NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

Národná stratégia kybernetickej bezpečnosti na roky 2026 až 2030

Obsah

I. Úvod

Fungovanie modernej digitálnej spoločnosti si vyžaduje dôveru v technológie a ich bezpečnosť, v čom kľúčovú úlohu zohráva štát. Rezonujúcim fenoménom je vývoj a rýchle nasadzovanie technológii umelej inteligencie. Zavádzanie týchto prvkov do digitálneho prostredia môže zvýšiť efektívnosť výkonu verejných politík, kvalitu služieb, zrýchliť vývoj a výskum, zefektívniť priemysel a skvalitniť bežný život obyvateľov. A aj v tejto oblasti je kybernetická bezpečnosť zásadným a kľúčovým faktorom na dosiahnutie vysokej úrovne kvality riadenia štátu, udržanie ústavno-právneho poriadku štátu, demokratickej spoločnosti a ekonomického rastu. **Národná stratégia kybernetickej bezpečnosti Slovenskej republiky na roky 2026 až 2030** (ďalej len „národná stratégia“) **je základným dokumentom, ktorý definuje priority a ciele** tak, aby v nasledujúcom období bola dosiahnutá adekvátna bezpečnosť kybernetického priestoru s prihliadnutím na vývoj nových technológií a s nimi aj nových hrozieb.

Národná stratégia stanovuje viacero strategických cieľov **v piatich prioritných oblastiach**:

1. **Ochrana národného kybernetického priestoru**
2. **Budovanie národných kapacít**
3. **Bezpečné a inovatívne digitálne produkty a služby**
4. **Vzdelávanie, zručnosti a povedomie**
5. **Strategické partnerstvá a medzinárodná spolupráca**

Návrh strategických cieľov reaguje na vnútorné a vonkajšie faktory, ktoré v súčasnosti kybernetickú bezpečnosť ovplyvňujú. Zohľadňuje dosiahnuté výsledky z predchádzajúceho obdobia a súčasný stav kybernetickej bezpečnosti, ako aj dynamiku budúceho vývoja, či už sa týka vývoja bezpečnostných hrozieb alebo technológií.

II. Vonkajšie faktory ovplyvňujúce kybernetickú bezpečnosť

Geopolitika a medzinárodné vzťahy

Kybernetický priestor je doménou globálnej politiky a celkového bezpečnostného prostredia. Digitalizácia štátov, vrátane ich ekonomík a verejných služieb spôsobuje, že stabilita a odolnosť kybernetického priestoru, ako taká, priamo ovplyvňuje národnú a medzinárodnú bezpečnosť. Takýto trend v nasledujúcich rokoch nepoľaví a jeho tempo bude určovať najmä rastúca polarizácia ideových skupín, technologická rivalita veľmocí ako aj intenzívne súťaženie o kontrolu nad údajmi či informačnými tokmi.

Z pohľadu najsilnejších vonkajších faktorov **súčasnú bezpečnostnú situáciu** v Európe zásadne ovplyvňuje pretrvávajúci **ozbrojený konflikt medzi Ruskou federáciou a Ukrajinou**, ktorý zároveň ukazuje, že kybernetické operácie sú neoddeliteľnou súčasťou moderného vojenského a politického pôsobenia. V priebehu konfliktu boli zaznamenané rozsiahle kybernetické útoky na energetické siete, médiá a štátne inštitúcie v Európskej únii (ďalej len „EÚ“), ako aj cielené kampane zamerané na manipuláciu verejnej mienky. Takýto vývoj preto mení bezpečnostné doktríny v Európe a posilňuje potrebu komplexného prístupu k obrane a bezpečnosti kybernetického priestoru.

Neuhasínajúce **napätie na Blízkom východe**, najmä pretrvávajúce regionálne konflikty Izraela s Iránom a militantnými moslimskými skupinami, majú okrem iného priamy dosah na vnútornú bezpečnosť EÚ a prispievajú k zvýšenej aktivite teroristických a hacktivistických skupín v širšom kontexte hybridných hrozieb.

Popri týchto konfliktoch rastie **vplyv Čínskej ľudovej republiky**, ktorá disponuje ohromným ľudským, ekonomickým a technologickým potenciálom. Čína, ktorá je nepochybne hegemónom juhozápadnej Ázie, sa postupne stáva globálnou veľmocou a jej centrálne riadená politika ovplyvňuje tiež zvyšné kontinenty sveta vrátane Európy. Čína je pre Európu nielen významným obchodným partnerom, ale zároveň aj systémovým rivalom. Jej rýchly rozvoj v oblasti vznikajúcich a prelomových technológií so zreteľom na režim, v ktorom sa aplikujú, predstavuje pre demokratické štáty početné výzvy nielen v oblasti technologickej autonómnosti a dôveryhodnosti ale najmä z pohľadu bezpečnosti. Čoraz väčší vplyv si Čína oproti minulosti uzurpuje aj **v medzinárodných organizáciách** vrátane tých zameraných na technológie [napríklad Medzinárodná telekomunikačná únia (ďalej len „ITU“), či iné štandardizačné orgány].

Súčasne sme svedkami, že **Spojené štáty americké prehodnocujú svoje vzťahy** s globálnymi partnermi. Táto snaha o optimalizáciu vlastného vplyvu znižuje predvídateľnosť ich zahraničnej politiky a vedie k záveru, že na americké vedenie sa v niektorých prípadoch na medzinárodnej scéne nemožno bezpodmienečne spoliehať. Zmeny sú zjavné aj na chode medzinárodných organizácií [napríklad Organizácia Spojených národov (ďalej len „OSN“), Organizácia Spojených národov pre vzdelávanie, vedu a kultúru, Rada Európy, Organizácia pre bezpečnosť a spoluprácu v Európe (ďalej len „OBSE“)], čo vytvára tlak na EÚ, aby posilnila svoju strategickú autonómiu a zvýšila investície do svojej obrany a kybernetickej bezpečnosti.

Preto sa dnes EÚ cíti byť ohrozenejšia než kedykoľvek pred tým. Bezpečnostné prostredie narúšajú hybridné operácie vrátane zahraničnej manipulácie a zasahovania do informačného priestoru (tzv. FIMI), kybernetické útoky na jej kritickú infraštruktúru a demokratické inštitúcie. K tomu sa pridávajú nové riziká vyplývajúce z klimatických zmien, degradácie životného prostredia a potenciálnych pandémií, ktoré môžu mať sekundárny dopad na digitálnu a kritickú infraštruktúru.

Pozícia Slovenskej republiky v geopolitickom priestore

Slovenská republika je pevnou súčasťou západného civilizačného okruhu, založeného na princípoch demokracie, právneho štátu, na základných ľudských právach a slobodách. **Spolupráca** s kľúčovými partnermi **na európskej, transatlantickej aj globálnej úrovni** ako aj dôsledné rešpektovanie medzinárodného poriadku a jeho noriem, posilňuje jeho príspevok ku kolektívnej odolnosti a prispieva k presadzovaniu spoločného naratívu EÚ, ktorého pevnou súčasťou je kybernetická bezpečnosť.

Bezpečnostné garancie pre Slovenskú republiku predstavujú predovšetkým Organizácia Severoatlantickej zmluvy (ďalej len „NATO“) a EÚ, ktoré poskytujú strategické, technologické a bezpečnostné zázemie, okrem iného, pre spoločné projekty, výmenu informácií a koordináciu reakcií na kybernetické bezpečnostné incidenty. Slovenská republika zároveň posilňuje svoje väzby a aktívne prispieva k činnosti **OBSE**, **Organizácie pre hospodársku spoluprácu a rozvoj** (ďalej len „OECD“), **ITU**, **Rady Európy** a **OSN**, ktoré zohrávajú významnú úlohu pri formovaní medzinárodných noriem a politík v oblasti kybernetickej bezpečnosti.

Kybernetické hrozby a trend ich vývoja

Dominantnými štátnymi aktérmi hrozieb v kybernetickom priestore zostávajú **Ruská federácia**, **Čínska ľudová republika**, ako aj **Kórejská ľudovodemokratická republika** a **Irán**. Tieto krajiny dlhodobo využívajú kybernetické operácie ako nástroj politického, spravodajského, vojenského a ekonomického pôsobenia. Ich činnosť je podporovaná štátom a často realizovaná prostredníctvom skupín, ktoré sa zameriavajú na pokročilé pretrvávajúce hrozby (tzv. APT skupiny), ergo vysoko organizovaných jednotiek, ktoré cielene prenikajú do sietí verejných inštitúcií, strategických podnikov a infraštruktúr kritických odvetví. Cieľom ich aktivít je získať prístup k citlivým informáciám, získať politický vplyv, narušiť dôveru v demokratické inštitúcie, destabilizovať spoločnosť alebo ekonomicky poškodiť konkurentov.

Medzi jednotlivými formáciami sú však určité rozdiely. **Ruské skupiny** sa sústreďujú najmä na hybridné operácie, kombinujúce **dezinformačné kampane**, **kybernetické útoky** a **psychologické pôsobenie** s cieľom oslabiť jednotu EÚ a NATO. **Čínske aktivity** majú prevažne **spravodajsko-ekonomický charakter**, zameraný na získavanie duševného vlastníctva, technologického know-how a na ovplyvňovanie dodávateľských reťazcov. **Kórejská ľudovodemokratická republika** využíva kybernetické útoky ako nástroj **finančného zabezpečenia režimu**, typicky prostredníctvom krádeží kryptomien a ransomvérových útokov. **Iránske aktivity** majú často **regionálny a ideologický** rozmer, pričom ciele nachádzajú najmä v oblasti energetiky a verejnej správy.

Podľa správy ***ENISA Threat Landscape 2025***, ktorá analyzovala viac ako 4 800 incidentov v období júl 2024 – jún 2025, zostávajú **štátom podporované skupiny a kyberzločinecké siete** hlavnými pôvodcami útokov proti členským štátom EÚ. **Najčastejším cieľom** sú **verejné**

inštitúcie (vyše 1/3 incidentov), nasledované sektormi **energetiky, dopravy, zdravotníctva a finančných služieb**. Prichádza tu tiež k rastúcej **konvergencii taktik a nástrojov** medzi štátnymi, kriminálnymi a aktivistickými skupinami, teda k prelínaniu motivácií, zdieľaniu nástrojov a k outsourcingu útočných kapacít medzi rôznymi typmi aktérov.

Významným trendom je tiež nárast **útokov vedených hacktivistami** (väčšinou typu **DDoS** – distribuovaný útok odmietnutia služby, *angl. Distributed denial-of-Service*), ktoré majú ideologické alebo politické pozadie, pričom sa čoraz častejšie prelínajú s agendou štátov alebo spriaznených subjektov. Tento jav potvrdzuje prechod od izolovaných kyberútokov ku **koordinovaným hybridným operáciám**, ktoré spájajú digitálne a informačné pôsobenie.

Popri štátnych aktéroch zohrávajú významnú úlohu aj **neštátni aktéri – hacktivisti, organizovaný kybernetický zločin a súkromné subjekty**, ktorých motivácie siahajú od ideologických po finančné. Rýchly rozvoj digitálneho podsvetia priniesol model **„kyberkriminality ako služby“** *(angl. Cybercrime-as-a-Service)*, v ktorom sú útočné nástroje, či prístupové údaje ponúkané na predaj alebo prenájom. Tento model zásadne znižuje technologickú bariéru pre nových páchateľov a zvyšuje celkový objem kybernetických útokov.

Pre **Slovenskú republiku** predstavujú tieto hrozby **komplexnú výzvu**. Útoky na verejné inštitúcie, samosprávy, univerzity, energetické a finančné podniky potvrdzujú, že štát i súkromný sektor sú vystavené rovnakým typom rizík ako väčšie európske krajiny. Ochrana pred nimi si vyžaduje **posilnenie spravodajskej a operatívnej spolupráce, koordinovaný monitoring hrozieb**, systematické **vyhodnocovanie rizík** a rýchlu **výmenu informácií o kybernetických bezpečnostných incidentoch** medzi národnými a európskymi orgánmi.

Technologické trendy a globalizácia dodávateľských reťazcov

Kvantové technológie

Európska komisia vydala ***Odporúčanie o Pláne koordinovaného vykonávania prechodu na postkvantovú kryptografiu***, ktorého cieľom je zabezpečiť jednotný a postupný prechod členských štátov na kvantovo odolné kryptografické riešenia. Na základe tohto odporúčania bol následne vypracovaný dokument ***Koordinovaný Plán vykonávania prechodu na postkvantovú kryptografiu***, ktorý slúži ako rámec pre koordinovaný prechod na kvantovo odolné šifrovanie. Táto mapa určuje základné princípy, etapy a zodpovednosti členských štátov pri **adaptácii na postkvantovú kryptografiu** (ďalej len „PQC“) v závislosti od kritickosti sektorov a systémov.

V nadväznosti na túto iniciatívu je pre Slovenskú republiku strategickým cieľom pripraviť a realizovať opatrenia na prechod na PQC. Na tomto prechode by mali byť zainteresovaní relevantní aktéri naprieč štátnou správou, súkromným sektorom a akademickou sférou. Národný bezpečnostný úrad bude poskytovať metodickú pomoc pri prechode na PQC algoritmy, tiež vydá osobitnú stratégiu kryptografickej ochrany a prechodu na PQC, ktorá bude obsahovať konkrétne ciele a úlohy v tejto oblasti. V rámci týchto opatrení Národný bezpečnostný úrad už vydal ***Odporúčania pre kryptografické algoritmy***, ktorých cieľom je zvýšiť povedomie a používanie moderných a overených kryptografických algoritmov s dôrazom na vysokú úroveň bezpečnosti a odolnosť voči kvantovým hrozbám.

Rozvoj kvantových technológií zásadne mení prostredie kybernetickej bezpečnosti. Kvantové počítače svojím výpočtovým výkonom dokážu teoreticky prelomiť väčšinu súčasných asymetrických kryptografických algoritmov, založených na diskrétnych algoritmoch a eliptických krivkách, ktoré tvoria základ dôveryhodnosti a bezpečnosti digitálnej komunikácie, elektronických služieb či ochrany údajov. Tento posun vytvára **potrebu včasného prechodu na nové, PQC mechanizmy,** ktoré zostanú bezpečné aj v ére kvantových počítačov.

Útoky typu „ukradni teraz – dešifruj neskôr“ predstavujú vážnu hrozbu, kedy súčasné dostatočne šifrované údaje môžu byť v budúcnosti dešifrované pomocou kvantových počítačov. Z toho dôvodu **je nevyhnutné** v predstihu reagovať na potenciálne hrozby vyplývajúce z rozvoja kvantových počítačov a **aplikovať existujúce PQC algoritmy** najmä v kritických systémoch a investovať do prechodu na bezpečnú a odolnú kryptografiu.

Prechod na PQC bude prebiehať postupne, na základe platnej legislatívy a v súlade so štandardami. Kryptografia nestojí len na štandardoch, technických riešeniach a ich správnej implementácii. Ak oblasť kryptografickej ochrany informácií nie je dostatočne legislatívne ošetrená, môže dochádzať k nesprávnej, alebo žiadnej implementácii vhodných opatrení na strane prevádzkovateľov systémov a služieb, resp. k nesprávnemu výkladu povinností, ktoré vyplývajú z právnych predpisov. Preto je správne legislatívne ukotvenie tejto problematiky nevyhnutné pre správnu implementáciu technických bezpečnostných opatrení súvisiacich s kryptografiou. Pre súkromný sektor má prípadná realizácia opatrení prechodu na PQC odporúčací charakter a v rámci predchádzania tzv. goldplatingu bude ich zozáväznenie pre súkromný sektor podmienené platnou európskou legislatívou.

Umelá inteligencia, produkty s digitálnymi prvkami a kybernetická bezpečnosť

Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie (**akt o umelej inteligencii**) je považované za prvý komplexný rámec, ktorý upravuje používanie umelej inteligencie a má ambíciu sa stať globálne uznávaným štandardom v oblasti regulácie umelej inteligencie.

Akt o umelej inteligencii je vzájomne prepojený s Nariadením Európskeho parlamentu a Rady (EÚ) 2024/2847 z 23. októbra 2024 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami (**akt o kybernetickej odolnosti**). Obe nariadenia sa však na seba explicitne odvolávajú, a to práve za účelom zabezpečenia kybernetickej bezpečnosti vysokorizikových systémov umelej inteligencie. Systémy umelej inteligencie majú podliehať ucelenému a koherentnému režimu kybernetickej bezpečnosti. Zároveň však platí, že táto harmonizácia nesmie viesť k zníženiu úrovne ochrany, ktorú stanovuje akt o kybernetickej odolnosti pre dôležité a kritické produkty s digitálnymi prvkami. Cieľom je znížiť regulačnú záťaž a súčasne zvýšiť právnu istotu pre výrobcov vysokorizikových systémov umelej inteligencie, najmä v komplexných prípadoch, kde umelá inteligencia a kybernetická bezpečnosť tvoria neoddeliteľný celok.

Akt o kybernetickej odolnosti predstavuje európsku legislatívu zameriavajúcu sa na zvýšenie úrovne bezpečnosti všetkých produktov, ktoré obsahujú digitálne prvky, s výnimkou produktov, pokrytých inými predpismi EÚ (napríklad zdravotnícke pomôcky, automobily a pod.) Praktická implementácia opatrení povedie k posilneniu kybernetickej bezpečnosti, keďže produkty s digitálnymi prvkami budú môcť byť uvedené na trh iba po odstránení

všetkých známych zneužiteľných zraniteľností. Výrobca týchto produktov je povinný počas vývoja a celého predpokladaného životného cyklu produktu zaručiť rovnakú úroveň kybernetickej odolnosti.

Umelá inteligencia patrí medzi najvýznamnejšie technologické trendy súčasnosti, ktorá zásadne mení digitálne prostredie aj spôsob fungovania spoločnosti.

Systémy umelej inteligencie dopĺňajú alebo nahrádzajú klasické systémy, otvárajúc úplne **nové spôsoby použitia, schopnosti a služby**, ktoré predtým neboli možné. Tým pretvárajú celé odvetvia. Zároveň sa však pochopenie hrozieb umelej inteligencie ešte len vyvíja a výskum nepretržite prináša nové a nové výzvy, hrozby a zraniteľnosti. Táto kombinácia predstavuje výrazné riziko pre úroveň kybernetickej bezpečnosti, najmä ak zavádzanie a používanie umelej inteligencie je živelné a bez uvedomenia si zodpovednosti a jasne definovaných pravidiel.

Využitie umelej inteligencie predstavuje aj významný prínos pre posilnenie ochrany digitálneho priestoru. Umožňuje rýchlejšiu a presnejšiu detekciu kybernetických bezpečnostných incidentov, efektívnejšiu analýzu hrozieb, spracovanie veľkého objemu údajov a podporu forenzných analýz. Vďaka týmto schopnostiam zvyšuje efektivitu reakcie na kybernetické bezpečnostné incidenty a prispieva k ochrane jednotlivcov, organizácií a kritickej infraštruktúry.

Systémy umelej inteligencie menia charakter útokov, prispievajú k **automatizácii phishingových útokov, generujú škodlivý kód, vyhľadávajú zraniteľnosti v systémoch, obchádzajú detekčné mechanizmy systémov**, či analyzujú správanie používateľov s cieľom **prispôsobiť útoky sociálneho inžinierstva** ich zvykom a správaniu. Objavujú sa aj formy malvéru, ktoré využívajú mechanizmy umelej inteligencie a dynamicky menia svoje správanie a upravujú ho v závislosti od identifikovaných obranných mechanizmov nastavených v systémoch alebo správania správcov systémov. Tieto javy, známe aj ako ***„weaponizácia umelej inteligencie“*, predstavujú zásadnú výzvu pre kybernetickú bezpečnosť**.

Umelá inteligencia už v súčasnosti prispieva k **informačným operáciám**. Systémy umelej inteligencie sú na sociálnych sieťach schopné automatizovane generovať množstvo príspevkov, často s cieľom ovplyvňovania používateľov alebo vedenia informačných operácií. Schopnosť umelej inteligencie vytvárať realistické ***„deepfake“*** videá napodobňovať hlasy či generovať vierohodné webové stránky vedie k oslabeniu dôvery vo verejný priestor a sťažuje odlíšenie reality od manipulácie.

Ďalšou výzvou sú **vnútorné zraniteľnosti samotných systémov umelej inteligencie**. Manipulácia tréningových údajov, ako vstupných databáz *(angl. data poisoning)* a pozmeňovanie vstupov môže viesť k chybným či účelovo zavádzajúcim výstupom. Na rozdiel od tradičného softvéru, kde je zneužitie možné najmä po nasadení systému, pri umelej inteligencii môže dôjsť k riziku už počas fázy učenia, čo výrazne komplikuje detekciu a nápravu takýchto zraniteľností.

V neposlednom rade **je dôležité riešiť regulačné a etické dilemy**, pretože rýchly rozvoj **umelej inteligencie vyžaduje robustné rámce zodpovedného využitia** (transparentnosť, kontrolovateľnosť a ochrana ľudských práv) v súlade s európskym prístupom známym ako ***„dôveryhodná umelá inteligencia zameraná na človeka“*** *(angl. Human-centred trustworthy Artificial Intelligence)*.

5G/6G

Implementácia 5G/6G technológií zásadne rozširuje a v budúcnosti rozšíria možnosti využívania digitálnej konektivity naprieč spoločnosťou aj hospodárskymi odvetviami. Táto moderná infraštruktúra umožňuje **rozvoj nových produktov a služieb**, ktoré menia fungovanie zdravotníctva, dopravy, energetiky, verejnej správy aj priemyslu. Zásadne rozširuje **konektivitu internetu vecí** *(angl. Internet of Things)*. V priemysle prináša kľúčový základ pre **rozvoj konceptu Priemyslu 4.0**, založeného na prepojení inteligentných zariadení, robotiky, umelej inteligencie a internetu vecí, ktoré umožňujú automatizáciu a optimalizáciu výrobných procesov.

Takéto prepojené prostredie však zároveň prináša **nové riziká**. 5G siete prenášajú rozsiahle množstvo citlivých údajov a tvoria základ kritickej digitálnej infraštruktúry, pričom ich **menej centralizovaná architektúra**, **vyššia závislosť od softvéru, sieťové a aplikačné rozhrania** a potreba väčšieho počtu zariadení vytvárajú **nové vstupné miesta pre útočníkov**. Zaistenie ich bezpečnosti a odolnosti je preto nevyhnutné nielen pre ochranu používateľov, ale aj pre stabilitu hospodárstva a spoločnosti.

Ďalšia generácia, **siete 6G**, prinesie ešte **hlbšiu integráciu komunikácie, senzorických funkcií**, ako aj **prepojenie s prvkami satelitnej infraštruktúry**. Očakáva sa širšie využitie veľmi vysokých frekvencií a nových architektúr, čo zvýši nároky na ochranu údajov, autentifikáciu a spoľahlivosť zariadení. **Sieť bude vo väčšej miere riadená algoritmami strojového učenia**, ktoré bude potrebné chrániť pred manipuláciou a zneužitím. Prioritou bude aj **pripravenosť na kvantové hrozby**, bezpečnosť zariadení a uzlov už od fázy návrhu a dôsledná správa kryptografických kľúčov. Nasadenie 6G sietí sa očakáva približne v roku 2030.

Bezpečnosť dodávateľských reťazcov

Dodávateľské reťazce sú dnes elementárnou súčasťou digitálnej infraštruktúry a zabezpečujú životný cyklus produktov a služieb, od vývoja a výroby, cez distribúciu a údržbu, až po ich vyradenie z používania. Ich stabilita a odolnosť je nevyhnutná pre plynulé fungovanie kritických sektorov, ako sú energetika, doprava, zdravotníctvo, telekomunikácie, financie či verejná správa.

V súčasnosti sú dodávateľské reťazce informačných a komunikačných technológií **pomerne komplexné z hľadiska vzájomnej obchodnej previazanosti v globálnom meradle** a prechádzajú viacerými právnymi systémami. Vzájomná prepojenosť nepriaznivo pôsobí na vytváranie závislosti od externých partnerov, pričom **rastie riziko prenosu zraniteľností** naprieč celým systémom. Aj jediný narušený článok v reťazci môže mať vážne následky. **Zlyhanie kybernetickej bezpečnosti dodávateľa vytvára vektor útoku**, ktorý môže spôsobiť negatívne dopady v celom reťazci, od úniku údajov až po prerušenie poskytovania kľúčových služieb.

Akákoľvek politika, ktorá nebude mať vplyv na diverzifikáciu dodávateľov, **podporu európskej technologickej základne a technologickej suverenity,** či vytváranie mechanizmov na rýchlu reakciu v prípade zistenia zraniteľností, bude mať významný negatívny dopad na EÚ a Slovenskú republiku.

Osobitnou kategóriou tu môžu byť tiež **identifikované závislosti od vysoko rizikových dodávateľov.** To platí aj **pre inovatívne technológie ako PQC a umelá inteligencia**, čo môže pre bezpečnosť celého ekosystému **predstavovať neakceptovateľné riziko**.

Súčasťou riadenia dodávateľského reťazca informačných a komunikačných technológií musí byť tiež apel na koordinovaný systém hodnotenia rizík a na čo najväčšiu transparentnosť, najmä prostredníctvom bezpečnostných certifikácií produktov, požiadaviek na auditovateľnosť a zdieľania informácií o pôvode komponentov.

III. Vnútorné faktory ovplyvňujúce kybernetickú bezpečnosť

Stav kybernetickej bezpečnosti v Slovenskej republike

Predkladaná národná stratégia je v poradí už tretím strategickým dokumentom, ktorého cieľom je dobudovanie a posilňovanie kybernetickej odolnosti Slovenskej republiky. Od prijatia prvej Koncepcie kybernetickej bezpečnosti v roku 2015, ako aj Národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025, vykonala Slovenská republika významné kroky k zlepšeniu úrovne kybernetickej bezpečnosti.

V prvom rade bol vytvorený **právny a inštitucionálny základ** riadenia a regulácie **kybernetickej bezpečnosti na národnej úrovni**. Stabilné právne prostredie stanovuje rozdelenie kompetencií a zodpovednosti.

Hierarchické usporiadanie riadenia kybernetickej bezpečnosti zastrešuje Národný bezpečnostný úrad ako samostatný ústredný orgán štátnej správy pre oblasť kybernetickej bezpečnosti. **Národné centrum kybernetickej bezpečnosti** (ďalej len „NCKB“) ako súčasť Národného bezpečnostného úradu priebežne **posilňuje kapacity svojej národnej jednotky CSIRT (SK-CERT)** v oblasti prevencie a reakcie na závažné kybernetické incidenty na národnej a medzinárodnej úrovni.

Sektor verejnej správy, v zmysle chápania regulácie kybernetickej bezpečnosti, predstavuje významnú oblasť národného kybernetického priestoru. Tento sektor je regulovaný Ministerstvom vnútra Slovenskej republiky (subjekty verejnej správy na úrovni ústredného orgánu štátnej správy a iný štátny orgán s celoštátnou pôsobnosťou a subjekty verejnej správy na regionálnej úrovni okrem oblasti finančnej správy), Ministerstvom financií Slovenskej republiky (subjekty verejnej správy pre oblasť finančnej správy) a Ministerstvom investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (správcovia a prevádzkovatelia informačných systémov verejnej správy). V pôsobnosti Ministerstva investícií, regionálneho rozvoja a informatizácie je zriadená vládna jednotka CSIRT (CSIRT.SK), ktorá pre sektor verejnej správy zabezpečuje tak preventívne opatrenia, ako aj reakciu na kybernetické bezpečnostné incidenty v tomto sektore.

Centrum pre kybernetickú obranu Slovenskej republiky ako osobitná organizačná zložka Vojenského spravodajstva, ktoré je súčasťou Ministerstva obrany Slovenskej republiky, **plní úlohy na úseku kybernetickej obrany,** ale aj sektorovej jednotky CSIRT pre organizácie spadajúce pod rezort obrany.

Neopomenuteľná je aj **oblasť kybernetickej diplomacie**, ktorú koordinuje Ministerstvo zahraničných vecí a európskych záležitostí Slovenskej republiky.

Zárukou efektívneho fungovania tohto ekosystému je vzájomná spolupráca jednotlivých zložiek v rámci zákonmi definovaných kompetencií a úloh.

V Národnej stratégii kybernetickej bezpečnosti na roky 2021 až 2025 boli ako strategické ciele definované

- dôveryhodný štát pripravený na hrozby,
- efektívne odhaľovanie a objasňovanie počítačovej kriminality,
- odolný súkromný sektor,
- kybernetická bezpečnosť ako základná súčasť verejnej správy,
- silné partnerstvá,
- vzdelaní odborníci a vzdelaná verejnosť,
- rozvoj výskumu a vývoja v kybernetickej bezpečnosti.

Analýza plnenia týchto cieľov ukazuje **pokrok v mnohých oblastiach**. Zlepšenia sú badateľné najmä **v legislatívnej oblasti**, **koordinácii a budovaní komunity naprieč verejným a súkromným sektorom, zlepšení reakcie na kybernetické bezpečnostné incidenty** a **zvyšovaní kybernetickej odolnosti prevádzkovateľov základných služieb**.

Stále však pretrvávajú významné rozdiely v úrovni bezpečnosti medzi jednotlivými sektormi, pričom výzvou je najmä zabezpečenie požadovanej úrovne bezpečnosti v sektore verejná správa, zdravotníctvo a školstvo. V týchto sektoroch spôsobuje problém aj nedostatočné finančného krytie nákladov na kybernetickú bezpečnosť. Problém s nedostatkom disponibilných zdrojov na investície čiastočne nahrádzajú grantové programy EÚ, ktoré je však možné čerpať iba na vopred definované účely. Takéto financovanie, zdá sa, nie je systematické. Zároveň pretrváva **problém s ľudskými zdrojmi**, najmä so zamestnávaním špecialistov na kybernetickú bezpečnosť, ktorí nie sú (najmä v sektore verejná správa) dostatočne finančne ohodnotení.

Systém vzdelávania, vedy a výskumu

Vzdelávací systém v oblasti kybernetickej bezpečnosti dnes možno považovať za nie dostatočne vyhovujúci. Systematické budovanie od základných stupňov vzdelávania až po vysokoškolské prostredie je však nesmierne žiaduce a potrebné. **V Slovenskej republike sa problematike kybernetickej bezpečnosti venuje viacero, prevažne vysokých škôl**, avšak chýba jednotný a koordinovaný prístup. Vysoké školy rozvíjajú vzdelávacie programy a výskumné aktivity v tejto oblasti rôznym spôsobom, ale bez komplexného prepojenia, ktoré by zabezpečovalo dlhodobú spoluprácu a synergiu medzi akademickou, verejnou a súkromnou sférou. Budovanie základného povedomia o kybernetickej bezpečnosti musí začať už na základných školách a musí byť rozvíjané na stredných školách.

Vzdelávací systém v súčasnosti v obmedzenej miere zohľadňuje, že kybernetická bezpečnosť nie je výlučne technickým odborom. V rámci tohto sektora bezpečnosti pôsobia odborníci aj z iných, ako iba IT profesií, ako napríklad právnici, projektoví manažéri, procesní analytici, audítori, manažéri kybernetickej bezpečnosti či analytici hrozieb. Napriek tomu **vzdelávacie inštitúcie pomaly vytvárajú programy, ktoré by reflektovali potrebu pracovného trhu**.

Ďalším pretrvávajúcim problémom je **odlev odborníkov a absolventov do zahraničia**. Študenti a absolventi vo zvýšenej miere odchádzajú študovať alebo pracovať mimo Slovenskej republiky, pričom jedným z dôvodov je nízke povedomie o kvalite domáceho vysokoškolského vzdelávania a o potrebách pracovného trhu, ale aj nižšie platové ohodnotenie v porovnaní s niektorými krajinami EÚ. Tento trend vedie k strate odborného potenciálu v oblasti, ktorá už

dnes čelí výraznému nedostatku kvalifikovaných pracovníkov. Počet kvalifikovaných a kvalitných pedagógov v oblasti kybernetickej bezpečnosti je nízky. Je žiaduce v spolupráci s Ministerstvom školstva, výskumu, vývoja a mládeže Slovenskej republiky posilniť koordinované celoživotné vzdelávanie pedagógov v oblasti kybernetickej bezpečnosti, informatizácie a digitalizácie.

Rovnako, **v oblasti výskumu pôsobí len obmedzený počet inštitúcií**, ktoré však napriek tomu zohrávajú významnú úlohu. Väčšina výskumných aktivít prebieha **na fakultách vysokých škôl** a zameriava sa najmä na aktuálne technologické trendy, ako sú umelá inteligencia a PQC. Výskum v oblasti kybernetickej bezpečnosti nie je systémovo financovaný. Inštitúcie sa spoliehajú predovšetkým na externé zdroje, ako sú európske grantové schémy alebo súkromní sponzori. Pre dlhodobú udržateľnosť a rozvoj výskumu je preto nevyhnutné vytvoriť stabilný národný systém financovania a koordinácie vedy a výskumu v oblasti kybernetickej bezpečnosti.

Popri vysokoškolskom vzdelávaní je potrebné venovať pozornosť aj **stredným odborným školám alebo gymnáziám**, ktoré môžu pripraviť kvalifikovaných pracovníkov pre niektoré typy profesií už na tejto úrovni. Rozšírenie odborných programov alebo dopĺňanie odborných predmetov by mohlo prispieť k **rýchlejšiemu dopĺňaniu pracovných síl** na základe potrieb pracovného trhu v oblasti kybernetickej bezpečnosti.

Podobne dôležité je aj **posilnenie inovačného prostredia**. V Slovenskej republike pôsobí len obmedzený počet startupov zameraných výlučne na kybernetickú bezpečnosť alebo na vývoj riešení v oblasti umelej inteligencie. **Absolventi vysokých škôl a odborníci uprednostňujú zamestnanie** v súkromnej sfére prípadne vo verejnom sektore **pred zakladaním vlastných inovačných projektov** – *startupov*. Tento stav je spôsobený absenciou motivačného systému založeného na systéme podpory podnikania ale tiež, napríklad, budovania špecializovaných inkubátorov a inovačných *hubov*. Tie by mali fungovať nielen ako fyzické priestory, ale aj ako platformy poskytujúce školenia, workshopy, financovanie a grantovú podporu. Vytvorenie takýchto centier by významne prispelo k rozvoju inovatívneho prostredia a posilnilo by celkové kapacity Slovenskej republiky v oblasti kybernetickej bezpečnosti.

IV. Východiská

Strategicko-politický rámec

Strategické dokumenty napriek svojej legislatívne nezáväznej povahe významne ovplyvňujú tvorbu politík a súčasne poskytujú základný rámec potrebný na určenie priorít kybernetickej bezpečnosti, predvídanie budúcich trendov, ale aj regulačných požiadaviek. Tieto dokumenty vznikajú na globálnej, európskej a národnej úrovni a napriek tomu, že sú vytvárané jednotlivo, často sa prelínajú a dopĺňajú, čo prispieva k vytváraniu koordinovaného prístupu ku kybernetickej bezpečnosti. V kontexte kybernetickej bezpečnosti je dôležitá najmä Stratégia kybernetickej bezpečnosti EÚ pre digitálne desaťročie a Strategický kompas pre bezpečnosť a obranu ako aj neverejné spravodajsko-operatívne materiály z dielne Európskej služby pre vonkajšiu činnosť (ďalej len „EEAS“).

Stratégia kybernetickej bezpečnosti EÚ pre digitálnu dekádu predstavuje prístup EÚ k budovaniu bezpečného a odolného digitálneho prostredia. Do popredia dáva najmä **odolnosť kritickej infraštruktúry**, rozvoj technológií a kapacít a schopnosť predchádzať, detegovať a reagovať na kybernetické bezpečnostné incidenty väčšieho rozsahu. Stratégia tiež kladie dôraz na **dosahovanie technologickej suverenity** a prehlbovanie spolupráce medzi členskými štátmi a inštitúciami, čím upevňuje postavenie EÚ ako globálneho aktéra v regulácii zodpovedného správania sa štátov v kybernetickom priestore. Predmetné požiadavky ďalej vo svojej pôsobnosti rozpracováva ***Stratégia odolnosti kritických subjektov Slovenskej republiky*** schválená uznesením vlády Slovenskej republiky č. 3 z 09.01.2026.

Strategický kompas pre bezpečnosť a obranu je jedným z najucelenejších súčasných dokumentov bezpečnostnej a obrannej politiky EÚ, predstavuje dosiahnuteľné ciele do roku 2030. **Kybernetický priestor považuje za strategicky dôležitú doménu**, v rámci ktorej definuje viacero konkrétnych odporúčaní, najmä čo sa týka zvyšovania kapacít či posilňovania spolupráce v témach, ako je **spoločné situačné povedomie a rýchla reakcia na kybernetické bezpečnostné incidenty**. Napriek tomu, že oba dokumenty majú vo svojej povahe prevažne politický charakter, zohrávajú významnú úlohu v smerovaní národných kyberbezpečnostných politík.

Záväzný právny rámec

Na rozdiel od strategických dokumentov, ktoré predstavujú politické smerovanie a stanovujú dlhodobé priority, **právne akty EÚ definujú špecifické požiadavky pre národné autority, kritické sektory, digitálne produkty či vznikajúce technológie**. Plnohodnotné vykonávanie týchto aktov je nevyhnutné nielen z hľadiska právneho súladu, ale aj koordinovaného postupu pri zvyšovaní kybernetickej odolnosti v rámci EÚ.

Národná stratégia preto priamo zohľadňuje povinnosti vyplývajúce z kľúčových právnych aktov, a to:

- *Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (**akt o kybernetickej bezpečnosti**) v platnom znení*

- *Nariadenie Európskeho parlamentu a Rady (EÚ) 2021/694 z 29. apríla 2021, ktorým sa zriaďuje **program Digitálna Európa** a zrušuje rozhodnutie (EÚ) 2015/2240 v platnom znení*

- *Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (**akt o umelej inteligencii**)*

- *Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 z 23. októbra 2024 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadení (EÚ) č. 168/2013 a (EÚ) 2019/1020 a smernice (EÚ) 2020/1828 (**akt o kybernetickej odolnosti**)*

Akt o kybernetickej odolnosti predstavuje európsku legislatívu zameriavajúcu sa na zvýšenie úrovne bezpečnosti všetkých produktov, ktoré obsahujú digitálne prvky, s výnimkou produktov, pokrytých inými EÚ predpismi, ako napríklad zdravotnícke pomôcky, automobily a podobne. Legislatíva sa týka hardvéru aj softvéru. Implementácia aktu o kybernetickej odolnosti do slovenského právneho poriadku bude realizovaná novým zákonom v oblasti kybernetickej odolnosti, ako aj novelizáciou zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a zákona č. 56/2018 Z. z. o posudzovaní zhody výrobku, sprístupňovaní určeného výrobku na trhu a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Praktická implementácia opatrení povedie k posilneniu kybernetickej bezpečnosti, keďže produkty s digitálnymi prvkami budú môcť byť uvedené na trh iba po odstránení všetkých známych zneužiteľných zraniteľností. Výrobca týchto produktov je povinný počas vývoja a celého predpokladaného životného cyklu produktu zaručiť rovnakú úroveň kybernetickej odolnosti. Zároveň je vyžadované, aby boli produkty s digitálnymi prvkami dodávané v nastavení, ktoré znižuje riziko zraniteľností z nesprávnej konfigurácie. Regulácia je navrhnutá v súlade s konceptom *„security by design“* a *„security by default“*.

- *Nariadenie Európskeho parlamentu a Rady (EÚ) 2025/38 z 19. decembra 2024, ktorým sa stanovujú opatrenia na posilnenie solidarity a kapacít v Únii na odhaľovanie kybernetických hrozieb a incidentov, prípravu a reakciu na ne a ktorým sa mení nariadenie (EÚ) 2021/694 (**akt o kybernetickej solidarite**)*

- *Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti*

*v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (**smernica NIS 2**)*

Smernica NIS 2 predstavuje základný právny rámec pre harmonizáciu opatrení a nástrojov kybernetickej bezpečnosti s cieľom posilňovať kybernetickú odolnosť a bezpečnosť v širšom kontexte európskej integrácie a globálnych hrozieb.

V rámci smernice NIS 2 sa rozšíril rozsah sektorov a subjektov, ktoré sa z hľadiska zabezpečenia vysokej kybernetickej odolnosti považujú za kritické alebo dôležité, upravili a spresnili postupy hlásenia kybernetických bezpečnostných incidentov, definície významnej kybernetickej hrozby, udalosti odvrátenej v poslednej chvíli a zraniteľností, ako aj procesy riešenia incidentov. Význam smernice je aj v tom, že definuje rámec strategického plánovania na národnej úrovni, riešenia a zdolávania rozsiahlych kybernetických incidentov a kybernetických kríz. Smernica tiež posilňuje medzinárodnú spolupráci vytvorení európskej siete jednotiek CSIRT a Európskej siete styčných organizácií pre kybernetické krízy (EU-CyCLONe).

- *Smernica Európskeho parlamentu a Rady (EÚ) 2022/2557 zo 14. decembra 2022 o odolnosti kritických subjektov a o zrušení smernice Rady 2008/114/ES (**smernica CER)***

Smernica CER vytvára nový rámec pre posilnenie odolnosti kritických subjektov voči fyzickým, technickým, ale aj prírodným hrozbám. Smernica CER bola do právneho poriadku Slovenskej republiky transponovaná zákonom č. 367/2024 Z. z. o kritickej infraštruktúre a o zmene a doplnení niektorých zákonov (ďalej len „zákon o kritickej infraštruktúre“), pričom tento obsahuje opatrenia na zníženie zraniteľnosti a posilnenie odolnosti kritických subjektov, ktoré prevádzkujú kritickú infraštruktúru. Zámerom je zabezpečiť kontinuálne poskytovanie základných služieb, ktoré sú kľúčové pre zachovanie základných spoločenských funkcií a hospodárskych činností štátu. Transpozícia do slovenskej legislatívy spôsobila reorganizáciu kompetencií orgánov štátnej správy na úseku kritickej infraštruktúry, zaviedli sa nové postupy pre identifikáciu kritických subjektov, ako aj povinnosti prevádzkovateľov týchto subjektov, taktiež zaviedla požiadavky na vypracovanie analýzy rizík, bezpečnostných plánov a hlásenie incidentov, pričom dôraz je kladený na výmenu informácií medzi Ministerstvom vnútra Slovenskej republiky ako ústredným koordinačným orgánom, štátnymi orgánmi a súkromným sektorom.

Tieto právne akty EÚ predstavujú základné regulačné východiská pre oblasť kybernetickej bezpečnosti v Slovenskej republike a definujú jasné pravidlá a nástroje na napĺňanie cieľov národnej stratégie.

V Slovenskej republike je základný právny rámec kybernetickej bezpečnosti tvorený **zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti** a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony (ďalej len „zákon o kybernetickej bezpečnosti“). Zákonom č. 366/2024 Z. z., ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých

zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony, sa **do právneho poriadku s účinnosťou od 1. januára 2025 úspešne transponovala smernica NIS 2**.

Zákon o kybernetickej bezpečnosti v novej podobe **je tak právnym základom na vypracovanie novej národnej stratégie**. Národná stratégia zohľadňuje požiadavky ustanovení § 7 zákona o kybernetickej bezpečnosti tým, že **poskytuje jasne stanovené ciele a priority** v oblasti kybernetickej bezpečnosti. **Národná stratégia spolu s akčným plánom**, ktorý bude na ňu nadväzovať, **zadefinuje mechanizmy na identifikáciu relevantných nástrojov** a hodnotenie rizík, opatrenia na zabezpečenie pripravenosti, schopnosti reakcie na kybernetické hrozby a kybernetické bezpečnostné incidenty, ako aj následnej obnovy. Národná stratégia sa rovnako venuje aj zvyšovaniu všeobecnej úrovne informovanosti občanov a spoločnosti v otázkach kybernetickej bezpečnosti. Zároveň podporuje spoluprácu medzi verejným sektorom a súkromným sektorom.

V. Vízia národnej stratégie

Cieľom každého členského štátu EÚ je **stať sa bezpečným a dôveryhodným digitálnym štátom** podporujúcim rozvoj a **bezpečné využívanie inovatívnych technológií**.

V súlade s európskymi hodnotami budú presadzované princípy právneho štátu, ochrany základných práv a slobôd a zabezpečenie dostupnosti, otvorenosti a bezpečnosti internetu. Dôležitá bude aj podpora iniciatív smerujúcich k vytvoreniu otvoreného, plne demokratického a pravidlami riadeného kybernetického prostredia, ktoré rešpektuje medzinárodné normy a zásady proporcionality a zodpovednosti. Súčasťou plnenia národnej stratégie teda musí byť aj **systematická integrácia kybernetickej bezpečnosti do digitálnej transformácie Slovenskej republiky**.

V oblasti technologickej suverenity je dôležité klásť dôraz na **rozvoj domáceho výskumu a vývoja v oblasti kybernetickej bezpečnosti**. Podpora domácich startupov, tvorba inovačných ekosystémov a využívanie národných talentov sú spôsoby, ako znížiť závislosť na zahraničných dodávateľoch a **zvyšovať digitálnu suverenitu**. Táto suverenita je zároveň hnacou silou inovácií, investície do výskumu, testovacích prostredí a verejno-súkromných partnerstiev umožnia rýchle nasadzovanie nových riešení, ktoré zvyšujú kvalitu služieb a podporujú hospodársky rast.

Budovanie technologickej suverenity by malo byť založené na princípe technologickej neutrality. Slovenská republika zároveň musí vytvoriť systém podpory, ktorý bude motivovať výskum a vývoj informačných technológií, služieb a nástrojov kybernetickej bezpečnosti alebo podporovať účasť na vývojových projektoch a procesoch v rámci Európskej únie. Zároveň musí podporiť nasadzovania takto vyvinutých technológií v slovenskom kybernetickom priestore. Systém podpory a motivácie musí prevažovať nad akýmikoľvek reštriktívnymi nástrojmi, ktoré by mohli spôsobiť izoláciu Slovenskej republiky od globálneho technologického pokroku alebo narušenie otvoreného trhu.

Významným prvkom budovania dôvery je **posilňovanie strategickej komunikácie a spoločenskej odolnosti voči dezinformačným operáciám**. Zvýšenie mediálnej a digitálnej gramotnosti občanov, transparentná komunikácia o bezpečnostných rizikách, kooperácia štátu so súkromnými spoločnosťami prispievajú k dôvere obyvateľstva v digitalizáciu. Práve dôvera používateľov je kľúčovým predpokladom používania digitálnych služieb, preto je nevyhnutné zvyšovať transparentnosť poskytovateľov digitálnych riešení, posilňovať ich zodpovednosť za nastavené bezpečnostné opatrenia a súčasne **zlepšovať povedomie občanov** o ich úlohe **v prevencii kybernetických hrozieb**. Digitálne prostredie, v ktorom občania a organizácie s dôverou využívajú online nástroje prispieva k prosperite štátu ako celku.

Rastúca komplexnosť digitálneho prostredia a narastajúce **kybernetické hrozby vyžadujú inovatívne prístupy k ochrane údajov, systémov a infraštruktúry**. Inovácie v oblasti kybernetickej bezpečnosti sú kľúčom k udržateľnej odolnosti voči kybernetickým hrozbám a zároveň predstavujú strategickú príležitosť pre rozvoj znalostnej ekonomiky. Tento cieľ podporuje vytváranie priaznivého prostredia pre výskum, vývoj a implementáciu moderných bezpečnostných technológií a zároveň posilňuje synergie medzi štátom, akademickou obcou a súkromným sektorom.

VI. Strategické piliere a ciele

Pilier 1: Ochrana národného kybernetického priestoru

Cieľ 1.1: Ochrana občanov, malých a stredných podnikateľov a podnikov

Východiskový stav

Podpora budovania bezpečnostného povedomia zo strany štátu nie je v súčasnosti dostatočne systematická a zjednotená, pričom reakcia na kybernetické hrozby často nastáva až v prípade vzniku kybernetického bezpečnostného incidentu. Malé a stredné podniky nie vždy kybernetickú bezpečnosť vnímajú ako súčasť ich zodpovedného podnikania a berú ju skôr ako dodatočnú finančnú záťaž, ktorej venujú obmedzené zdroje. V dôsledku toho ostávajú zraniteľné voči rôznym typom kybernetických hrozieb.

Cieľový stav

Cieľom je vytvoriť bezpečné prostredie a zároveň rozvíjať digitálne služby tak, aby boli vnímané ako prirodzená súčasť každodenného života občanov aj podnikateľov.

Odolnosť populácie, podnikateľov a podnikov voči škodlivým aktivitám v kybernetickom priestore **vzrastie** a miera úspešnosti kybernetických útokov klesne.

Štát zohráva aktívnu rolu v **budovaní povedomia o kybernetických rizikách** a zároveň **poskytuje jednoduché návody na ochranu** pred nimi. Zároveň podporuje vytváranie a **dostupnosti nástrojov na ochranu pred kybernetickými hrozbami**, ktoré nevyžadujú vysokú technickú zdatnosť.

Súčasťou **prevencie** sú znalosti, metódy a prostriedky na identifikáciu a ochranu **pred škodlivými aktivitami a falošnými informáciami vytváranými technológiami umelej inteligencie**, ktorých rozpoznávanie je čoraz ťažšie.

Štát podporuje **kybernetickú bezpečnostnú komunitu**, v rámci ktorej sa realizuje **zdieľanie informácií a znalostí a spolupráca** medzi občianskou spoločnosťou, podnikateľským prostredím a štátom samotným samozrejmosťou. Súčasťou tohto systému bude podpora účasti komunitných centier, stavovských a záujmových organizácií a iných mimovládnych organizácií na organizácii vzdelávacích programov, workshopov a vytváraní kompetenčných a podporných centier. Tým sa štát stane nielen rešpektovanou autoritou ale aj uznávaným partnerom.

Cieľ 1.2: Kybernetická odolnosť prevádzkovateľov základných služieb

Východiskový stav

Prevádzkovateľmi základných služieb nie sú iba štátne orgány a orgány verejnej moci, ale v prevažnej miere súkromné podniky. V mnohých organizáciách možno pozorovať postupný rast úrovne kybernetickej bezpečnosti, avšak stále existujú prípady, kde bezpečnosť nedosahuje ani základné požadované štandardy. Miera zabezpečenia kybernetickej ochrany závisí predovšetkým od prístupu a vôle vedenia jednotlivých prevádzkovateľov základných služieb.

Cieľový stav

Bezpečnostné štandardy sú na úrovni štátu definované a systematicky zavádzané na základe **odborne vykonanej analýzy rizík štátu a prevádzkovateľov základných služieb**. Prevádzkovatelia základných služieb ich implementujú a rozvíjajú vo svojich plánoch kontinuity činností v súlade s centrálne určenou metodikou a vlastnou analýzou rizík s dôrazom na posilnenie kybernetickej bezpečnosti a zabezpečenie kybernetickej odolnosti.

Vysoko kritické alebo technologicky špecifické sektory rovnako efektívne implementujú aj **osobitné bezpečnostné štandardy** vychádzajúce z legislatívy a dobrej praxe v danom priemysle.

Štát metodicky podporuje a aktívne dohliada na plnenie povinností zo strany prevádzkovateľov základných služieb.

Účinnosť bezpečnostných mechanizmov, ako aj opatrení na zmiernenie dopadov incidentov, **je pravidelne overovaná a prispôsobovaná aktuálnym kybernetickým hrozbám** prostredníctvom pravidelného vykonávania testov, auditov a revízií.

Systém kybernetickej bezpečnosti **interaguje s odolnosťou kritickej infraštruktúry** vrátane identifikovaných závislostí medzi jednotlivými sektormi a organizáciami, príčinnými súvislosťami dopadov závažných kybernetických bezpečnostných incidentov ako aj integrovanej reakcie na závažné a rozsiahle kybernetické bezpečnostné incidenty postihujúce kritické subjekty.

Štát aktívne **podporuje nasadzovanie takých produktov a služieb** v rámci informačno-komunikačných technológií a operačných technológií do infraštruktúry organizácií a podnikov, ktoré zaručujú **vysokú kybernetickú odolnosť**, a to predovšetkým **produktov s bezpečnostnou certifikáciou**, **kryptografické prostriedky odolné voči známym PQC hrozbám a podobne**.

Zároveň štát dohliada na **zodpovedné nasadzovanie** technológií, ktoré môžu vnášať nové bezpečnostné riziká do infraštruktúry informačných a komunikačných technológií a operačných technológií podnikov, **najmä umelú inteligenciu** a **siete pripojených objektov a zariadení** *(angl. Internet of Things)*.

Cieľ 1.3: Bezpečnosť dodávateľských reťazcov

Východiskový stav

Budovanie spoľahlivého a odolného dodávateľského reťazca je podceňované a pozostáva iba na zmluvnom základe bez vynucovania dodatočných opatrení. Podniky, ktoré sú súčasťou dodávateľských reťazcov, sú čoraz častejšie cieľom útokov, čo je spôsobené absenciou systematického riadenia rizík a menej efektívnym zavádzaním bezpečnostných opatrení. Na úrovni EÚ bol vytvorený *Súbor nástrojov pre bezpečnosť dodávateľského reťazca služieb, systémov alebo produktov informačných a komunikačných technológií*, ktorý definuje koncepty bezpečnosti dodávateľského reťazca informačno-komunikačných technológií, identifikuje potenciálne rizikové scenáre a poskytuje odporúčania na adresovanie a minimalizáciu rizík. Poskytuje spoločný štrukturalizovaný nezáväzný prístup k zabezpečeniu dodávateľského reťazca informačných a komunikačných technológií a všeobecný rámec na vykonávanie analýzy rizík kritických dodávateľských reťazcoch.

Cieľový stav

Štát zabezpečí implementáciu jednotného európskeho rámca pre analýzu a minimalizovanie rizík, ktorý umožňuje spoločný a **štruktúrovaný prístup k bezpečnosti dodávateľských reťazcov** produktov a služieb informačných a komunikačných technológií.

V rámci európskeho strategického smerovania štát **posilňuje spoločnú technologickú a strategickú autonómiu** prostredníctvom **diverzifikácie partnerov** a **znižovaním závislosti od rizikových dodávateľov**. Tento proces je úzko previazaný s cieľom budovať **bezpečné, transparentné a odolné dodávateľské reťazce**, ktoré podporia digitálnu suverenitu a dôveryhodnosť národného technologického prostredia.

Riziká vyplývajúce z dodávateľských reťazcov budú poskytovateľmi kritických základných služieb **pravidelne posudzované** a minimalizované. Vysokorizikoví dodávatelia systémov informačných a komunikačných technológií môžu byť vylúčení z prevádzky základných a dôležitých služieb či kritickej infraštruktúry.

Zavedený je rámec auditovania dodávateľských reťazcov pre kritické sektory.

Diverzifikované a transparentné dodávateľské reťazce budú zvyšovať odolnosť a zabezpečovať kontinuálne fungovanie prevádzkovateľov kritických základných služieb.

Pilier 2: Budovanie národných kapacít v oblasti kybernetickej bezpečnosti

Cieľ 2.1: Integrovaná architektúra riadenia kybernetickej bezpečnosti

Východiskový stav

S rastúcou komplexnosťou kybernetických hrozieb je nevyhnutné vybudovať integrovanú architektúru kybernetickej bezpečnosti. Táto architektúra zabezpečí komplexnú ochranu informačných systémov, efektívnu koordináciu a rýchlu reakciu na kybernetické bezpečnostné incidenty. Cieľom je centralizovaný prístup pod vedením Národného bezpečnostného úradu a vybudovanie systému situačného povedomia, ktorý umožní včasnú detekciu a znižovanie kybernetických hrozieb.

Informačné systémy a digitálne služby sú v súčasnosti fragmentované, s rôznymi úrovňami zabezpečenia a obmedzenou koordináciou medzi sektormi. Nielen kybernetická bezpečnosť, ale aj úroveň digitalizácie a s ňou súvisiaca informačná architektúra trpí na silne decentralizovaný prístup jednotlivých zodpovedných orgánov a organizácii. Hoci Národný bezpečnostný úrad plní koordinačnú úlohu, na národnej úrovni absentuje jednotný systém situačného povedomia a štandardizované krízové postupy. Zodpovednosť sektorových orgánov je často obmedzená a koordinácia má prevažne neformálny charakter, čo znižuje efektivitu reakcie na kybernetické bezpečnostné incidenty a kybernetické hrozby na národnej úrovni.

Procesy riadenia zraniteľností vo verejnej správe, ale i v niektorých iných subjektoch, nie sú zavedené vôbec, alebo sú zavedené neefektívne. Mnohé subjekty reflektujú na zraniteľnosti až v reakcii na kybernetický bezpečnostný incident, čo zvyšuje pravdepodobnosť narušenia poskytovania služieb alebo k úniku údajov. Prevádzkovatelia základných služieb často nemajú prehľad o aktuálnych zraniteľnostiach v používaných informačných technológiách, ani o dostupných mechanizmoch na ich preverovanie a odstraňovanie.

Cieľový stav

Riadenie kybernetickej bezpečnosti na národnej úrovni je integrované a systematicky koordinované tak, aby jednotlivé subjekty a zložky a ich činnosti vzájomne vytvárali **funkčný systém odolný voči komplexným kybernetickým hrozbám**. Zodpovednosť za kybernetickú bezpečnosť je zmysluplne distribuovaná medzi **Národný bezpečnostný úrad, ako národnú autoritu a hlavného garanta kybernetickej bezpečnosti v Slovenskej republike** a ústredné orgány štátnej správy, či už v pozícií sektorových autorít alebo špecifických orgánov zodpovedných za kybernetickú diplomaciu, kybernetickú obranu alebo za boj proti kybernetickej kriminalite.

Národný bezpečnostný úrad vydáva **metodiky a stanoviská** k aplikácii všeobecne záväzných právnych predpisov a nelegislatívnych dokumentov na úseku kybernetickej bezpečnosti.

Ústredné orgány disponujú **dostatočnou ľudskou, odbornou, finančnou a technickou spôsobilosťou vykonávať svoje úlohy**, tak aby kybernetická odolnosť zvereného sektora alebo plnenie zverených úloh bolo kontinuálne zlepšované.

Sú jasne stanovené a ohraničené kompetencie jednotlivých orgánov, pričom sú zároveň medzi nimi zavedené **transparentné procesy na vzájomnú spoluprácu** a komunikáciu. Tieto medzirezortné procesy zabezpečia **efektívne výstupy a postupy** od tvorby pravidiel a legislatívy, cez reakciu na kybernetické bezpečnostné incidenty až po krízové riadenie.

Vo verejnom sektore je vybudovaná optimalizovaná a integrovaná architektúra kybernetickej bezpečnosti založená na efektívne riadenej IT architektúre.

Systém detekcie kybernetických hrozieb a kybernetických bezpečnostných incidentov zabezpečuje **včasnú detekciu kybernetických hrozieb naprieč celým kybernetickým priestorom** v Slovenskej republike a tým zlepšuje situačné povedomie. Zvyšuje sa **včasnosť a adresnosť varovania relevantných subjektov**.

Je **akceptovaný** a zavedený prehľadný **systém plnenia úloh a zodpovedností všetkých zainteresovaných jednotiek CSIRT pri preventívnych a reaktívnych službách**, pričom je **dodržiavaný** Národným bezpečnostným úradom určený **postup pri eskalácii** kybernetických hrozieb a kybernetických bezpečnostných incidentov.

Riadenie zraniteľností je bežnou súčasťou prevádzky sietí, informačných systémov a prevádzkových technológií. Zisťovanie zraniteľností je vykonávané pravidelne a preventívne. Prevádzkovatelia základných služieb majú **prehľad o dostupných riešeniach** a aktívne využívajú podporu jednotiek CSIRT pri ich odhaľovaní a odstraňovaní zraniteľností, ako aj pri overovaní bezpečnostnej úrovne svojich systémov, čím sa zvyšuje kybernetická odolnosť štátu a znižujú sa dopady potenciálnych kybernetických bezpečnostných incidentov.

Cieľ 2.2: Efektívne zavádzanie bezpečnostných technológií a procesov

Východiskový stav

Využívanie inovatívnych technológií je na národnej úrovni stále v počiatočnej fáze. Ústredné orgány štátu v oblasti kybernetickej bezpečnosti začínajú pri svojej činnosti využívať modely umelej inteligencie a to predovšetkým v rámci analýz veľkého množstva údajov, spracúvanie reportov, prípadne aj v rámci detekčných činností. Využívanie výhod umelej inteligencie v týchto oblastiach je iba v začiatkoch. Organizácie si neuvedomujú riziká a zavádzaním nových technológií vytvárajú nové zraniteľnosti ale aj priamo incidentné stavy. Na organizačnej úrovni neexistujú interné metodiky na bezpečnú prácu s umelou inteligenciou.

Cieľový stav

Ústredné orgány štátnej správy, prevádzkovatelia základných služieb, jednotky CSIRT a iné relevantné subjekty sú schopné **využívať modely a nástroje založené na umelej inteligencii** pri zlepšovaní svojej informačnej infraštruktúry a procesov, a to aj **v rámci bezpečnostných technológií.** Tieto nástroje sú využívané nielen ako **automatizované detekčné nástroje na rýchlu identifikáciu kybernetických hrozieb**, kybernetických

bezpečnostných **incidentov,** ale aj na rýchle vyhľadávanie a **analýzu relevantných informácií z otvorených zdrojov**, analýzu veľkého množstva údajov napríklad **pri forenzných analýzach ako aj pri simuláciách**.

Bezpečnostné dohľadové centrá sa budú pri budovaní aktuálneho situačného povedomia spoliehať na **technológie a mechanizmy** zabezpečujúce nepretržitú a **včasnú detekciu incidentných stavov**, výmenu a **analýzu údajov o hrozbách**, meranie ich výskytu a proaktívne všeobecné alebo adresné varovanie pred nimi. Celkové **situačné povedomie** na národnej úrovni bude **zabezpečené automatizovanými nástrojmi vrátane využitia prostriedkov umelej inteligencie** a efektívnymi procesmi, tak aby reakcia na hrozby a incidenty bola okamžitá a adekvátna.

Cieľ 2.3: Reakcia na kybernetické bezpečnostné incidenty, kybernetické krízy a spolupráca s justičnými orgánmi

Východiskový stav

Efektívna reakcia na kybernetické bezpečnostné incidenty je základom funkčného systému kybernetickej bezpečnosti. Systém reakcie na kybernetické bezpečnostné incidenty je na národnej úrovni funkčný, avšak má nedostatky v rámci koordinácie medzi jednotkami CSIRT a národnou jednotkou CSIRT (SK-CERT). Kapacity jednotiek CSIRT nie sú dostatočné, detekcia, hlásenie a riešenie kybernetických bezpečnostných incidentov je často závislá len na konkrétnych situáciách a individuálnych rozhodnutiach. Nie sú interne zavedené manuály vzhľadom na závažnosť alebo rozsah kybernetického bezpečnostného incidentu. Proces riešenia kybernetických bezpečnostných incidentov je v dôsledku organizačných, technických a ľudských faktorov zdĺhavý. Policajný zbor a justičné orgány nie sú prispôsobené a vybavené na efektívne odhaľovanie a vyšetrovanie kybernetickej kriminality. Pretrvávajú rozdiely v postupoch pri získavaní a zaisťovaní digitálnych dôkazov, čo je spôsobené faktormi ako sú rôzna vnútroštátna právna úprava, technologická zložitosť, problém teritoriality, komplikovaná jurisdikcia, nejednotnosť celoeurópskych štandardov pre nástroje a metodiky používané k získaniu, zaisteniu, analýze a uchovávaniu digitálnych dôkazov a nedostatok špecializovaných školení pre Policajný zbor a justičné orgány. Policajný zbor a prokuratúra čelia nedostatku odborníkov, technických prostriedkov a znalostí na vyšetrovanie počítačových trestných činov. Cvičenia na simuláciu útokov a reakcií na ne sú organizované v nedostatočnej frekvencii a implementáciu záverov cvičení nemožno overiť, čo znižuje pripravenosť na krízové situácie. S rozvojom informačných a komunikačných technológií bol zaznamenaný nárast intolerancie aj v kybernetickom priestore. Zraniteľnou skupinou sú primárne deti, ktoré sú často vystavené dezinformáciám a kybernetickým hrozbám.

Cieľový stav

Tento cieľ podporuje rozvoj kapacít jednotiek CSIRT, bezpečnostných zložiek a zavedenie pravidelných cvičení na zvýšenie pripravenosti a je zavedené vzdelávanie v oblasti kyberšikany.

Integrovaný systém reakcie na kybernetické bezpečnostné incidenty (tzv. „národný blueprint“) zahŕňa národnú jednotku CSIRT (SK-CERT) a siete sektorových a iných jednotiek

CSIRT, ktoré pokrývajú orgány verejnej moci a iné dôležité sektory. Na koordinované postupy pri riešení závažných kybernetických bezpečnostných incidentov sa využívajú funkcionality jednotného informačného systému kybernetickej bezpečnosti. Pre **zdolávanie rozsiahlych kybernetických bezpečnostných incidentov a kybernetických kríz sú definované jasné postupy** a kompetencie jednotlivých zložiek, čím sa zabezpečuje rýchla a koordinovaná reakcia. Tieto postupy sú pravidelne preskúšavané. Národný blueprint bude zároveň prepojený s európskym mechanizmom na riadenie kybernetických kríz (tzv. blueprint EÚ).

Prevádzkovatelia kritických základných služieb sú dostatočne **pripravení na riešenie závažných kybernetických incidentov**. Spôsobilosť reakcie na kybernetické bezpečnostné incidenty je posilnená tak, že včasná intervencia zabraňuje rozsiahlejším dopadom.

Spolupráca **Policajného zboru, prokuratúry a justičných orgánov** zabezpečuje **efektívne odhaľovanie a vyšetrovanie kybernetickej kriminality** s cieľom vyvodiť trestnoprávnu zodpovednosť jej páchateľov, vrátane boja proti kyberterorizmu a kyberšpionáži. Justičné orgány pre efektívne vyšetrovanie kybernetickej kriminality **využívajú vytvorené znalecké útvary, odborníkov a znalcov.** Zároveň **efektívne komunikujú a kooperujú s justičnými orgánmi iných krajín** v rámci EÚ, ale aj mimo EÚ.

V oblasti boja proti kybernetickej kriminalite sú zavedené **zmeny** v národnom právnom rámci, **ktoré umožňujú vyvodzovať trestnoprávnu zodpovednosť** v súvislosti s hrozbami **kyberterorizmu alebo kyberšpionáže** aj na základe zabezpečených **elektronických dôkazov**. Je zavedený účinný systém stíhania najzávažnejších foriem kybernetickej kriminality a zároveň je poskytnutá primeraná právna ochrana osobám vykonávajúcim vyšetrovanie, pričom informácie a dôkazy získané počas vyšetrovania sú chránené pred zneužitím.

Policajný zbor má personálne **posilnené špecializované útvary** na boj proti trestným činom spáchaným v kyberpriestore. V digitálnom rozmere má štát **posilnenú aj ochranu** duševného vlastníctva a ochranu **pred priemyselnou a technologickou špionážou**, najmä v oblasti nových a prelomových technológií, no najmä tých, ktoré majú uplatnenie na úseku národnej bezpečnosti a pri obrane štátu.

Je zavedené vzdelávanie žiakov, pedagógov, výchovných poradcov, ďalších spolupracujúcich odborníkov, nepedagogických zamestnancov a rodičov v problematike **dezinformácií, kybernetických hrozieb a ich prevencie**.

Rýchla reakcia na kybernetické bezpečnostné incidenty, efektívne a razantné vyvodenie zodpovednosti aktérov hrozieb v trestnoprávnej alebo diplomatickej rovine musia pôsobiť tak, aby znižovali motiváciu vykonávať škodlivé aktivity alebo páchať kybernetickú kriminalitu.

Pilier 3: Bezpečné a inovatívne digitálne produkty a služby

Cieľ 3.1: Zabezpečenie kybernetickej bezpečnosti v celom životnom cykle digitálnych produktov a služieb

Východiskový stav

Kybernetická bezpečnosť je vnímaná ako dodatočný prvok, nie ako integrálna súčasť vývoja a správy digitálnych riešení. V dnešnom stave neodzrkadľuje v plnohodnotnej miere technologické trendy, najmä nasadzovanie a využívanie modelov umelej inteligencie.

Cieľový stav

Tento cieľ si kladie za úlohu vytvoriť regulačné, procesné a technické podmienky, ktoré zabezpečia, aby produkty a služby boli bezpečné už od svojho vzniku a po celý čas ich životnosti.

Rozvoj technologických firiem je kľúčový pre budovanie vyspelej ekonomiky a digitálnej suverenity. Systém priamej a nepriamej podpory, regulácie a bezpečnostnej certifikácie je nastavený tak, aby technologické firmy sú konkurencie schopné a motivované **vyvíjať a poskytovať moderné a vysoko bezpečné digitálna produkty a služby**. Tieto sú navrhované v súlade s princípmi ***„security-by-design“*** a ***„privacy-by-design“***. Všetky fázy ich životného cyklu zahŕňajú **bezpečnostné požiadavky ako základné vlastnosti produktu** alebo služby. Vhodne zvolená metodika riadenia rizík reflektuje aj zavádzanie umelej inteligencie do digitálnych produktov a služieb, identifikuje a posudzuje nové riziká s tým súvisiace (napr. modelovanie kybernetických hrozieb).

Digitálne produkty a služby sú vyvíjané a uvádzané na trh **v súlade s požiadavkami aktu o kybernetickej odolnosti, aktu o umelej inteligencii a ďalšími legislatívnymi požiadavkami**. Ich výrobcovia a poskytovatelia počas celého životného cyklu uplatňujú požiadavky na primeranú bezpečnosť, dodržiavajú zásady bezpečného vývoja, vedú a zdieľajú softvérový súpis materiálov (SBOM, *angl. Software Bill of Materials*), vykonávajú bezpečnostné testovanie, prevádzkujú procesy efektívneho odhaľovania a odstraňovania zraniteľností a plnia oznamovacie povinnosti.

Procesy odhaľovania a **zodpovedného oznamovania zraniteľností** sú jasne definované a efektívne zavedené do praxe. Znižuje sa rizikovosť nielen sietí a informačných systémov, ale aj digitálnych produktov. Digitálne produkty, postavené na **technológiách umelej inteligencie**, spĺňajú regulačné požiadavky ako aj **etické a bezpečnostné štandardy uznávané v priemysle**.

Cieľ 3.2: Zavádzanie bezpečných digitálnych produktov, služieb a inovácií

Východiskový stav

Výber platforiem a softvéru často prebieha bez dôkladného zohľadnenia rizík, zraniteľnosti sa odhaľujú až po nasadení a zložitosť prepojených systémov sťažuje ucelené analýzy rizík. V prostredí EÚ zároveň nadobúdajú účinnosť horizontálne pravidlá pre digitálne produkty a systémy (akt o kybernetickej odolnosti, akt o umelej inteligencii), ktoré zavádzajú povinnosti v bezpečnom vývoji, správe zraniteľností, transparentnosti, riadení rizík a posudzovaní zhody počas celého životného cyklu. Paralelne sa rozvíja oblasť certifikácie osôb, výrobkov, procesov a služieb, avšak komplexné portfólio schém zatiaľ chýba, počet akreditovaných orgánov (najmä pre výrobky) je nízky a dopyt po certifikácii je obmedzený.

Cieľový stav

Nové technológie, informačné systémy, digitálne produkty a služby sú uvádzané na trh, obstarávané alebo **implementované podľa princípov *„security-by-default“*** so systematickým testovaním zraniteľností, ochranou pred bežnými vektormi útokov a uplatnením tzv. *zero-trust prístupov* (riadenie prístupov, segmentácia).

Organizácie pri zavádzaní nových technológií **zohľadňujú požiadavky na vysokú odolnosť voči kybernetickým hrozbám** a neuprednostňujú funkčné požiadavky voči požiadavkám na kybernetickú bezpečnosť. Primárne sú obstarávané certifikované produkty a služby.

Je zavedený **účinný systém bezpečnostnej certifikácie** podľa európskych certifikačných rámcov. Štát disponuje funkčnými certifikačnými kapacitami uznávanými na európskej úrovni.

Výrobcovia si uvedomujú potrebu certifikovať svoje výrobky a služby. **Počet certifikačných schém** na produkty, procesy a služby na európskej úrovni, ktoré sú prebraté do slovenského certifikačného rámca, sa navýšil. **Výrobcovia digitálnych produktov** a služieb prirodzene považujú **bezpečnostnú certifikáciu ako trhovú výhodu**. Požiadavky aktu o kybernetickej odolnosti, aktu o umelej inteligencii, ako aj požiadavky na bezpečnostnú certifikáciu sú vhodne integrované do kritérií verejného obstarávania a zmluvných podmienok.

Poskytovatelia a **integrátori technológií umelej inteligencie realizujú riadenie rizík**, zabezpečujú kvalitu údajov, dokumentáciu, transparentnosť a ľudský dohľad, pričom systémy s vysokým rizikom prechádzajú posúdením zhody.

Vzrástol počet akreditovaných a notifikovaných orgánov posudzovania zhody, čím sa zabezpečí zdravé konkurenčné prostredie.

Pilier 4: Vzdelávanie, zručnosti a povedomie

Cieľ 4.1: Budovanie národných znalostných kapacít a vzdelávanie

Východiskový stav

Pre posilnenie národného systému kybernetickej bezpečnosti je kľúčová podpora spolupráce medzi verejnou správou, súkromným sektorom a akademickou obcou, ako aj zavedenie systematického vzdelávania naprieč všetkými úrovňami školstva. Dôležitým prvkom je vytvorenie podmienok pre rozvoj a certifikáciu odborníkov v oblasti kybernetickej bezpečnosti, čo prispeje k zvyšovaniu odbornosti a udržateľnosti celého systému. Osobitnú pozornosť je potrebné venovať budovaniu vzdelanostnej bázy a kapacít v špecifických oblastiach internetu vecí, umelej inteligencie a PQC. V slovenskej republike pretrváva nedostatok kvalifikovaných odborníkov v oblasti kybernetickej bezpečnosti, čo je dôsledkom absencie systematického vzdelávania v tejto oblasti na všetkých úrovniach školského systému. Kybernetická bezpečnosť nie je dostatočne integrovaná do školského kurikula, chýba komplexná príprava pedagógov, ktorí by tému vedeli efektívne pokrývať. Ponuka odborných študijných programov nie je dostatočne rozvinutá, slabo reaguje na potreby trhu práce a tiež chýbajú národné certifikačné mechanizmy na overovanie odbornosti v oblasti kybernetickej bezpečnosti.

Cieľový stav

Kybernetická bezpečnosť je **integrálnou súčasťou vzdelávacích programov na všetkých úrovniach školstva**, čím sa zabezpečí dlhodobá pripravenosť ľudských zdrojov na nové výzvy digitálneho prostredia. Existuje efektívny systém prípravy odborníkov, certifikácie a podpory inovatívneho výskumu, pričom dôraz sa kladie na budovanie povedomia už od najnižších úrovní vzdelávania.

Je vytvorený ucelený a koordinovaný systém vzdelávania v oblasti kybernetickej bezpečnosti, ktorý podporuje rozvoj odborných kapacít na všetkých úrovniach vzdelávania. **Základné a stredné školy** systematicky **rozvíjajú povedomie a návyky** v oblasti kybernetickej bezpečnosti a digitálnych zručností. **Vysoké školy** a odborné inštitúcie zabezpečujú **prípravu kvalifikovaných odborníkov** naprieč profesiami.

Posilnená je spolupráca medzi vzdelávacími inštitúciami, pričom je rozšírená **ponuka akreditovaných programov** a zavedený **systém celoživotného vzdelávania** a odborných školení. Je vytvorený **špecializovaný druh vzdelávania pre špecifické sektory** na posilnenie kompetencií a udržateľné budovanie ľudského kapitálu v oblasti kybernetickej bezpečnosti. Takto vytvorené prostredie umožní nepretržitý rozvoj kompetencií a udržateľné budovanie ľudského kapitálu v oblasti kybernetickej bezpečnosti.

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti, ako aj ďalšie kompetenčné alebo podporné centrá na úrovni iných ústredných orgánov štátnej správy a univerzít, plnia dôležitú úlohu pri budovaní znalostnej bázy a odborných ľudských kapacít. Národné koordinačné centrum pôsobí ako platforma, ktorej hlavným cieľom je budovanie

a podpora odbornej komunity a zdieľanie informácií, ktorá aktívne organizuje a podporuje odborné konferencie, semináre, workshopy, tréningy.

Systém budovania vedomostnej bázy je integrálne doplnený o **vedecko-výskumné pracoviská so zameraním na aplikovanú kybernetickú bezpečnosť** vrátane vývoja a nasadzovania umelej inteligencie.

Partnerstvá so súkromným sektorom a akademickou sférou sú systémovo ukotvené s cieľom podporovať zdieľanie znalostí, informácií a osvedčených postupov a prinášajú inovatívne riešenia pre kybernetickú odolnosť štátu.

Cieľ 4.2: Zvyšovanie digitálnej gramotnosti občanov a bezpečnostného povedomia

Východiskový stav

Rozvoj digitálnej gramotnosti a povedomia verejnosti predstavuje základný predpoklad pre budovanie odolnej spoločnosti voči kybernetickým hrozbám a manipulatívnym technikám. V ére umelej inteligencie a narastajúcej digitalizácie je nevyhnutné, aby občania disponovali znalosťami a zručnosťami potrebnými na bezpečné a zodpovedné využívanie technológií. Je možné konštatovať, že laická verejnosť má stále nízku úroveň digitálnej gramotnosti a povedomia o rizikách spojených s používaním informačných a komunikačných technológií. Občania často nepoznajú princípy bezpečného správania sa v online prostredí, ako sú ochrana osobných údajov, bezpečné používanie hesiel, či overovanie pravdivosti informácií. Znalosti o fungovaní umelej inteligencie, algoritmov a ich vplyve na každodenný život sú obmedzené. Rovnako chýba povedomie o nových hrozbách, ako sú dezinformácie vytvárané prostredníctvom umelej inteligencie alebo kybernetické podvody založené na sociálnom inžinierstve. Vzdelávanie v oblasti digitálnej bezpečnosti sa síce čiastočne realizuje prostredníctvom školských programov, avšak chýba systematický a dlhodobý prístup, ktorý by pokrýval všetky vekové a sociálne skupiny obyvateľstva.

Cieľový stav

Cieľom je vytvoriť informovanú spoločnosť, ktorá dokáže s využitím kritického myslenia rozpoznať riziká digitálneho prostredia, vyhodnotiť ich dôveryhodnosť a efektívne im predchádzať.

Spoločnosť v Slovenskej republike dosahuje **vysokú úroveň digitálnej gramotnosti**. Občania poznajú a aplikujú základné princípy bezpečného správania sa v online prostredí, **poznajú riziká spojené s používaním moderných technológií** a dokážu sa voči nim aktívne chrániť. Základné znalosti o kybernetickej bezpečnosti, hybridných hrozbách, umelej inteligencii a jej etických, právnych a spoločenských dôsledkoch sú prirodzenou súčasťou všeobecného vzdelania. Systematická ochrana detí, žiakov a mládeže v kybernetickom priestore je zabezpečená.

Obyvatelia sú schopní **rozpoznať obsah vytvorený umelou inteligenciou** a kriticky zhodnotiť získané informácie. Vzdelávací systém a inštitúcie verejnej správy podporujú rozvoj

zručností pre bezpečné a etické používanie nových technológií. Podporuje sa vývoj a nasadzovanie metodík, návodov a postupov na odhaľovanie falošného obsahu a iných manipulatívnych techník.

Zavádzanie umelej inteligencie do vzdelávacieho procesu a digitálneho prostredia je sprevádzané **špecifickými bezpečnostnými a etickými opatreniami**, ktoré zohľadnia ich ochranu pred neoprávnenou manipuláciou, dezinformáciami, zneužitím údajov a ďalšími kybernetickými hrozbami.

Rámec základného povedomia o digitálnych zručnostiach a kybernetickej bezpečnosti je **všeobecnou vedomostnou výbavou celej spoločnosti**. Je **zahrnutý do všeobecných vzdelávacích osnov** na základných a stredných školách v rámci povinných predmetov. Zároveň sú podporované programy, kurzy, semináre a iné nástroje celoživotného vzdelávania zamerané na všetky vekové kategórie ako aj úzka spolupráca so súkromným sektorom v danom ohľade.

Národný bezpečnostný úrad na národnej úrovni podporuje cielenú a systematickú digitalizáciu verejných služieb a ich bezpečné využívanie.

Pilier 5: Strategické partnerstvá a medzinárodná spolupráca

Cieľ 5.1: Efektívna medzinárodná spolupráca

Východiskový stav

Slovenská republika systematicky buduje a udržiava **partnerstvá v oblasti kybernetickej bezpečnosti a kybernetickej obrany** v rámci významných medzinárodných organizácií (EÚ, NATO, OSN, OBSE, Rada Európy) a prostredníctvom bilaterálnych dohôd. Podieľa sa na iniciatívach, ktoré prispievajú k posilňovaniu globálnej kybernetickej odolnosti. Slovenská republika sa aktívne angažuje v aktivitách ENISA. Dôležitú rolu zohráva aj pôsobenie Slovenskej republiky v Centre výnimočnosti NATO pre kooperatívnu kybernetickú obranu. Slovenská republika je pevnou súčasťou európskeho a transatlantického priestoru založeného na demokracii, právnom štáte a ochrane základných práv. EÚ a NATO poskytujú strategické, technologické a bezpečnostné zázemie pre spoločné projekty, výmenu informácií a koordináciu reakcií na kybernetické bezpečnostné incidenty. Slovenská republika zároveň posilňuje väzby a príspevok v OBSE a OSN, ktoré formujú medzinárodné normy a politiky v kybernetickej oblasti. Doterajšia prax potvrdzuje význam regionálnej spolupráce, najmä v rámci V4, pre výmenu informácií, zdieľanie osvedčených postupov a koordináciu pri cezhraničných incidentoch. Národná jednotka CSIRT (SK-CERT), ktorá je súčasťou Národného centra kybernetickej bezpečnosti, je členom európskej siete národných CSIRT jednotiek. Viaceré slovenské jednotky CSIRT sa zapájajú do medzinárodných komunít a spoločných cvičení.

Cieľový stav

Štát je aj naďalej **dôveryhodným, rešpektovaným a integrovaným partnerom v rámci EÚ, NATO, OSN, OBSE, ako aj relevantných regionálnych zoskupení** s jasne definovanými rolami, kontaktnými bodmi a procesmi pre bežnú spoluprácu, ako pre koordináciu v rámci krízových situácií. Slovenská republika efektívne využíva kanály na zdieľanie informácií, koordináciu reakcií a spoločné zásahy pri cezhraničných kybernetických bezpečnostných incidentoch, a zároveň sa **pravidelne zúčastňuje na cvičeniach** ENISA, NATO a ďalších medzinárodných cvičeniach s preukázateľným zlepšovaním interoperability.

Slovenská republika zároveň **buduje a rozvíja koncept kybernetickej a digitálnej diplomacie,** okrem iného náležite aplikuje normy zodpovedného správania sa v globálnom kyberpriestore a dodržiava princípy medzinárodného práva. V úzkej spolupráci medzi Ministerstvom zahraničných vecí a európskych záležitostí Slovenskej republiky a ďalšími relevantnými orgánmi Slovenská republika aktívne pôsobí v medzinárodných organizáciách, svetových a európskych fórach, ktoré formujú normy, štandardy a politiky v oblasti kybernetickej bezpečnosti s cieľom zvyšovať diplomatickú angažovanosť Slovenskej republiky, posilňovať jej viditeľnosť a budovať tzv. imidž modernej a bezpečnej krajiny a prispievať k utváraniu medzinárodného prostredia založeného na **zodpovednom správaní sa štátov v kybernetickom priestore**.

Na regionálnej úrovni je zodpovedným partnerom pri koordinácii pripravenosti, rýchlych varovaniach a strategickej komunikácii počas veľkých incidentov. Slovenská republika

zabezpečuje tiež plnú aplikáciu Súboru nástrojov kybernetickej diplomacie ako mechanizmu na prevenciu a odrádzanie od škodlivých kybernetických aktivít a bude aktívne spolupracovať na modalitách atribúcie s členskými štátmi EÚ a so strategickými partnermi z tretích krajín.

V súlade s odporúčaniami EEAS, ako aj so zreteľom na aktuálne medzinárodné trendy, je na národnej úrovni vytvorená plne etablovaná organizačná jednotka vedená veľvyslancom s osobitným určením zameraná na riešenie problematiky kybernetickej, digitálnej diplomacie a technológií. Táto jednotka umožní plnú integráciu Slovenska do zodpovedajúcich medzinárodných štruktúr v EÚ, OSN, OBSE, Rade Európy a ďalších diplomatických technologických platforiem.

Slovenská republika nezaostáva pri aktivovaní mechanizmu **európskych nástrojov kybernetickej solidarit**y, ktorých cieľom je pomôcť ostatným zasiahnutým členským štátom EÚ a kandidátskym krajinám pri reakcii na kybernetické bezpečnostné incidenty väčšieho rozsahu. Slovenská republika tiež v tomto ohľade prispieva svojimi odbornými kapacitami a informáciami na zabezpečenie a zvyšovanie odolnosti celej EÚ.

V rámci solidarity s napadnutými partnermi v rámci EÚ a NATO sa pripája k **spoločným atribučným procesom**. Uvedený mechanizmus je pokračovaním činností a cieľov, ktoré boli začaté na základe predchádzajúcej stratégie. **V rámci kybernetickej diplomacie je zavedený účinný atribučný mechanizmus**, ktorý posilní možnosti **diplomatickej reakcie** na kybernetické bezpečnostné incidenty osobitne alebo v spolupráci s dôveryhodnými partnermi.

S cieľom zaistiť vlastnú národnú bezpečnosť v kybernetickom priestore Slovenská republika vykonáva **atribúciu kybernetických útokov. Atribúcia útočníkov** je veľmi náročný proces, ktorý si vyžaduje dostatočné personálne kapacity a dobre nastavené procesy. Štát posilňuje analytické kapacity v oblasti bezpečnostných hrozieb so špecializáciou na atribúciu kybernetických bezpečnostných incidentov. Dobre nastavený proces technickej, ale aj politickej atribúcie kybernetických bezpečnostných incidentov, dopĺňa právne mechanizmy a mechanizmy kybernetickej diplomacie.

Slovenská republika je **súčasťou európskych nástrojov kybernetickej solidarity**, ktorých cieľom je agregovať a využívať spoločné kapacity členských štátov pri reakcii na rozsiahle kybernetické bezpečnostné incidenty a kybernetické krízy. Na regionálnej úrovni je lídrom vo V4 pri koordinácii pripravenosti, rýchlych varovaniach a strategickej komunikácii počas rozsiahlych kybernetických bezpečnostných incidentoch.

V oblasti umelej inteligencie štát uplatňuje a zosúlaďuje **štandardy bezpečného a etického využívania umelej inteligencie** (riadenie rizík, auditovateľnosť, zodpovedné nasadenie), ktoré chránia základné práva a zvyšujú odolnosť kritickej infraštruktúry, tieto štandardy sú v praxi realizované prostredníctvom spoločných programov, cvičení a výskumných projektov so spojencami.

VII. Implementačný rámec

Pre úspešné naplnenie strategických cieľov stanovených v národnej stratégii je nevyhnutné vytvoriť komplexný Akčný plán realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030 (ďalej len „akčný plán“), ktorý jasne zadefinuje úlohy, časový harmonogram, zodpovednosti a merateľné ukazovatele implementácie (KPI, *angl. Key Performance Indicators*) tak, aby proces napĺňania strategických cieľov bol efektívny a kontrolovateľný. Akčný plán musí byť v súlade s prioritami stratégie a zároveň dostatočne flexibilný, aby mohol reagovať na trendy, meniace sa podmienky a potreby spoločnosti.

Vzhľadom na výraznú dynamiku rozvoja systémov informačných a komunikačných technológií a nových technológií musí byť tiež možné predmetný akčný plán počas nasledujúceho obdobia aktualizovať, ak si to situácia vyžiada.

Po prijatí národnej stratégie, Slovenská republika notifikuje o národnej stratégii Európsku komisiu do troch mesiacov od jej prijatia.

Akčný plán

Akčný plán realizácie národnej stratégie určí:

- konkrétne úlohy rozdelené podľa strategických cieľov spolu s jednotlivými krokmi,
- zodpovedné subjekty v roli gestorov a participujúcich subjektov,
- spôsob realizácie jednotlivých úloh a aktivít a dopady, resp. odhadované náklady vyvolané jednotlivými úlohami,
- časový horizont plnenia úloh.

Za vypracovanie akčného plánu zodpovedá Národný bezpečnostný úrad, ktorý do jeho prípravy zapojí všetky zainteresované subjekty.

Navrhované opatrenia budú vychádzať z analýzy prostredia, rizík a potrieb subjektu, pričom financovanie bude prebiehať v rámci vlastných rozpočtov, programov a projektov, medzirezortných programov a zdieľaných zdrojov EÚ. EÚ ponúka široké možnosti financovania projektov v kybernetickej bezpečnosti. Popri známejších eurofondoch, existujú aj tzv. priamo riadené programy EÚ, cez ktoré priamo Brusel vyhlasuje výzvy na financovanie projektov. Príkladom takýchto programov je Digitálna Európa a Horizont Európa. Národný bezpečnostný úrad poskytne metodickú pomoc s predložením projektu. Navrhované opatrenia však nebudú nad rámec povinností ustanovených všeobecne záväznými právnymi predpismi zaťažovať podnikateľské subjekty, ktoré boli určené ako prevádzkovatelia základných služieb alebo ako prevádzkovatelia kritických základných služieb

Zainteresované subjekty

Medzi hlavné zainteresované subjekty v systéme kybernetickej bezpečnosti Slovenskej republiky, ktoré sa budú podieľať na napĺňaní cieľov tejto národnej stratégie, patria najmä:

- Generálna prokuratúra Slovenskej republiky,
- Kompetenčné a certifikačné centrum kybernetickej bezpečnosti,

- Ministerstvo dopravy Slovenskej republiky,
- Ministerstvo financií Slovenskej republiky,
- Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky,
- Ministerstvo obrany Slovenskej republiky,
- Ministerstvo spravodlivosti Slovenskej republiky,
- Ministerstvo školstva, výskumu, vývoja a mládeže Slovenskej republiky,
- Ministerstvo vnútra Slovenskej republiky,
- Ministerstvo zahraničných vecí a európskych záležitostí Slovenskej republiky,
- Ministerstvo zdravotníctva Slovenskej republiky,
- Prezídium Policajného zboru,
- Slovenská informačná služba,
- Úrad na ochranu osobných údajov Slovenskej republiky,
- Úrad vlády Slovenskej republiky,
- Vojenské spravodajstvo,
- prevádzkovatelia základných služieb,
- vysoké školy a iné vzdelávacie inštitúcie,
- zástupcovia podnikov, podnikateľov a prevádzkovateľov základných služieb zo súkromného sektora.

Kybernetická bezpečnosť priamo súvisí alebo úzko interaguje s inými oblasťami práva a správy veci verejných. Ide predovšetkým o oblasti súvisiace s:

- informatizáciou a digitalizáciou verejnej správy,
- ochranou kritickej infraštruktúry,
- krízovým riadením štátu,
- obranou štátu,
- ochranou osobných údajov,
- interoperabilitou údajov a
- reguláciou umelej inteligencie.

Dôraz sa bude klásť na pravidelnú vzájomnú komunikáciu, výmenu informácií, interoperabilitu procesov a konzistentnosť odporúčaní tak, aby sa opatrenia v oblasti kybernetickej bezpečnosti prirodzene dopĺňali s opatreniami v iných oblastiach.

Kľúčovými partnermi Národného bezpečnostného úradu sú ústredné orgány štátnej správy (ministerstvá, ostatné ústredné orgány štátnej správy) a orgány štátnej správy s celoslovenskou pôsobnosťou (napr. Úrad na ochranu osobných údajov Slovenskej republiky).

Koordinácia a kooperácia medzi uvedenými ústrednými orgánmi štátnej správy bude zabezpečovaná zriaďovaním prierezových alebo tematických pracovných skupín, ktoré prepoja expertízu medzi kybernetickou bezpečnosťou a inými oblasťami. Pracovné skupiny takto vytvoria jednotný priestor na koordináciu plánovania, metodického prístupu a výmeny informácií medzi vyššie uvedenými ústrednými orgánmi a ďalšími rezortmi, regulátormi a verejnými inštitúciami. Dôraz sa bude klásť na pravidelnú vzájomnú komunikáciu,

interoperabilitu procesov a konzistentnosť odporúčaní tak, aby sa opatrenia v oblasti kybernetickej bezpečnosti prirodzene dopĺňali s opatreniami v iných oblastiach.

Osobitne v oblasti umelej inteligencie bude potrebné dôsledne implementovať regulačný rámec EÚ a vybudovať inštitucionálny základ pre reguláciu vývoja, nasadzovania, využívania a bezpečnosti umelej inteligencie v Slovenskej republike. Očakávaná legislatíva nastaví rozdelenie kompetencií a úloh jednotlivých ústredných orgánov štátnej správy, ktoré budú vykonávať reguláciu a štátny dohľad.

Monitorovací výbor

Kľúčovú úlohu v procese implementácie bude zohrávať Monitorovací výbor pre implementáciu úloh vyplývajúcich z akčného plánu (ďalej len „monitorovací výbor“). Monitorovací výbor bude vytvorený a zložený zo zástupcov tých orgánov štátu, ktorých zástupcovia sú povinnými členmi výboru Bezpečnostnej rady Slovenskej republiky pre kybernetickú bezpečnosť, ktorý je pracovným orgánom Bezpečnostnej rady Slovenskej republiky.

Úlohou monitorovacieho výboru bude koordinovať spoluprácu medzi jednotlivými zainteresovanými subjektmi, monitorovať priebeh plnenia úloh akčného plánu, identifikovať prípadné problémy a navrhovať riešenia. Zároveň bude slúžiť ako dôležitá platforma pre výmenu informácií, odborný dialóg a zabezpečenie transparentnosti celého implementačného procesu. Jeho aktívne pôsobenie predstavuje jeden z pilierov úspešného napĺňania strategických cieľov v oblasti kybernetickej bezpečnosti Slovenskej republiky.

Financovanie

Aby bola Slovenská republika schopná naplniť svoje predpoklady a docieliť výsledky, je nutné, aby malo zabezpečený primeraný prístup k dostatočným finančným prostriedkom z verejných, ale aj súkromných zdrojov. V tomto ohľade do popredia vstupujú možnosti financovania zo štátneho rozpočtu, zdieľaných zdrojov EÚ, ako sú programy kohéznej politiky, či z takzvaných priamo riadených prostriedkov. Kybernetická bezpečnosť nesmie zostať bokom pri programovaní národných cieľov, či pri otváraní možností spolufinancovania súkromného kapitálu. Obzvlášť dôležité bude správne nastavenie budúceho viacročného finančného rámca 2028 – 2034.

Každý z relevantných subjektov zapojených do plnenia cieľov národnej stratégie a úloh, ktoré budú určené v súvisiacom akčnom pláne, bude zodpovedný za zabezpečenie primeraného financovania týchto úloh a aktivít.

VIII. Záver

Národná stratégia predstavuje strategický plán a záväzok štátu chrániť a posilňovať digitálne prostredie ako neoddeliteľnú súčasť národnej bezpečnosti, hospodárskej stability a ochrany demokratických hodnôt. Úspešná realizácia stratégie bude závisieť od schopnosti všetkých zainteresovaných subjektov konať koordinovane, zdieľať informácie, implementovať osvedčené postupy a flexibilne reagovať na dynamicky sa meniace hrozby.

Rovnako dôležitá bude schopnosť kontinuálne investovať do prevencie, výskumu, vzdelávania a inovácií, aby Slovenská republika dokázala udržať a posilniť svoju odolnosť voči kybernetickým hrozbám a kybernetickým bezpečnostným incidentom. Národná stratégia vyjadruje odhodlanie Slovenskej republiky zabezpečiť integritu, dostupnosť a dôvernosť digitálnych služieb a infraštruktúry, posilniť spoluprácu so spojencami a partnermi, presadzovať princípy otvoreného, slobodného, stabilného a bezpečného kybernetického priestoru, zvyšovať digitálnu gramotnosť a bezpečnostné povedomie obyvateľstva a podporovať technologické inovácie v súlade s princípmi kybernetickej bezpečnosti.

Národná stratégia zohľadňuje aj otázku predchádzania a boja proti kybernetickej kriminalite a schopnosti vykonávať celé spektrum škodlivých aktivít v kybernetickom priestore.

Implementácia opatrení definovaných v tejto národnej stratégii bude prebiehať v súlade s právnym rámcom Európskej únie, všeobecne záväznými právnymi predpismi Slovenskej republiky, ako aj relevantnými medzinárodnými záväzkami. Týmto prístupom sa zabezpečí vytvorenie bezpečného digitálneho prostredia, ktoré podporí hospodársky rast, zvýši dôveru občanov v digitalizáciu a ochráni národné záujmy.