzkov.

II. KĽÚČOVÉ PRINCÍPY STRATÉGIE

9. Slovenská republika bude pri zabezpečovaní kybernetickej obrany postupovať v súlade s nasledovnými princípmi:

   a) Za obranu Slovenskej republiky zodpovedá vláda Slovenskej republiky. Ministerstvo obrany Slovenskej republiky je okrem iného ústredným orgánom štátnej správy pre riadenie a kontrolu obrany Slovenskej republiky. Ministerstvo obrany Slovenskej republiky zabezpečuje plnenie tejto úlohy v kybernetickom priestore prostredníctvom Vojenského spravodajstva v spolupráci s OS SR.

   b) Prvky riadenia kybernetickej obrany budú založené na princípe riadenia rizík, podpore, spolupráci, prevencie a kontinuálneho budovania spôsobilostí a kapacít.

   c) V rámci komplexného prístupu ku kybernetickej obrane bude Ministerstvo obrany Slovenskej republiky rozvíjať spoluprácu s ďalšími orgánmi verejnej správy Slovenskej republiky, súkromným a akademickým sektorom a zvyšovať povedomie obyvateľov Slovenskej republiky o kybernetickej obrane a v spolupráci s Národným bezpečnostným úradom aj o kybernetickej bezpečnosti.

   d) Dodržiavanie národnej legislatívy, základných ľudských a občianskych práv a slobôd, ako aj princípov demokratického zriadenia štátu.

   e) Dodržiavanie záväzkov vyplývajúcich z medzinárodných zmlúv a záväzkov vyplývajúcich z členstva v NATO, EÚ a Organizácii Spojených národov, ktorými je Slovenská republika viazaná, rovnako ako aj členstva Slovenskej republiky v iných globálnych a regionálnych medzinárodných organizáciách.

   f) Rešpektovanie, že kybernetický priestor je nedeliteľnou operačnou doménou, ktorej zabezpečenie a obrana si vyžaduje komplexnú spoluprácu na národnej a medzinárodnej úrovni.

   g) Primeranosť použitia kybernetických spôsobilostí.

III. KYBERNETICKÝ PRIESTOR A BEZPEČNOSTNÉ PROSTREDIE

10. Z pohľadu kybernetického priestoru je bezpečnostné prostredie Slovenskej republiky determinované nie len jej členstvom v EÚ a NATO, ale aj rozvojom, šírením a vojenským využitím technológií, ktoré zvyšujú sofistikovanosť hrozieb, komplexnosť ich účinkov, možnosti ohrozenia štátu a skracujú čas na jeho reakciu. Kybernetický priestor sa preto stáva kľúčovým dejiskom geopolitického súperenia, čo má za následok nárast hrozieb, ktoré môžu negatívne ovplyvniť riadenie obrany štátu, velenie ozbrojených síl a funkčnosť infraštruktúry dôležitej pre obranu štátu.

11. Kybernetický priestor predstavuje novú operačnú doménu vytvorenú človekom. Okrem človeka sa na tvorbe kybernetického priestoru podieľa aj umelá inteligencia, ktorá je v súčasnosti už aj jeho súčasťou. Je možné predpokladať, že z dlhodobého hľadiska bude umelá inteligencia pri tvorbe kybernetického priestoru zohrávať významnejšiu úlohu ako človek.

12. Vo všeobecnosti je možné konštatovať, že kybernetický priestor je tvorený súborom troch vrstiev:

    a) personálnou vrstvou, ktorú predstavujú fyzické a právnické osoby pôsobiace v kybernetickom priestore prostredníctvom jednej alebo viacerých virtuálnych identít;

    b) logickou vrstvou, ktorú predstavujú softvér a údaje;

    c) fyzickou vrstvou, ktorú predstavujú hardvér a prvky informačnej a komunikačnej infraštruktúry.

13. Špecifickou vlastnosťou kybernetického priestoru z pohľadu obrany štátu a použitia OS SR je skutočnosť, že táto operačná doména priamo ovplyvňuje ďalšie operačné domény. Táto špecifická vlastnosť kybernetického priestoru ponúka na úseku vedenia bojovej činnosti množstvo príležitostí na strategickej, operačnej a taktickej úrovni, výsledkom čoho je dosahovanie výrazných synergických efektov s relatívne nízkymi nákladmi.

14. Jednou zo základných charakteristík kybernetického priestoru je závislosť na informačnej a komunikačnej infraštruktúre a umelej inteligencie na zdrojoch elektrickej energie, ako aj vzájomná prepojenosť informačnej a komunikačnej infraštruktúry. Táto prepojenosť má globálny a komplexný charakter čím zasahuje do všetkých fyzických operačných domén, pričom nie je vymedzená žiadnymi fyzickými ani geografickými hranicami. Rastúce množstvo informácií, formy a metódy ich spracovania, nároky a požiadavky na ich ukladanie a spracovanie, rovnako aj časový faktor dokazujú komplexnosť kybernetického priestoru.

15. Významná časť informačnej a komunikačnej infraštruktúry je vo vlastníctve a prevádzke subjektov súkromného sektora.

16. V kybernetickom priestore neúmerne narastá význam neštátnych aktérov, ktorí predstavujú široké spektrum entít počnúc fyzickými osobami, cez legálne a nelegálne subjekty

rozličného zamerania a významu, končiac transnacionálnymi aktérmi so širokým spektrom pôsobnosti,

17. Anonymita a vysoká miera sofistikovanosti útokov významne sťažujú prisúdenie škodlivých aktivít konkrétnemu bezpečnostnému aktérovi. Tento bezpečnostný problém sa môže ešte prehĺbiť v prípade neregulovaného rozvoja umelej inteligencie. Kybernetický priestor ponúka nové možnosti pre hybridný spôsob vedenia bojových činností, pôsobenie spravodajských služieb, nelegálne aktivity jednotlivcov alebo entít z teroristického či kriminálneho prostredia.

18. Z civilného hľadiska poskytuje kybernetický priestor prelomové príležitosti pre celospoločenský rozvoj a zlepšovanie kvality života a služieb. Z vojenského hľadiska poskytuje významné príležitosti predovšetkým v oblasti zvyšovania bojového potenciálu prostredníctvom nasadzovania kybernetických prostriedkov na podporu kinetických operácií ozbrojených síl, ako aj v oblasti dosahovania strategickej rovnováhy a stability štátu.

IV. HROZBY V KYBERNETICKOM PRIESTORE

19. Slovenská republika v kybernetickom priestore môže čeliť najmä nasledujúcim hrozbám:

    a) kybernetickému útoku, ktorý môže zapríčiniť škody porovnateľné s následkami ozbrojených útokov;

    b) kybernetickej kríze, kde kybernetický útok zapríčinil škody veľkého rozsahu a paralyzuje viaceré prvky kybernetickej bezpečnosti a kybernetickej obrany naraz, pričom jeho dopad a dosah môžu predstavovať podstatný vplyv na riadenie štátu;

    c) dočasnému alebo dlhodobému vyradeniu obrannej a kritickej infraštruktúry alebo ich častí;

    d) dočasnému alebo dlhodobému paralyzovaniu systémov velenia a riadenia OS SR;

    e) dočasnému alebo dlhodobému znefunkčneniu alebo narušeniu poskytovaných služieb alebo prístupov k nim v jednotlivých sektoroch verejnej správy a súkromného sektora;

    f) zneužitiu kybernetického priestoru na znemožnenie alebo sťaženie prisúdenia škodlivých aktivít konkrétneho aktéra voči obrannej infraštruktúre, kritickej infraštruktúre alebo jej časti;

    g) skrytému prevzatiu a/alebo skrytej modifikácii systémových procesov a služieb, ich častí alebo prístupov k nim v jednotlivých sektoroch verejnej správy a súkromného sektora s cieľom ich využívania alebo zneužívania na vojenské, spravodajské, teroristické a iné nelegálne účely;

    h) odcudzeniu a zneužitiu alebo modifikácii dát, databáz, osobných údajov, citlivých informácií, neverejných informácií a utajovaných skutočností na vojenské, spravodajské, trestné alebo teroristické aktivity;

i) využívaniu kybernetického priestoru na šírenie dezinformácií na strategickej úrovni ako súčasti hybridného/vplyvového pôsobenia na vybrané cieľové skupiny spoločnosti, vrátane OS SR;

j) zneužitiu kybernetického priestoru štátnym alebo neštátnym aktérom spôsobilým poškodiť základy demokracie, narúšať, obmedzovať alebo potláčať základné ľudské práva a slobody;

k) zneužitiu nových, vyvíjaných a experimentálnych technológií zo strany štátnych aj neštátnych aktérov v kybernetickom priestore na ohrozenie záujmov Slovenskej republiky;

l) skryté alebo otvorené jednorazové alebo opakujúce sa narušenie obrany kybernetického priestoru Slovenskej republiky v personálnej vrstve vedomou alebo nevedomou spoluprácou jednotlivca alebo skupiny v spojení s cudzou mocou alebo s cudzím činiteľom so zámerom poškodiť ústavné zriadenie alebo obranyschopnosť Slovenskej republiky.

V. KYBERNETICKÁ OBRANA V PODMIENKACH SLOVENSKEJ REPUBLIKY

20. Vedecko-technologický pokrok, vznik nových technológií a rozvoj umelej inteligencie vytvára predpoklady pre vysokú mieru neistoty vo vzťahu k budúcnosti, predvídateľnosti a prognózam ďalšieho vývoja. V oblasti zvyšovania bojového potenciálu a vojenských implikácií predstavuje najvýznamnejšiu príležitosť predovšetkým využívanie umelej inteligencie pre podporu veliteľských rozhodovacích procesov, riadiacich procesov, ako aj zabezpečovanie obrany informačnej a komunikačnej infraštruktúry, nasadzovanie dronov, autonómnych a robotických zbraňových systémov, vysoko-presnej a inteligentnej munície a raketových systémov, systémov prieskumu a riadenia paľby, systémov rušenia a elektronického boja, komunikačných systémov, neurónových sietí a kryptografických šifrovacích systémov, optických maskovacích technológií a nano-biotechnologických systémov.

21. Na zabezpečenie realizácie cieľa *Stratégie* a z neho vyplývajúcich povinností na úseku obrany štátu je potrebné:

a) Rozvíjať plnohodnotné národné spôsobilosti kybernetickej obrany

22. Vojenské spravodajstvo a vybrané prvky OS SR budú systematicky budovať národné spôsobilosti kybernetickej obrany, prostredníctvom ktorých budú schopné vykonávať kybernetické operácie. Konkrétne spôsobilosti, rozsah, doba a zodpovednosť za budovanie budú bližšie popisné v Akčnom pláne kybernetickej obrany Slovenskej republiky. Primárnym krokom je zabezpečenie dlhodobej kontinuity pri implementácii strategických rozhodnutí a opatrení vo vzťahu k problematike kybernetického priestoru. Cieľom bude vytvorenie legislatívneho a doktrinálneho rámca Slovenskej republiky na vykonávanie kybernetickej obrany v súlade s Ústavou Slovenskej republiky, všeobecne záväznými právnymi predpismi, princípmi demokratického a právneho štátu,

medzinárodnými záväzkami a etickými normami. To umožní nastavenie väzieb a definovanie zodpovedností medzi Vojenským spravodajstvom a vybranými prvkami OS SR. Takýto legislatívny a doktrinálny rámec bude reflektovať existujúce národné a medzinárodné záväzky, politiky a strategické dokumenty. V podmienkach rezortu obrany je potrebné nastaviť jasné riadenie, budovať a posilňovať štruktúry a prvky kybernetickej obrany a ich interakcie pre potreby dosahovania synergie v oblasti kybernetickej obrany, ako aj plnenia záväzkov kolektívnej obrany v stave bezpečnosti, v čase núdzového stavu, výnimočného stavu, vojnového stavu a vojny.

23. Systematicky sa budú rozvíjať a zdokonaľovať spôsobilosti Vojenského spravodajstva ako najdôležitejšieho národného výkonného prvku systému kybernetickej obrany v zmysle aktuálneho doktrinálneho rámca NATO. Cieľom Vojenského spravodajstva bude kvalifikované plnenie úloh vrcholného riadiaceho a koordinačného prvku kybernetickej obrany v plnom spektre, ktoré budú zahŕňať plánovanie, prípravu, koordináciu a výkon nasledovných kybernetických operácií:

    a) operácie na podporu infraštruktúry komunikačných a informačných systémov (CISIO – Communication and Information Infrastructure Operations);

    b) operácie zamerané na získavanie spravodajských informácií, sledovanie a prieskum v kybernetickom priestore (CISRO – Cyberspace Intelligence, Surveillance and Reconnaissance Operations);

    c) obranné operácie v kybernetickom priestore (DCO – Defensive Cyber Operations);

    d) útočné operácie v kybernetickom priestore (OCO – Offensive Cyber Operations).

24. Základnou podmienkou pre budovanie plnohodnotných národných spôsobilostí v oblasti kybernetickej obrany je zabezpečenie stability dlhodobého zdrojového a finančného rámca a ľudských zdrojov. Ľudské zdroje predstavujú najdôležitejšiu a najcennejšiu spôsobilosť kybernetickej obrany. Získanie, udržanie a rozvíjanie odborne zdatného personálu predstavuje úlohu, ktorá si vyžaduje dôkladnú personálnu politiku na všetkých stupňoch riadenia. Personálna politika bude nastavená tak, aby bola vojenská služba atraktívna, motivačná a adekvátne finančne ohodnotená s cieľom dlhodobého udržania odborníkov v štruktúrach. Tento princíp bude v podmienkach rezortu obrany platiť aj pre štátnych zamestnancov a zamestnancov pri výkone práce vo verejnom záujme, ktorí vykonávajú činnosti na úseku kybernetickej obrany v rámci plnenia služobných úloh a tiež školiaceho personálu a akademického zboru v pôsobnosti rezortu obrany. Zároveň bude rozvíjaný systém odborného rastu vo forme pravidelných odborných školení a výcviku pre personál, pravidelná účasť na národných a medzinárodných odborných kurzoch a cvičeniach. Personálna politika bude reflektovať moderné trendy v oblasti zabezpečenia odborného personálu.

b) Budovať a rozvíjať nasaditeľné kybernetické spôsobilosti OS SR

25. OS SR vybudujú nasaditeľné kybernetické spôsobilosti v rozsahu príslušnej národnej legislatívy v súlade s Cieľmi spôsobilostí NATO a procesom Koordinovaného ročného hodnotenia obrany v rámci Stálej štruktúrovanej spolupráce EÚ. Základným

predpokladom úspešného budovania nasaditeľných kybernetických spôsobilostí OS SR je zavedenie systému vzájomných väzieb a prvkov, nastavenie systematickej spolupráce medzi Vojenským spravodajstvom a OS SR. To je kľúčové pre úspešné použitie OS SR na území Slovenskej republiky, ako aj mimo územia Slovenskej republiky v stave bezpečnosti a v čase núdzového stavu, výnimočného stavu, vojnového stavu a vojny. Pre úspešné použitie OS SR na úseku obrany štátu a kolektívnej obrany vo všetkých operačných doménach je potrebné zabezpečiť ucelenú, kompaktnú a kompatibilnú nasaditeľnú informačnú a komunikačnú infraštruktúru, ktorá umožní zabezpečený prenos, spracovanie a zdieľanie utajovaných a neutajovaných informácií v reálnom čase. Pri plánovaní použitia OS SR na účely obrany štátu je nevyhnutné implementovať do plánov aj úlohy týkajúce sa kybernetickej obrany štátu.

c) Implementovať medzinárodné záväzky kybernetickej obrany

26. Slovenská republika rešpektuje svoje politické a právne záväzky v oblasti kybernetickej obrany, ktoré jej vyplývajú z členstva v NATO a EÚ a vynaloží úsilie, aby tieto záväzky boli plnené v deklarovaných termínoch. Pri budovaní obranných spôsobilostí bude rezort obrany nastavovať pravidlá a kritéria na svoje zbraňové systémy v súlade s normami a štandardmi NATO a EÚ. Rezort obrany zabezpečí, že informačné a komunikačné systémy, zavádzané v podmienkach rezortu obrany budú plne kompatibilné s minimálnymi požiadavkami NATO a EÚ. Za týmto účelom budú revidované a vytvorené národné politické smernice, bezpečnostné projekty a nariadenia. V záujme účinného vykonávania integrovaného prístupu NATO a EÚ bude Slovenská republika v plnej miere súdržným spôsobom využívať všetky dostupné politiky a nástroje NATO a EÚ a maximalizovať synergie a komplementárnosť medzi vnútornou a vonkajšou bezpečnosťou, bezpečnosťou a rozvojom, ako aj civilným a vojenským rozmerom bezpečnostnej a obrannej politiky Slovenskej republiky.

d) Posilňovať spoluprácu medzi príslušnými štátnymi inštitúciami, súkromným sektorom a akademickým sektorom

27. Napriek skutočnosti, že na jednej strane kybernetický priestor predstavuje špecifické implikácie separátne pre civilný a vojenský sektor, na druhej strane ide taktiež o operačnú doménu, v rámci ktorej sa navzájom oba sektory prelínajú. Z tohto dôvodu je na účely komplexného a efektívneho zabezpečenia kybernetickej obrany nezastupiteľná existencia spolupráce medzi civilným a vojenským sektorom.

28. Z dôvodu efektívneho využitia obmedzených finančných zdrojov ako aj maximálneho využitia limitovaného ľudského kapitálu, rezort obrany bude spolupracovať pri zabezpečovaní kybernetickej obrany v čo najširšej možnej miere so štátnymi inštitúciami s dôrazom na Národný bezpečnostný úrad, Slovenskú informačnú službu, Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky a Ministerstvo vnútra Slovenskej republiky a takisto aj so súkromným a akademickým sektorom. Cieľom takejto spolupráce je:

a) prevencia a posilňovanie odolnosti obrannej informačnej a komunikačnej infraštruktúry voči kybernetickým hrozbám;

b) riešenie a znižovanie dopadov kybernetických bezpečnostných incidentov;

c) zamedzenie zneužívaniu národného kybernetického priestoru pre uskutočnenie kybernetických útokov;

d) asistencia pri obnovovaní činnosti napadnutých informačných a komunikačných systémov;

e) obrana pred novými a budúcimi typmi hrozieb;

f) organizácia spoločných výcvikov a cvičení v oblasti kybernetickej obrany na národnej úrovni a spoločná koordinovaná účasť na medzinárodných cvičeniach.

29. Tento cieľ bude dosahovaný prostredníctvom vzájomného zdieľania informácií o platných riadiacich dokumentoch, legislatívnych povinnostiach, technologických a praktických poznatkoch, ako aj najlepších skúseností pri zabezpečovaní informačných a komunikačných systémov. Rezort obrany poskytne v prípade potreby v rozsahu svojich kompetencií súčinnosť aj na technickom stupni prostredníctvom jednotky CSIRT.MIL.SK. Výsledkom tejto spolupráce bude posilnenie kybernetickej odolnosti kľúčovej informačnej a komunikačnej infraštruktúry štátneho, súkromného a akademického sektora, čo v konečnom dôsledku prispeje k zefektívneniu obrany Slovenskej republiky v kybernetickom priestore. Vo vzťahu k vzdelávacím, školiacim a výcvikovým inštitúciám zriadeným v pôsobnosti rezortu obrany bude potrebné venovať zvýšenú pozornosť aj adekvátnemu materiálnemu a personálnemu zabezpečeniu.

e) Zvyšovať odbornosť a povedomie v oblasti kybernetickej obrany

30. Riziko zlyhania ľudského faktora nie je možné nikdy plnohodnotne odstrániť, ale je možné ho výrazne zredukovať prostredníctvom budovania bezpečnostného povedomia a odborného vzdelávania na úrovni používateľa, experta a riadiaceho pracovníka. Rezort obrany bude pokračovať v rozvoji systému bezpečnostného povedomia, budovania, udržania a rozvoja systému vzdelávania a prípravy špecialistov, odborníkov a personálu, ako aj kybernetickej hygieny zamestnancov a profesionálnych vojakov. Cieľom bude prehlbovanie vedomostí, praktických zručností a takisto šírenie osvety týkajúcej sa osvojenia správnych a bezpečných návykov a zásad pri práci s informačnými a komunikačnými technológiami. Rezort obrany je pripravený v prípade záujmu poskytovať takéto odborné vzdelávanie a šírenie osvety aj príslušníkom iných ozbrojených zborov a zamestnancom ostatných ústredných orgánov štátnej správy. Dôležitým prvkom v oblasti zabezpečenie kybernetickej obrany bude aj zvyšovanie gramotnosti verejnosti vo vzťahu ku kybernetickému priestoru a aktivitám, ktoré s ním súvisia. V konečnom dôsledku Slovenská republika na úseku kybernetickej obrany štátu musí disponovať kompetentnými a preverenými ľudskými zdrojmi.

f) Zlepšovať povedomie o kybernetických hrozbách prostredníctvom zdieľania informácií a hodnotení

31. Čeliť kybernetickým hrozbám nie je možné bez detailného poznania špecifík kybernetických hrozieb a ich pôvodcov. Rezort obrany bude participovať na národných a medzinárodných platformách, ktoré sú zamerané na zdieľanie technických a politických

informácií týkajúcich sa existujúcich a potenciálnych kybernetických hrozieb. Na bilaterálnej úrovni bude rezort obrany presadzovať nadväzovanie, budovanie, udržiavanie a posilňovanie vzťahov s partnerskými inštitúciami členských a partnerských krajín NATO a EÚ, ako aj s orgánmi NATO a EÚ. Výsledkom musí byť získavanie a poskytovanie širokého situačného povedomia o kybernetických hrozbách v reálnom čase našim partnerom na národnej a medzinárodnej úrovni.

g) Podporovať vzdelávanie, výcvik a cvičenia

32. Základným predpokladom na výkon efektívnej kybernetickej obrany je existencia odborne zdatného a adekvátne vycvičeného personálu. Rezort obrany v spolupráci so vzdelávacími inštitúciami vo svojej pôsobnosti, ako aj vzdelávacími inštitúciami NATO a EÚ bude pripravovať vzdelávacie a výcvikové programy určené pre operácie v kybernetickom priestore na taktickej, operačnej a strategickej úrovni . Rezort obrany bude zabezpečovať pravidelnú účasť na medzinárodných a národných cvičeniach, odborných seminároch a iných aktivitách, ktorých cieľom bude posilňovanie spôsobilostí vedenia kybernetických operácií pre potreby zabezpečovania kybernetickej obrany.

ZÁVER

33. Opatrenia identifikované v tejto Stratégii podrobnejšie rozpracuje rezort obrany vo forme úloh v separátnom podpornom dokumente na jej vykonanie - *Akčný plán Stratégie kybernetickej obrany Slovenskej republiky*, ktorý vzhľadom na svoj charakter bude vypracovaný v príslušnom stupni utajenia v zmysle platnej národnej legislatívy.

34. *Stratégiu* schvaľuje vláda Slovenskej republiky, pričom jej plnenie bude vyhodnocované každoročne v gescii Rady na zabezpečenie kybernetického priestoru (ďalej len „Rada“) zriadenej v pôsobnosti rezortu obrany. Výsledné odpočtové plnenie bude predkladané prostredníctvom predsedu Rady ministrovi obrany Slovenskej republiky, ktorý bude informovať vládu Slovenskej republiky.

35. *Stratégia* je platná na obdobie spravidla 5 rokov pričom sa bude aktualizovať pri zásadnej zmene vývoja v oblasti bezpečnostného prostredia, technologického rozvoja, vývoja problematiky kybernetickej obrany NATO a EÚ a vývoja vojenstva, na základe získaných praktických skúseností a pri zásadnej zmene zdrojového rámca zabezpečovania kybernetickej obrany Slovenskej republiky.