

VYHODNOTENIE PRIPOMIENKOVÉHO KONANIA
Národná stratégia kybernetickej bezpečnosti na roky 2026 až 2030
LP/2025/679

Spôsob pripomienkového konania

Počet vznesených pripomienok, z toho zásadných:	153/50
Počet vyhodnotených pripomienok:	153

Počet akceptovaných pripomienok, z toho zásadných:	64/24
Počet čiastočne akceptovaných pripomienok, z toho zásadných:	55/20
Počet neakceptovaných pripomienok, z toho zásadných:	27/6

Počet vznesených hromadných pripomienok:	0
Počet vyhodnotených hromadných pripomienok:	0

Počet akceptovaných hromadných pripomienok:	0
Počet čiastočne akceptovaných hromadných pripomienok:	0
Počet neakceptovaných hromadných pripomienok:	0

Vysvetlivky k použitým skratkám v tabuľkách:

O – obyčajná A – akceptovaná
 Z – zásadná N – neakceptovaná
 ČA – čiastočne akceptovaná
 NEP – neprihliada sa

Vyhodnotenie vecných pripomienok

Vznesené pripomienky

Subjekt	Typ	Pripomienka	Vyh.	Spôsob vyhodnotenia
AFCEA AFCEA Slovakia	O	časť V, str.16 Oceňujeme, že Stratégia kladie dôraz na technologickú suverenitu a preferenciu národných technologických riešení. Zároveň považujeme za vhodné vyjasniť, že technologická suverenita a preferencia národných technologických riešení nemajú za cieľ obmedzovanie technologickej neutrality, zvyšovanie nákladov poskytovateľov kritických služieb, spomaľovanie inovácií a izoláciu, ani oslabovanie odolnosti a bezpečnosti tým, že by sa obmedzil prístup k moderným cloudovým a bezpečnostným službám, ktoré poskytujú globálne spoločnosti s vyššou mierou investícií, know-how a prevádzkových skúseností. Na to poukazuje aj Deklarácia o európskej digitálnej suverenite, ktorá bola podpísaná 18. novembra 2025 všetkými členskými štátmi EÚ, vrátane Slovenska, a ktorá okrem iného uvádza, že: „digitálna suverenita by nemala byť vykladaná ako protekcionizmus, ale ako spoločný európsky prístup, ktorý posilní našu schopnosť konať slobodne a zároveň spolupracovať s globálnymi trhmi a partnermi. Európa by preto mala zostať otvorená globálnym partnerom, ktorí	ČA	Doplnený text: „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 sa na vývojových projektoch a procesoch

		zdieľajú rovnaké hodnoty ako EÚ, a spoločnému úsiliu o ďalšie využívanie výhod globálnej vedeckej a technologickej spolupráce.“ Odporúčame preto, aby Stratégia v súlade s uvedenou Deklaráciou vyjasnila, že cieľom nie je obmedzovať využívanie komerčných cloudových služieb, ktoré spĺňajú bezpečnostné, certifikačné a compliance požiadavky, princíp „technologickej autonómie“ nemá byť chápaný ako automatická preferenčná podpora lokálnych alebo vlastných riešení, ani nemá narušovať otvorený trh a požiadavku na interoperabilitu technológií, a že kľúčovým kritériom má byť merateľná úroveň bezpečnosti, prevádzkovej spoľahlivosti a auditovateľnosti. toto doplnenie by zabezpečilo, že Stratégia posilní kybernetickú bezpečnosť Slovenskej republiky spôsobom, ktorý zároveň podporí modernizáciu, digitálnu transformáciu a využívanie najpokročilejších dostupných technológií bez neúmyselného obmedzovania inovácií či trhu. Návrh úpravy: Technologickou suverenitou a dôrazom na podporu domácich dodávateľov sa nemyslí snaha izolovať Slovenskú republiku od globálnych technologických trendov, narušovať otvorený trh alebo spochybňovať požiadavky na štandardizáciu a interoperabilitu technológií. Cieľom týchto požiadaviek nie je obmedziť využívanie komerčných cloudových a iných digitálnych služieb, ktoré spĺňajú bezpečnostné, certifikačné a právne predpisy. Kľúčovým kritériom pri výbere dodávateľov týchto služieb zostane aj naďalej bezpečnosť, prevádzková spoľahlivosť a auditovateľnosť.		v rámci Európskej únie. Zároveň musí podporiť nasadzovania takto vyvinutých technológií v slovenskom kybernetickom priestore. Systém podpory a motivácie musí prevažovať nad akýmkoľvek reštriktívnymi nástrojmi, ktoré by mohli spôsobiť izoláciu Slovenskej republiky od globálneho technologického pokroku alebo narušenie otvoreného trhu.“.
APZD Asociácia priemyselných zväzov a dopravy	Z	K celému materiálu Navrhujeme, aby sa v stratégii výslovne uviedlo, že energetické zdroje s inštalovaným výkonom do 2,5 MW (elektrickým alebo tepelným) nemajú byť v ďalšej implementácii politiky	N	Pripomienku nie je možné akceptovať z dôvodu, že sa netýka priamo predloženého

		kybernetickej bezpečnosti klasifikované ako regulované subjekty (najmä ako prevádzkovatelia základnej služby podľa § 17 zákona o kybernetickej bezpečnosti). Odôvodnenie: Predložený materiál nerozlišuje medzi malými a veľkými energetickými zdrojmi, hoci smernica NIS2 umožňuje uplatniť proporcionálny prístup pri určovaní povinností. Malé bioplynové zdroje nevytvárajú systémové riziko pre energetickú bezpečnosť a ich prípadný výpadok neohrozuje kritické štátne funkcie ani stabilitu prenosovej a distribučnej sústavy. Uplatnenie plného režimu NIS2 na tieto malé zdroje by predstavovalo neprimeranú administratívnu a finančnú záťaž, ktorá môže prekračovať prevádzkové kapacity malých prevádzok. Takéto opatrenie by zároveň kontrastovalo s cieľmi SR v oblasti podpory obnoviteľných zdrojov energie, decentralizácie výroby a rozvoja biometánu.		materiálu, ale spôsobu identifikácie prevádzkovateľa základnej služby, resp. klasifikácie regulovaného subjektu, ktorý je stanovený zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 69/2018 Z. z.“). Predložená stratégia má povahu deklaratorneho materiálu a nepresahuje všeobecne záväzný právny predpis, odráža faktický právny stav, preto v nej nie je možné riešiť ani zakladať žiadne nové vzťahy. Predkladaná stratégia je východiskovým strategickým dokumentom, ktorý
--	--	--	--	--

				nadväzuje na predchádzajúce strategické dokumenty v oblasti kybernetickej bezpečnosti a je vypracovaný v súlade s vyvíjajúcim sa právnym rámcom Európskej únie, tzn. priamo zohľadňuje povinnosti vyplývajúce z kľúčových právnych aktov. Stratégia komplexne určuje strategický prístup Slovenskej republiky k zabezpečeniu vysokej úrovne kybernetickej bezpečnosti v súlade s § 7 zákona č. 69/2018 Z. z. v nadväznosti na čl. 7 smernice NIS 2. Mechanizmus identifikácie prevádzkovateľa základnej služby podľa zákona č. 69/2018 Z. z. vychádza najmä z princípu
--	--	--	--	---

				samoidentifikácie subjektu, pričom je potrebné v kontexte § 17 a § 18 zákona č. 69/2018 Z. z. prihliadať aj na kritériá veľkosti podniku. Pri posudzovaní veľkosti podniku sa vychádza z Odporúčania Komisie 2003/361/ES zo 6. mája 2003 o vymedzení pojmu mikro, malých a stredných podnikov. Prvým kritériom posudzovania veľkosti podniku je počet zamestnancov a druhým kritériom je ročný obrát alebo celková ročná bilancia. Pripomienkujúci subjekt súhlasil s predloženým návrhom vyhodnotenia mejlom 19.01.2026. Rozpor odstránený.
AZZZ SR Asociácia	Z	k VI. (VII.) Implementačný rámec Pripomienka k VI. (VII.) Implementačný rámec	ČA	Pripomienka sa týka konkrétneho sektora

zamestnávateľský ch zväzov a združení Slovenskej republiky		Návrh: zabezpečiť finančnú podporu pre kybernetickú ochranu vodárenských spoločností, Zdôvodnenie: Takto bude zabezpečená finančná udržateľnosť a stabilita poskytovania základných služieb.	(vodárenskej infraštruktúry). Stratégia má povahu deklarátneho materiálu a nepresahuje všeobecne záväzný právny predpis, odráža faktický právny stav. Všetky povinnosti prevádzkovateľa základnej služby alebo subjekt verejnej správy, začleneného v konkrétnom sektore podľa prílohy I. alebo prílohy II. zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 69/2018 Z. z.“), sú ustanovené v zákone č. 69/2018 Z. z. vychádzajúc zo smernice NIS 2. Do Doložky
---	--	---	--

				vybraných vplyvov v časti 10. Poznámky doplnená informácia: „Financovanie v oblasti kybernetickej bezpečnosti bolo zohľadnené pri legislatívnom procese zákona 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. Financovanie opatrení v predkladanej stratégii bude zabezpečené v rámci kapitol jednotlivých ústredných orgánov (sektorové politiky), rozpočtových opatrení pre rozpočtové organizácie, medzirezortných
--	--	--	--	---

			programov (napr. v rámci ochrany kritickej infraštruktúry je vytvorený medzirezortný rozpočtový program 0AS Ochrana kritickej infraštruktúry v SR), zdieľaných zdrojov EÚ [programy kohéznej politiky (napr. Program Slovensko), priamo riadené programy (napr. Digital Europe Programme], bilaterálnych programov SR zameraných na vedu a výskum, a iných, ktoré podporujú činnosti v oblasti vedy, výskumu a inovácií aj z oblasti bezpečnosti) a príspevkov jednotlivých prevádzkovateľov základnej služby.“. Pripomienkujúci subjekt súhlasil s
--	--	--	---

				predloženým návrhom vyhodnotenia mejlom 19.01.2026.
AZZZ SR Asociácia zamestnávateľských zväzov a združení Slovenskej republiky	Z	k VI. (VII.) Implementačný rámec Pripomienka k VI. (VII.) Implementačný rámec Návrh: Zodpovedné orgány štátnej správy (gestori sektorov) v spolupráci s Ministerstvom financií SR a Úradom pre reguláciu sieťových odvetví zabezpečia, aby náklady regulovaných subjektov na plnenie povinností kybernetickej odolnosti, vyplývajúcich z tejto stratégie a súvisiacej legislatívy, boli plne akceptované ako ekonomicky oprávnené náklady v rámci mechanizmov cenovej regulácie. Zdôvodnenie: Takto bude zabezpečená finančná udržateľnosť a stabilita poskytovania základných služieb.	ČA	Uplatnenie nákladov na zabezpečenie kybernetickej bezpečnosti a odolnosti systémov, ktoré sa týkajú služieb poskytovaných podnikmi v sieťových odvetviach, nepovažujeme za problematické. Všetky povinnosti prevádzkovateľa základnej služby alebo subjekt verejnej správy, začleneného v konkrétnom sektore podľa prílohy I. alebo prílohy II. zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 69/2018 Z. z.“), sú

			ustanovené v zákone č. 69/2018 Z. z. vychádzajúc zo smernice NIS 2. Do Doložky vybraných vplyvov v časti 10. Poznámky doplnená informácia: „Financovanie v oblasti kybernetickej bezpečnosti bolo zohľadnené pri legislatívnom procese zákona 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. Financovanie opatrení v predkladanej stratégii bude zabezpečené v rámci kapitol jednotlivých
--	--	--	---

			ústredných orgánov (sektorové politiky), rozpočtových opatrení pre rozpočtové organizácie, medzirezortných programov (napr. v rámci ochrany kritickej infraštruktúry je vytvorený medzirezortný rozpočtový program 0AS Ochrana kritickej infraštruktúry v SR), zdieľaných zdrojov EÚ [programy kohéznej politiky (napr. Program Slovensko), priamo riadené programy (napr. Digital Europe Programme], bilaterálnych programov SR zameraných na vedu a výskum, a iných, ktoré podporujú činnosti v oblasti vedy, výskumu a inovácií aj z oblasti bezpečnosti) a príspevkov
--	--	--	--

				jednotlivých prevádzkovateľov základnej služby.“. V neposlednom rade problematika kybernetickej odolnosti bude riešená národnou právnou úpravou, ktorá implementuje Akt o kybernetickej odolnosti [Cyber Resilience Act (CRA)], ktorá bude zohľadňovať finančný rámec opatrení na zabezpečenie kybernetickej odolnosti. Pripomienkujúci subjekt súhlasil s predloženým návrhom vyhodnotenia mejlom 19.01.2026.
AZZZ SR Asociácia zamestnávateľských zväzov a združení	Z	k VI. Strategické piliere a ciele/ Pilier 5: Strategické partnerstvá a medzinárodná spolupráca Pripomienka k VI. Strategické piliere a ciele/ Pilier 5: Strategické partnerstvá a medzinárodná spolupráca Návrh: Zapojiť vodárenské spoločnosti do medzinárodných	ČA	Pripomienku sa týka konkrétneho sektora (vodárenskej infraštruktúry) a konkrétnej úlohy, čo

Slovenskej republiky		cvičení kybernetickej odolnosti, Zdôvodnenie: Umožniť nepretržitý rozvoj kompetencií a udržateľné budovanie ľudského kapitálu v oblasti kybernetickej bezpečnosti pre bezpečnosť vodárenských systémov.	vzhľadom na povahu predloženého dokumentu (stratégia má povahu deklarátorného materiálu a nepresahuje všeobecne záväzný právny predpis, odráža faktický právny stav) v nej nie je možné riešiť. Predložená stratégia je východiskovým strategickým dokumentom, ktorá nadväzuje na predchádzajúce strategické dokumenty v oblasti kybernetickej bezpečnosti a plnenie strategických cieľov v nej stanovených sa bude realizovať na základe jasne zadefinovaných úloh, časovom harmonograme, zodpovednosti a merateľných ukazovateľov v Akčnom pláne
----------------------	--	---	---

				realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030, kam možno úlohy pre vodárenské spoločnosti zahrnúť. Pripomienkujúci subjekt súhlasil s predloženým návrhom vyhodnotenia mejlom 19.01.2026.
AZZZ SR Asociácia zamestnávateľských zväzov a združení Slovenskej republiky	Z	k VI. Strategické piliere a ciele/ Pilier 1: Ochrana národného kybernetického priestoru Pripomienka k VI. Strategické piliere a ciele/ Pilier 1: Ochrana národného kybernetického priestoru Návrh: - doplniť aj vodárenskú infraštruktúru medzi prioritné ciele kybernetickej ochrany, - riešiť riziká zahraničných komponentov v SCADA (riadiace systémy vodárenskej infraštruktúry) a podporiť certifikovaných dodávateľov, - zaviesť kontrolu bezpečnosti a simulované útoky na SCADA systémy, Zdôvodnenie: Bez jasného zaradenia vodárenských spoločností medzi kritické sektory, adekvátneho financovania a povinných bezpečnostných opatrení nebude možné zabezpečiť stabilnú a bezpečnú dodávku pitnej vody.	ČA	Pripomienka sa týka konkrétneho sektora (vodárenskej infraštruktúry) a požaduje príliš konkrétne ciele, priority a úlohy, čo vzhľadom na povahu predloženého dokumentu (stratégia má povahu deklaratorného materiálu a nepresahuje všeobecne záväzný právny predpis, odráža faktický právny stav) v ňom nie je možné

		Vítame prijatie Národnej stratégie kybernetickej bezpečnosti 2026 – 2030. Dodávka pitnej vody a odkanalizovanie patria medzi základné verejné služby, ktorých bezpečnosť je priamo závislá od odolnosti digitálnych systémov. Preto je nevyhnutné, aby stratégia zohľadnila špecifiká vodárenského sektora.	riešiť. Zaradenie vodárenských spoločností medzi kritické sektory nerieši predložená stratégia, ale všeobecne záväzný právny predpis. Predložená stratégia je východiskovým strategickým dokumentom, ktorá nadväzuje na predchádzajúce strategické dokumenty v oblasti kybernetickej bezpečnosti a plnenie strategických cieľov v nej stanovených sa bude realizovať na základe jasne zadefinovaných úloh, časovom harmonograme, zodpovednosti a merateľných ukazovateľov v Akčnom pláne realizácie Národnej stratégie kybernetickej bezpečnosti na roky
--	--	--	---

				2026 až 2030, kam možno úlohy pre vodárenské spoločnosti zahrnúť. Pripomienkujúci subjekt súhlasil s predloženým návrhom vyhodnotenia mejlom 19.01.2026.
AZZZ SR Asociácia zamestnávateľských zväzov a združení Slovenskej republiky	Z	k VI. Strategické piliere a ciele/ Pilier 2: Budovanie národných kapacít v oblasti kybernetickej bezpečnosti Pripomienka k VI. Strategické piliere a ciele/ Pilier 2: Budovanie národných kapacít v oblasti kybernetickej bezpečnosti Návrh: Poskytnúť metodickú podporu zo strany NBÚ a CSIRT.SK Zdôvodnenie: NBÚ je zastrešujúci ústredný orgán štátnej správy pre celú oblasť kybernetickej bezpečnosti v štáte, vrátane kritickej infraštruktúry. CSIRT.SK zabezpečuje služby spojené so zvládaním bezpečnostných incidentov, odstraňovaním ich následkov a obnovou činnosti informačných systémov verejnej správy.	A	Doplnený text: „Národný bezpečnostný úrad vydáva metodiky a stanoviská k aplikácii všeobecne záväzných právnych predpisov a nelegislatívnych dokumentov na úseku kybernetickej bezpečnosti.“.
AZZZ SR Asociácia zamestnávateľských zväzov a združení	Z	k VI. Strategické piliere a ciele/ Pilier 4: Vzdelávanie, zručnosti a povedomie Pripomienka k VI. Strategické piliere a ciele/ Pilier 4: Vzdelávanie, zručnosti a povedomie Návrh: Vytvoriť špecializované školenia pre technikov (SCADA, IoT),	A	Doplnený text: „Je vytvorený špecializovaný druh vzdelávania pre špecifické sektory na posilnenie kompetencií

Slovenskej republiky		Zdôvodnenie: Umožniť nepretržitý rozvoj kompetencií a udržateľné budovanie ľudského kapitálu v oblasti kybernetickej bezpečnosti pre bezpečnosť vodárenských systémov.		a udržateľné budovanie ľudského kapitálu v oblasti kybernetickej bezpečnosti.“.
AZZZ SR Asociácia zamestnávateľských zväzov a združení Slovenskej republiky	O	k VI. (VII.) Implementačný rámec Formálna pripomienka Pripomienka k VI. (VII.) Implementačný rámec Návrh: opraviť číslovanie pri Implementačnom rámci – ide o časť VII. nie VI.	A	Text upravený v zmysle pripomienky: „VII. Implementačný rámec“.
AmCham Slovakia Americká obchodná komora v Slovenskej republike	O	Celému materiálu Zásadná pripomienka: AmCham Slovakia oceňuje, že Národná stratégia kladie dôraz na technologickú suverenitu a preferenciu národných technologických riešení. Zároveň je však dôležité zdôrazniť, že technologická suverenita a preferencia národných technologických riešení nemajú za cieľ i) obmedzovanie technologickej neutrality ani ii) oslabovanie odolnosti a bezpečnosti tým, že obmedzí prístup k moderným cloudovým a bezpečnostným službám, ktoré poskytujú globálne spoločnosti s vyššou mierou investícií, know-how a prevádzkových skúseností. Na to poukazuje aj Deklarácia o európskej digitálnej suverenite, ktorá bola podpísaná 18. novembra 2025 všetkými členskými štátmi EÚ, vrátane Slovenska, a ktorá okrem iného uvádza, že: „digitálna suverenita by nemala byť vykladaná ako protekcionizmus, ale ako spoločný európsky prístup, ktorý posilní našu schopnosť konať slobodne a zároveň spolupracovať s globálnymi trhmi a partnermi. Európa by preto mala zostať otvorená globálnym partnerom, ktorí zdieľajú rovnaké hodnoty ako EÚ, a spoločnému úsiliu o ďalšie využívanie výhod	ČA	Bude dooplnený text v približnom znení: „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 sa na vývojových

		globálnej vedeckej a technologickej spolupráce.“ Odporúčame preto, aby Stratégia v súlade s uvedenou Deklaráciou doplnila nasledovné: i) cieľom Stratégie nie je obmedzovať využívanie komerčných cloudových služieb, ktoré spĺňajú bezpečnostné, certifikačné a compliance požiadavky, ii) princíp „technologickej autonómie“ nemá byť chápaný ako automatická preferenčná podpora lokálnych alebo vlastných riešení, ani nemá narušovať otvorený trh a požiadavku na interoperabilitu technológií, iii) kľúčovým kritériom má byť merateľná úroveň bezpečnosti, prevádzkovej spoľahlivosti a auditovateľnosti. Toto doplnenie by zabezpečilo, že Stratégia posilní kybernetickú bezpečnosť Slovenskej republiky spôsobom, ktorý zároveň podporí modernizáciu, digitálnu transformáciu a využívanie pokročilejších dostupných technológií bez neúmyselného obmedzovania inovácií či trhu.		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 akýmkoľvek reštriktívnymi nástrojmi, ktoré by mohli spôsobiť izoláciu Slovenskej republiky od globálneho technologického pokroku alebo narušenie otvoreného trhu.“. Pripomienkujúci subjekt súhlasil s predloženým návrhom vyhodnotenia mejlom 20.01.2026. Rozpor odstránený.
AmCham Slovakia	O	Časť V. - Vízia národnej stratégie Zásadná pripomienka: Navrhujeme doplniť do Časti V. - Vízia	ČA	Doplnený text v približnom znení:

Americká obchodná komora v Slovenskej republike		národnej stratégie na s. 16 nasledujúce: "Technologickou suverenitou a dôrazom na podporu domácich dodávateľov sa nemyslí snaha izolovať Slovenskú republiku od globálnych technologických trendov, narušovať otvorený trh alebo spochybňovať požiadavky na štandardizáciu a interoperabilitu technológií. Cieľom týchto požiadaviek nie je obmedziť využívanie komerčných cloudových a iných digitálnych služieb, ktoré spĺňajú bezpečnostné, certifikačné a právne predpisy. Kľúčovým kritériom pri výbere dodávateľov týchto služieb zostane aj naďalej bezpečnosť, prevádzková spoľahlivosť a auditovateľnosť."	„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 akýmkoľvek reštriktívnymi nástrojmi, ktoré by mohli spôsobiť
--	--	--	---

				izoláciu Slovenskej republiky od globálneho technologického pokroku alebo narušenie otvoreného trhu.“. Pripomienkujúci subjekt súhlasil s predloženým návrhom vyhodnotenia mejlom 20.01.2026. Rozpor odstránený.
Asociácia kritickej infraštruktúry SR Asociácia kritickej infraštruktúry Slovenskej republiky	O	Celému materiálu Túto pripomienku podávame ako zásadnú: Nejasná úloha súkromného sektora a absencia Asociácie kritickej infraštruktúry Slovenskej republiky v implementácii Odôvodnenie: Sektorové profesijné organizácie, ako AKI SR, zabezpečujú odbornú koordináciu, výmenu informácií a pripomienkovanie opatrení na úrovni jednotlivých odvetví kritickej infraštruktúry. Návrh stratégie však ignoruje ich systémovú úlohu a nezaraďuje ich medzi partnerov implementácie, konzultácií ani do pracovných skupín. Takýto prístup obmedzuje možnosť participácie sektorov na formovaní štátnych opatrení a môže viesť k nízkej akceptácii regulácií zo strany prevádzkovateľov KI. Návrh AKI SR: Doplniť AKI SR ako: • povinného konzultačného partnera,	A	V kapitole VII. Implementačný rámec v časti „Zainteresované subjekty“ doplnený text: „zástupcovia podnikov, podnikateľov a prevádzkovateľov základných služieb zo súkromného sektora“.

		• člena pracovných skupín pre PQC, SCRM, NIS2/CER implementáciu a architektúru SOC, • partnera pri tvorbe akčného plánu, • partnera Monitorovacieho výboru.		
Asociácia kritickej infraštruktúry SR Asociácia kritickej infraštruktúry Slovenskej republiky	O	Celému materiálu Túto pripomienku podávame ako zásadnú: Neexistujúci model financovania dopadov NIS2 a CER na kritickú infraštruktúru Odôvodnenie: Prevádzkovatelia KI budú musieť investovať do rozsiahlych bezpečnostných úprav (sieťová segmentácia, monitoring, detekčné systémy, penetračné testovanie, audity, implementácia PQC, certifikácie, školenia). Bez definovaného mechanizmu spolufinancovania, grantových schém, daňových úľav alebo európskych finančných nástrojov môže byť implementácia pre niektoré odvetvia ekonomicky neudržateľná, najmä pre regulované sektory (energia, voda, doprava, zdravotníctvo). Návrh AKI SR: Doplniť záväzné mechanizmy financovania, najmä: • národný fond kybernetickej odolnosti KI, • možnosť čerpania z fondov EÚ (DIGITAL, CEF2, Horizon Europe), • daňové stimuly pre investície do kyberbezpečnosti, • schému spolufinancovania pre povinné opatrenia podľa NIS2/CER, • cenovú reguláciu v regulovaných odvetviach umožňujúcu premietnutie nákladov.	ČA	Pripomienku nie je možné akceptovať z dôvodu, že skupina kritických subjektov je užšia ako skupina prevádzkovateľov základnej služby a taktiež ochrana kritickej infraštruktúry a zvyšovanie jej odolnosti, resp. odolnosti kritických subjektov je regulovaná zákonom č. 367/2024 Z. z. o kritickej infraštruktúre a o zmene doplnení niektorých zákonov. Taktiež financovanie kritických subjektov je záležitosťou sektorového regulátora a MV SR. Do Doložky vybraných vplyvov v časti 10. Poznámky

				doplnená informácia: „Financovanie v oblasti kybernetickej bezpečnosti bolo zohľadnené pri legislatívnom procese zákona 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. Financovanie opatrení v predkladanej stratégii bude zabezpečené v rámci kapitol jednotlivých ústredných orgánov (sektorové politiky), rozpočtových opatrení pre rozpočtové organizácie, medzirezortných programov (napr. v rámci ochrany kritickej
--	--	--	--	--

			infraštruktúry je vytvorený medzirezortný rozpočtový program 0AS Ochrana kritickej infraštruktúry v SR), zdieľaných zdrojov EÚ [programy kohéznej politiky (napr. Program Slovensko), priamo riadené programy (napr. Digital Europe Programme], bilaterálnych programov SR zameraných na vedu a výskum, a iných, ktoré podporujú činnosti v oblasti vedy, výskumu a inovácií aj z oblasti bezpečnosti) a príspevkov jednotlivých prevádzkovateľov základnej služby.“. Pripomienkujúci subjekt súhlasil s predloženým návrhom vyhodnotenia mejlom
--	--	--	--

				19.01.2026. Rozpor odstránený.
Asociácia kritickej infraštruktúry SR Asociácia kritickej infraštruktúry Slovenskej republiky	O	Celému materiálu Neadresované problémy s nedostatkom špecialistov a odlevom odborníkov Odôvodnenie: Na trhu práce pretrváva nedostatok kvalifikovaných odborníkov v oblasti kybernetickej a infraštruktúrnej bezpečnosti. Stratégia neobsahuje systémové opatrenia na stabilizáciu personálnych kapacít v kritických odvetviach (napr. podpora certifikácií, kariérne programy, štátne stimuly, sektorové školenia). Bez riešenia tejto oblasti nie je možné zabezpečiť dlhodobú udržateľnosť implementácie. Návrh AKI SR: Doplniť opatrenia na podporu odborníkov v KI sektoroch, najmä: • národné programy certifikácií, • podporné schémy pre odborníkov pracujúcich v KI, • finančné a kariérne stimuly, • spoločné vzdelávacie programy s priemyslom.	ČA	Pripomienka bude zohľadnená pri tvorbe Akčného plánu realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030.
Asociácia kritickej infraštruktúry SR Asociácia kritickej infraštruktúry Slovenskej republiky	O	Celému materiálu Túto pripomienku podávame ako zásadnú: Chýbajúci mechanizmus pre hodnotenie vysokorizikových dodávateľov (SCRM) Odôvodnenie: Hoci návrh stratégie zdôrazňuje potrebu posilnenia bezpečnosti dodávateľských reťazcov, absentujú kritériá, procesy a metodiky na posudzovanie rizikovosti dodávateľov, ako aj postupy pre eskaláciu, audit a nápravné opatrenia. Prevádzkovatelia kritickej infraštruktúry nemajú bez tohto rámca oporu pre riadené uplatňovanie SCRM opatrení. Nejasné je aj to, ako budú	N	Povinnosti týkajúce dodávateľského reťazca sú ustanovené priamo v zákone č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov [napr. § 7 ods. 3 písm

		implementované odporúčania európskeho ICT Supply Chain Security Toolboxu. Návrh AKI SR: Doplniť celonárodný rámec bezpečnosti dodávateľských reťazcov ICT, ktorý bude obsahovať: • definíciu kategórií rizikovosti dodávateľov, • postupy hodnotenia vysokorizikových dodávateľov, • kritériá pre vylúčenie dodávateľa z KI sektorov, • požiadavky na auditovateľnosť a transparentnosť komponentov • štandardizované zmluvné podmienky pre dodávateľov ICT, • proces centrálnej eskalácie a rozhodovania.	a) v rámci národnej stratégie kybernetickej bezpečnosti sa prijímajú politiky najmä na zabezpečenie kybernetickej bezpečnosti v dodávateľskom reťazci produktov IKT a služieb IKT; § 19 ods. 6 prevádzkovateľ základnej služby je ďalej povinný analyzovať závislosti svojich aktív, informačných systémov, využívaných produktov IKT a služieb IKT tretích strán v dodávateľskom reťazci a poskytovaných služieb s cieľom identifikovať možné dopady kybernetického bezpečnostného incidentu; § 20 ods. 2 písm. q) bezpečnostné opatrenia sa prijímajú aspoň pre dodávateľský reťazec].
--	--	--	---

				Nie je možné zovšeobecniť kritériá, procesy a metodiky na posudzovanie rizikovosti dodávateľov, ako aj postupy pre eskaláciu, audit a nápravné opatrenia vzhľadom na odlišnú analýzu rizík jednotlivých prevádzkovateľov základnej služby a na ňu viažuce sa bezpečnostné opatrenia (týkajúce sa aj dodávateľského reťazca). Pripomienkujúci subjekt súhlasil s predloženým návrhom vyhodnotenia mejlom 19.01.2026. Rozpor odstránený.
Asociácia kritickej infraštruktúry SR Asociácia kritickej	O	Celému materiálu Nedostatočné prepojenie kybernetickej diplomacie s ochranou kritickej infraštruktúry Odôvodnenie: Prevádzkovatelia KI sú častými cieľmi štátom podporovaných útokov. Strategické dokumenty EÚ v oblasti kyberdiplomacie	ČA	Predložená stratégia sa vzťahuje na všetkých prevádzkovateľov základnej služby, aj tých ktorí sú kritickými subjektmi.

infraštruktúry Slovenskej republiky		zdôrazňujú potrebu prepojenia atribúcie, sankčných mechanizmov a ochrany infraštruktúry. Návrh stratégie tieto väzby ignoruje. Návrh AKI SR: Doplniť mechanizmy pre: • diplomatickú podporu pri útokoch na KI, • technickú a politickú atribúciu s priamym zapojením KI sektorov, • zdieľanie informácií s európskymi partnermi.		Kybernetická diplomacia, účinný atribučný mechanizmus, strategické partnerstvá a medzinárodná spolupráca sú v predloženej stratégii riadne zadefinované. V oblasti kritickej infraštruktúry bola prijatá Stratégia odolnosti kritických subjektov SR (uznesenie vlády SR č. 3 z 09.01.2026), ktorá okrem iného rieši aj spoluprácu (vrátane zdieľania informácií) aj na medzinárodnej úrovni.
Asociácia kritickej infraštruktúry SR Asociácia kritickej infraštruktúry Slovenskej republiky	O	Celému materiálu Túto pripomienku podávame ako zásadnú: Chýbajúca integrácia rámcov NIS2 a CER v oblasti kritickej infraštruktúry Odôvodnenie: V praxi tvoria opatrenia NIS2 a CER jeden spoločný systém riadenia rizík prevádzkovateľov kritickej infraštruktúry. Stratégia však pristupuje k týmto rámcom izolovane, bez harmonizácie postupov, terminológie, kontrolných mechanizmov a reportingových požiadaviek. To môže viesť k duplicite kontrol,	ČA	Z hľadiska povahy predloženého materiálu je prepojenie na oblasť kritickej infraštruktúry dostatočné (previazanie na smernicu CER, zvyšovanie odolnosti kritických subjektov,

		regulačnej neistote a neprimeranému administratívne mu zaťaženiu. Prevádzkovatelia KI potrebujú jednotný ucelený rámec. Návrh AKI SR: Vytvoriť jednotný model implementácie NIS2 + CER pre kritickú infraštruktúru, ktorý bude obsahovať: • harmonizované procesy riadenia rizík, • jednotnú terminológiu, • spoločné auditné štandardy, • zjednotený reporting incidentov, • spoločný rámec pre kontrolnú a dohľadovú činnosť štátu.	prevádzkovateľov kritickej základnej služby). Povinnosti kritického subjektu pri zabezpečovaní odolnosti kritickej infraštruktúry a zabezpečovaní kontinuity poskytovania základnej služby upravuje zákon č. 367/2024 Z. z. o kritickej infraštruktúre a o zmene a doplnení niektorých zákonov, ktorého gestorom je Ministerstvo vnútra Slovenskej republiky. V schválenej Národnej stratégii odolnosti kritických subjektov (uznesenie vlády SR č. 3 z 09.01.2026) sú definované opatrenia, ktoré riešia jednotný model implementácie (napr. IS na reporting incidentov v správe MV SR, ktorý bude
--	--	--	---

				kompatibilný s JISKB, aktualizácia terminologického slovníka a pod.). V prípade aplikačných nejasností NBÚ aj MV SR vie metodicky usmerniť a ak by problémy v aplikačnej praxi pretrvávali je možné iniciovať zmenu všeobecne záväzných právnych predpisov. Pripomienkujúci subjekt súhlasil s predloženým návrhom vyhodnotenia mejlom 19.01.2026. Rozpor odstránený.
Asociácia kritickej infraštruktúry SR Asociácia kritickej infraštruktúry Slovenskej republiky	O	Celému materiálu Túto pripomienku podávame ako zásadnú: Nedostatočné ukotvenie post-kvantovej kryptografie (PQC) Odôvodnenie: Dokument len deklaratívne odkazuje na odporúčania Európskej komisie týkajúce sa prechodu na PQC, avšak neobsahuje národný migračný plán, sektorové priority, požiadavky na verejné obstarávanie, termíny, ani architektúru správy kryptografických kľúčov. Prevádzkovatelia kritickej infraštruktúry potrebujú jasné smerovanie, aby sa predišlo riziku	ČA	Pripomienku nie je možné akceptovať z dôvodu, že oblasť post-kvantovej kryptografie (PQC) bude ukotvená v samostatnom strategickom dokumente, čiže doplnením do

		tzv. „store-now-decrypt-later“ a aby prechod na PQC prebehol riadeným a koordinovaným spôsobom. Absencia konkrétnych opatrení odporuje medzinárodným odporúčaniam a oslabuje národnú bezpečnosť. Návrh AKI SR: Doplniť samostatnú kapitolu „Národný plán prechodu na PQC“, ktorá bude obsahovať: • harmonogram migrácie PQC pre sektory KI (2026–2030), • určenie kritických systémov, kde je prechod povinný, • PQC požiadavky pre verejné obstarávania, • definíciu správy kryptografických kľúčov, • požiadavky na certifikáciu PQC-ready produktov, • povinnosť uplatňovať PQC pre komunikáciu so štátom a medzi KI subjektmi.		predloženej stratégie by vznikla nadbytočná duplicita aj v súvislosti s plnením jednotlivých opatrení a ich odpočtom. Špecifiká však budú ďalej upravené v Akčnom pláne, kde budú zohľadnené a upravené aj Vaše návrhy. Akčný plán bude mať samostatný proces a každý zainteresovaný subjekt bude mať možnosť sa k nemu vyjadriť. Pripomienkujúci subjekt súhlasil s predloženým návrhom vyhodnotenia mejlom 19.01.2026. Rozpor odstránený.
Asociácia kritickej infraštruktúry SR Asociácia kritickej infraštruktúry	O	Celému materiálu Túto pripomienku podávame ako zásadnú: Absencia finančného rámca a záväzných rozpočtových indikátorov Odôvodnenie: Návrh stratégie definuje množstvo opatrení s významnými investičnými dopadmi na prevádzkovateľov kritickej	ČA	Nie je ambíciou predkladaného materiálu určovať záväzný finančný rámec. Predložená stratégia má povahu deklaratorného

Slovenskej republiky		infraštruktúry (napr. prechod na post-kvantovú kryptografiu, budovanie SOC kapacít, bezpečnostné certifikácie, modernizácia OT/IT prostredí, dodávateľské audity, implementácia AI bezpečnostných mechanizmov). Dokument však neobsahuje žiadny rámcový finančný plán, investičné odhady, časové rozdelenie ani mechanizmy spolufinancovania zo strany štátu či EÚ. Bez finančného rámca nie je možné posúdiť uskutočniteľnosť cieľov ani pripravovať investičné plány prevádzkovateľov KI. Ide o nedostatok, ktorý môže výrazne ohroziť implementáciu stratégie. Návrh AKI SR: Doplniť záväzný finančný rámec stratégie, ktorý bude obsahovať: • minimálne ročné investičné potreby podľa jednotlivých pilierov, • mechanizmus spolufinancovania investícií prevádzkovateľov KI (granty, dotácie, daňové nástroje, úvery), • záväzok vyčlenenia stabilného rozpočtu štátu na kybernetickú odolnosť, • prepojenie na európske finančné mechanizmy v období 2026–2030.	materiálu a nepresahuje všeobecne záväzný právny predpis, odráža faktický právny stav. Navrhované opatrenia, ktoré budú premietnuté do úloh v rámci Akčného plánu realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030, a budú sa týkať zmeny právneho rámca (zmeny všeobecne záväzných právnych predpisov – zákonov) sa budú týkať súčasne aj zmeny finančných rámcov k jednotlivým zákonom. Do Doložky vybraných vplyvov v časti 10. Poznámky doplnená informácia: „Financovanie v oblasti kybernetickej bezpečnosti bolo zohľadnené pri
----------------------	--	---	--

				legislatívnom procese zákona 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. Financovanie opatrení v predkladanej stratégii bude zabezpečené v rámci kapitol jednotlivých ústredných orgánov (sektorové politiky), rozpočtových opatrení pre rozpočtové organizácie, medzirezortných programov (napr. v rámci ochrany kritickej infraštruktúry je vytvorený medzirezortný rozpočtový program 0AS Ochrana kritickej
--	--	--	--	---

				infraštruktúry v SR), zdieľaných zdrojov EÚ [programy kohéznej politiky (napr. Program Slovensko), priamo riadené programy (napr. Digital Europe Programme], bilaterálnych programov SR zameraných na vedu a výskum, a iných, ktoré podporujú činnosti v oblasti vedy, výskumu a inovácií aj z oblasti bezpečnosti) a príspevkov jednotlivých prevádzkovateľov základnej služby.“. Pripomienkujúci subjekt súhlasil s predloženým návrhom vyhodnotenia mejlom 19.01.2026. Rozpor odstránený.
Asociácia kritickej infraštruktúry	O	Celému materiálu Absencia merateľných ukazovateľov (KPI) a termínov Odôvodnenie:	ČA	Predložená stratégia je východiskovým strategickým

SR Asociácia kritickej infraštruktúry Slovenskej republiky		Stratégia je prevažne deklaratívna a neobsahuje konkrétne merateľné ukazovatele výkonu ani termíny realizácie. Bez KPI nie je možné vyhodnocovať priebeh implementácie ani riadiť verejné investície. Návrh AKI SR: Doplniť sadu KPI pre každý strategický cieľ, vrátane merateľných výsledkov a termínov na roky 2026–2030.	dokumentom, ktorá nadväzuje na predchádzajúce strategické dokumenty v oblasti kybernetickej bezpečnosti a plnenie strategických cieľov v nej stanovených sa bude realizovať na základe jasne zadaných úloh, časovom harmonograme, zodpovednosti a merateľných ukazovateľov v Akčnom pláne realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030. Špecifiká budú ale ďalej upravené v Akčnom pláne, kde budú zohľadnené a upravené aj Vaše návrhy. Akčný plán bude mať samostatný proces a každý zainteresovaný subjekt
--	--	---	--

				bude mať možnosť sa k nemu vyjadriť.
Asociácia kritickej infraštruktúry SR Asociácia kritickej infraštruktúry Slovenskej republiky	O	Celému materiálu Túto pripomienku podávame ako zásadnú: Neexistujúci bezpečnostný rámec pre umelú inteligenciu v kritickej infraštruktúre Odôvodnenie: AI Act síce stanovuje pravidlá pre vysokorizikové systémy, no nerieši špecifiká prevádzky umelej inteligencie v kritickej infraštruktúre (OT/ICS/SCADA). Návrh stratégie neobsahuje žiadne bezpečnostné požiadavky, obmedzenia alebo kontrolné mechanizmy pre AI v týchto prostrediach. Chýba rámec pre AI-audit, AI-red-teaming, transparentnosť modelov, zákaz black-box systémov a mitigáciu AI-generovaných hrozieb. To predstavuje zásadné riziko pre národnú bezpečnosť. Návrh AKI SR: Doplniť bezpečnostný rámec pre AI v kritických sektoroch, ktorý bude obsahovať: • zákaz black-box AI modelov v KI bez možnosti auditu, • povinné AI-red-teaming testy, • pravidlá pre transparentnosť a vysvetliteľnosť modelov, • ochranné opatrenia proti AI-generovaným hrozbám (deepfake, spear-phishing, autonómne kódy), • požiadavky na bezpečnú integráciu AI do OT systémov.	ČA	Pripomienku nie je možné akceptovať z dôvodu absencie všeobecne záväzného právneho predpisu v oblasti umelej inteligencie na národnej úrovni. Napriek tomu, že problematika umelej inteligencie sa v mnohých oblastiach prelína v súčasnosti nie je možné ísť nad rámec kompetencií a pôsobnosti ústredných orgánov štátnej správy. V súčasnosti prebieha legislatívny proces k návrhu zákona o organizácii štátnej správy v oblasti umelej inteligencie a o zmene a doplnení niektorých zákonov (LP/2025/401). Na základe schváleného a účinného zákona bude

				možné bezpečnostný rámec pre umelú inteligenciu (aj na úseku kritickej infraštruktúry) doplniť. Špecifiká budú ale ďalej upravené v Akčnom pláne, kde budú zohľadnené a upravené aj Vaše návrhy. Akčný plán bude mať samostatný proces a každý zainteresovaný subjekt bude mať možnosť sa k nemu vyjadriť. Pripomienkujúci subjekt súhlasil s predloženým návrhom vyhodnotenia mejlom 19.01.2026. Rozpor odstránený.
Asociácia kritickej infraštruktúry SR Asociácia kritickej infraštruktúry	O	Celému materiálu Slabé prepojenie na Situačné centrum Asociácie kritickej infraštruktúry SR (SC-KI-SR) Odôvodnenie: SC-KI-SR predstavuje už existujúci projekt s významným dopadom na monitoring a ochranu kritickej infraštruktúry. Jeho úplné vynechanie zo stratégie môže viesť k duplicite národných kapacít a k neefektívnemu riadeniu zdrojov.	ČA	Pripomienka bude zohľadnená pri tvorbe Akčného plánu realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030. Zároveň je potrebné prihliadať

Slovenskej republiky		Návrh AKI SR: Doplniť do stratégie explicitnú úlohu SC-KI-SR ako súčasti národného ekosystému monitoringu a reakcie.		na zákoné rámce a úlohy stanovené v oblasti kybernetickej bezpečnosti jednotlivým ústredným orgánom. Špecifiká budú ale ďalej upravené v Akčnom pláne, kde budú zohľadnené a upravené aj Vaše návrhy. Akčný plán bude mať samostatný propces a každý zainteresovaný subjekt bude mať možnosť sa k nemu vyjadriť.
Asociácia kritickej infraštruktúry SR Asociácia kritickej infraštruktúry Slovenskej republiky	O	Celému materiálu Túto pripomienku podávame ako zásadnú: Absencia architektúry národného situačného povedomia (SOC/CSIRT/SIEM) Odôvodnenie: Stratégia deklaruje potrebu vybudovania národného systému situačného povedomia, no neobsahuje žiadny opis architektúry, štandardov, rozhraní, požiadaviek na integráciu ani modelu zdieľania údajov. Prevádzkovatelia KI tak nemajú možnosť plánovať integráciu svojich SOC alebo OT systémov. Absencia architektúry hrozí duplicitou investícií, nekompatibilitou systémov a právnou neistotou pri ochrane údajov. Návrh AKI SR: Doplniť technickú architektúru národného situačného	ČA	Vzhľadom na povahu predloženého materiálu nepovažujeme za potrebné problematiku riešiť v tomto dokumente. Národný bezpečnostný úrad v zmysle ustanovení § 7 ods. 6 zákona o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení

		povedomia, vrátane: • definície dátových tokov KI ↔ sektorové CSIRT ↔ SK-CERT ↔ štátne orgány, • jednotných API a bezpečnostných štandardov, • požiadaviek na PQC-ready komunikáciu • pravidiel pre integráciu sektorových SOC, • štandardov pre AI-asistované detekčné mechanizmy.	neskorších predpisov (ďalej len „zákon č. 69/2018 Z. z.“) pripravuje samostatný strategický dokument, ktorý určí ciele a spôsoby riadenia rozsiahlych kybernetických bezpečnostných incidentov a kybernetických kríz. Zároveň úlohy jednotky CSIRT a povinnosti toho, kto plní úlohy jednotky CSIRT, vyplývajú priamo z ustanovení zákona č. 69/2018 Z. z. (§ 15 a § 16). Povinnosti prevádzkovateľa základnej služby sú ustanovené zákonom č. 69/2018 Z. z. (okrem iných aj prijatie bezpečnostných opatrení) a akékoľvek ďalšie potreby prevádzkovateľa základnej služby sú na
--	--	--	---

				jeho individuálnom zvážení. Pripomienkujúci subjekt súhlasil s predloženým návrhom vyhodnotenia mejlom 19.01.2026. Rozpor odstránený.
BBSK Banskobystrický samosprávny kraj	Z	k celému vlastnému materiálu Zásadná pripomienka k celému vlastnému materiálu v nasledovnom znení: Stratégia sa nezaoberá kontinuitou prevádzky a obnovou po kybernetickom incidente (BCM/DRP), čo je štandardná súčasť všetkých národných kybernetických stratégií. Chýba: • rámec pre kontinuitu činností, • povinné testovanie scenárov, • prepojenie s civilnou ochranou, • prepojenie s krízovým riadením štátu. Návrh na úpravu: Doplniť kapitolu „Kybernetická krízová pripravenosť, kontinuita a obnova“. Odôvodnenie: Bez plánovania obnovy sú všetky bezpečnostné opatrenia neúplné.	ČA	Uvedené je predmetom platných bezpečnostných štandardov. Pripomienku nie je možné akceptovať aj z dôvodu, že Národný bezpečnostný úrad v súčasnosti pripravuje v súlade s § 7 ods. 6 zákona č. 69/2018 o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov strategický dokument Národný plán reakcie na zozsiahle kybernetické bezpečnostné incidenty a kybernetické krízy,

				pričom pri akceptovaní tejto pripomienky by vznikla nadbytočná duplicita. Materiál bude dostupný na pripomienkovanie. Pripomienkujúci subjekt sa k vyhodnoteniu pripomienky v stanovenom termíne nevyjadril, ani sa nezúčastnil rozporového konania (mejl 20.01.2026). Rozpor netrvá.
BBSK Banskobystrický samosprávny kraj	Z	K celého vlastnému materiálu Zásadná pripomienka k celému vlastnému materiálu v nasledovnom znení: V materiáli úplne absentuje národná analýza rizík kybernetickej bezpečnosti, ktorá má byť podľa článku 7 Smernice 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) (ďalej len „NIS2“) a § 7 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov základom pre vypracovanie Národnej stratégie kybernetickej bezpečnosti. Dokument obsahuje len všeobecný opis hrozieb, avšak	ČA	Pripomienku nie je možné akceptovať z praktického a vecne logického dôvodu, že Národný bezpečnostný úrad v súčasnosti pripravuje v súlade s § 7 ods. 6 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

	neobsahuje žiadne vyhodnotenie rizík, ich prioritizáciu, dopady, pravdepodobnosti, ani väzbu medzi rizikami a strategickými cieľmi stratégie. Rovnako chýba akýkoľvek odkaz na existujúce štátne hodnotenia rizík (napr. hodnotenie rizík kritickej infraštruktúry, správy CSIRT.SK, správy SK-CERT alebo iné vnútroštátne analýzy). Bez riadneho hodnotenia rizík nie je možné: • odôvodniť priority a opatrenia stratégie, • určiť rozsah potrebných investícií, • identifikovať najkritickejšie oblasti ohrozenia štátu, • definovať primerané a efektívne opatrenia pre verejnú správu, vrátane VÚC a obcí, • merať úspešnosť implementácie stratégie. Absencia analýzy rizík je v rozpore s princípom strategického plánovania založeného na rizikách, ktorý vyžaduje NIS2, ENISA, OECD aj medzinárodné štandardy (ISO 27005, ISO 31000). Návrh na úpravu: Žiadame doplniť do materiálu samostatnú kapitolu „Národná analýza rizík kybernetickej bezpečnosti“, ktorá bude obsahovať: • Metodiku hodnotenia rizík použité v rámci štátu (min. rámcové – aktíva, hrozby, zraniteľnosti, dopady, pravdepodobnosti). • Zhrnutie existujúcich národných rizík, vrátane ich klasifikácie podľa závažnosti. • Odkaz na existujúce vnútroštátne dokumenty, z ktorých stratégia vychádza. • Vyhodnotenie najkritickejších rizík pre verejnú správu, samosprávu, zdravotníctvo, školstvo, energetiku, dopravu a ďalšie sektory. • Väzbu medzi identifikovanými rizikami a strategickými	(ďalej len „zákon č. 69/2018 Z. z.“), v nadväznosti na čl. 9 ods. 4 smernice NIS 2, strategický dokument Národný plán reakcie na rozsiahle kybernetické bezpečnostné incidenty a kybernetické krízy, ktorý určí ciele a spôsoby rozsiahlych kybernetických bezpečnostných incidentov a kybernetických kríz. Predkladaná stratégia bola vypracovaná v súlade s § 7 ods. 2 zákona č. 69/2018 Z. z. vychádzajúc z čl. 7 smernice NIS 2 a zainteresované subjekty sa budú moci k Národnému plánu reakcie plnohodnotne vyjdiť. Materiál teda nebude chýbať, len nie je súčasťou tohto dokumentu.
--	---	---

		piliermi a cieľmi. • Prioritizáciu rizík, ktorá bude základom pre tvorbu akčného plánu. Odôvodnenie: Stratégia, ktorá neobsahuje prepojenie na národnú analýzu rizík, nie je strategickým dokumentom v zmysle požiadaviek NIS2, ale iba deklaratórnym materiálom bez analy-tic-kého základu. Pre úspešnú implementáciu kybernetickej bezpečnosti na úrovni štátu, samospráv, kritických subjektov aj celej verejnej správy je nevyhnutné, aby národná stratégia vychádzala z reálnych a vyhodnotených rizík, ktoré Slovenská republika čelí.		Pripomienkujúci subjekt sa k vyhodnoteniu pripomienky v stanovenom termíne nevyjadril, ani sa nezúčastnil rozporového konania (mejl 20.01.2026). Rozpor netrvá.
BBSK Banskobystrický samosprávny kraj	Z	K celému vlastnému materiálu Zásadná pripomienka k celému vlastnému materiálu v nasledovnom znení: Vlastný materiál neobsahuje opis architektúry riadenia kybernetickej bezpečnosti na národnej úrovni: • nie je definované prepojenie medzi SK-CERT, CSIRT.SK, sektorovými CSIRT a rezortmi, • nie je definovaná úloha samosprávy, • nie je definovaný model eskalácie incidentov, • nie je definovaná úloha Národného situačného centra, • chýba organigram a distribúcia kompetencií. Návrh na úpravu: Doplniť kapitolu „Governance model národnej kybernetickej bezpečnosti“ obsahujúcu: • Organizačnú architektúru (NBÚ → CSIRT.SK → SK-CERT → rezorty → VÚC/obce). • Kompetenčný rámec pre každý uzol. • Tok informácií pri incidente.	ČA	Máme za to, že materiál všeobecne uvedené obsahuje. Pripomíname, že všetky povinnosti a právne postavenie sú uvedené v zákone č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Stratégia nie je dokument, ktorý uvedené vzťahy môže nanovo zakladať alebo riešiť. Pripomienku nie je možné akceptovať z

		• Rámec rozhodovania v krízových situáciách. Odôvodnenie: Bez jasného riadenia nie je možné zabezpečiť konzistentnú implementáciu stratégie.	dôvodu, že stratégia má povahu deklarátneho materiálu a nepresahuje všeobecne záväzný právny predpis (zákon, vyhláška), odráža faktický právny stav. Postavenie a pôsobnosť národnej jednotky CSIRT, vládnej jednotky CSIRT, úlohy a povinnosti toho, kto plní úlohy jednotky CSIRT ustanovuje zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (§ 6, § 11, § 15 a § 16). Rovnako, pripravovaný materiál Národný plán reakcie na rozsiahle kybernetické bezpečnostné incidenty a kybernetické krízy
--	--	---	---

				bude obsahovať bližší popis reakcie na incidenty a krízy, pričom stále platí vzťah definovaný právnym predpisom. V prípade nejasností úrad poskytuje metodiky a konzultácie. Pripomienkujúci subjekt sa k vyhodnoteniu pripomienky v stanovenom termíne nevyjadril, ani sa nezúčastnil rozporového konania (mejl 20.01.2026). Rozpor netrvá.
BBSK Banskobystrický samosprávny kraj	Z	K Predkladacej správa a Doložke vybraných vplyvov Zásadná pripomienka k predkladacej správe a doložke vybraných vplyvom v nasledovnom znení: V doložke vybraných vplyvov aj v predkladacej správe sa uvádza, že materiál „nemá vplyv na rozpočet verejnej správy“. Toto je v príkrom rozpore s realitou implementácie NIS2, CRA, AI Act a s požiadavkami na kybernetickú bezpečnosť verejnej správy. Implementácia stratégie bude mať nevyhnutne rozsiahle dopady na rozpočty: • ministerstiev, • VÚC,	ČA	Stratégia má povahu deklaratórneho materiálu a nepresahuje všeobecne záväzný právny predpis, odráža faktický právny stav. Všetky povinnosti prevádzkovateľa základnej služby alebo subjekt verejnej

		• obcí, • nemocníc a zdravotníckych zariadení, • školských organizácií, • sociálnych služieb, • kultúrnych inštitúcií, • a ďalších subjektov VS. Bez vyčíslenia dopadov nie je možné zabezpečiť reálnu implementáciu stratégie. Návrh na úpravu: Doplniť kapitolu o finančných dopadoch, ktorá bude obsahovať: • Minimálne kategórie nákladov (ľudia, technológie, audit, logovanie, vzdelávanie). • Rámcový odhad finančných potrieb pre verejnú správu. • Návrh zdrojov financovania. • Osobitné opatrenia pre malé obce a organizácie s nízkou IT kapacitou. Odôvodnenie: Bez záväzného finančného rámca je stratégia neimplementovateľná a odporuje zásadám programového riadenia verejných politík.	správy, začleneného v konkrétnom sektore podľa prílohy I. alebo prílohy II. zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 69/2018 Z. z.“), sú ustanovené v zákone č. 69/2018 Z. z. vychádzajúc zo smernice NIS 2. Do Doložky vybraných vplyvov v časti 10. Poznámky doplnená informácia: „Financovanie v oblasti kybernetickej bezpečnosti bolo zohľadnené pri legislatívnom procese zákona 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. Financovanie opatrení v predkladanej stratégii bude zabezpečené v rámci kapitol jednotlivých ústredných orgánov (sektorové politiky), rozpočtových opatrení pre rozpočtové organizácie, medzirezortných programov (napr. v rámci ochrany kritickej infraštruktúry je vytvorený medzirezortný rozpočtový program 0AS Ochrana kritickej infraštruktúry v SR), zdieľaných zdrojov EÚ [programy kohéznej politiky (napr. Program Slovensko), priamo riadené
--	--	--	--	--

				programy (napr. Digital Europe Programme], bilaterálnych programov SR zameraných na vedu a výskum, a iných, ktoré podporujú činnosti v oblasti vedy, výskumu a inovácií aj z oblasti bezpečnosti) a príspevkov jednotlivých prevádzkovateľov základnej služby.“. Pripomienkujúci subjekt sa k vyhodnoteniu pripomienky v stanovenom termíne nevyjadril, ani sa nezúčastnil rozporového konania (mejl 20.01.2026). Rozpor netrvá.
BBSK Banskobystrický samosprávny kraj	O	k celému vlastnému materiálu Obyčajná pripomienka k celému vlastnému materiálu v nasledovnom znení: Pre malé obce nedosiahnuteľné. Návrh: Vytvoriť Národné SOC služby.	NEP	Nemá charakter pripomienky.

BBSK Banskobystrický samosprávny kraj	Z	k celému vlastnému materiálu Zásadná pripomienka k celému vlastnému materiálu v nasledovnom znení: Stratégia nereflektuje moderné bezpečnostné architektúry: • Zero Trust Architecture, • cloud governance, • AI Security by Design, • bezpečné identity a IAM, • segmentácia a mikrosegmentácia. Návrh na úpravu: Doplniť tieto koncepty do strategických cieľov. Odôvodnenie: Ide o základ modernej kybernetickej bezpečnosti v súlade s EÚ trendmi.	N Pripomienku nie je možné akceptovať vzhľadom na povahu materiálu. Predkladaná stratégia bola vypracovaná v súlade s § 7 ods. 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 69/2018 Z. z.“) vychádzajúc z čl. 7 smernice NIS 2. Národný bezpečnostný úrad v súčasnosti pripravuje v súlade s § 7 ods. 6 zákona č. 69/2018 Z. z. v nadväznosti na čl. 9 ods. 4 smernice NIS 2, strategický dokument Národný plán reakcie na rozsiahle kybernetické bezpečnostné incidenty a kybernetické krízy, ktorý určí ciele a
---	-----------------	--	--

				spôsoby rozsiahlych kybernetických bezpečnostných incidentov a kybernetických kríz. Pripomienkujúci subjekt sa k vyhodnoteniu pripomienky v stanovenom termíne nevyjadril, ani sa nezúčastnil rozporového konania (mejl 20.01.2026). Rozpor netrvá.
BBSK Banskobystrický samosprávny kraj	Z	k celému vlastnému materiálu Zásadná pripomienka k celému vlastnému materiálu v nasledovnom znení: Samospráva (obce a VÚC) reprezentuje viac ako polovicu informačných aktív verejného sektora. Stratégia však: • vôbec nedefinuje jej úlohy, • neidentifikuje riziká samosprávy, • nepopisuje minimálne požiadavky, • neponúka podporu pre malé obce, • neuvádza riešenia pre školy, nemocnice, sociálne služby, dopravu – všetko pod VÚC. Návrh na úpravu: Doplniť samostatnú kapitolu „Kybernetická bezpečnosť v samospráve“, vrátane:	ČA	Platí odôvodnenie uvedené aj vyššie. Pripomienku nie je možné akceptovať z dôvodu, že ide o špecifické požiadavky sektora verejná správa, v ktorom ústredným orgánom je Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky. Predložený materiál

		• Špecifických rizík pre VÚC/obce. • Modelu centrálnej podpory (shared services). • Minimálnych požiadaviek na školy, sociálne služby, nemocnice. • Návrhu centrálneho SOC/SIEM/logovania pre obce. Odôvodnenie: Najväčšie incidenty v EÚ zasiahli primárne samosprávy. Ich ignorovanie v stratégii je systémovou chybou.	má všeobecný národný charakter, preto nie je možné ustanoviť konkrétne ciele pre špecifické oblasti verejného sektora. Pripomienka bude zohľadnená pri tvorbe Akčného plánu realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030. Rovnako odporúčame sledovať aj Stratégiu kybernetickej a informačnej bezpečnosti vydávanú ústredným orgánom pre verejnú správu (MIRRI SR). Pripomienkujúci subjekt sa k vyhodnoteniu pripomienky v stanovenom termíne nevyjadril, ani sa nezúčastnil rozporového konania
--	--	---	--

				(mejl 20.01.2026). Rozpor netrvá.
BBSK Banskobystrický samosprávny kraj	Z	K celému vlastnému materiálu Zásadná pripomienka k celému vlastnému materiálu v nasledovnom znení: Vlastný materiál nijako neodkazuje na nové vykonávacie predpisy Národného bezpečnostného úradu (a to vyhlášky č. 226/2025 Z. z., ktorou sa ustanovujú podrobnosti o hláseniach v znení neskorších predpisov a vyhlášky č. 227/2025 Z. z. o bezpečnostných opatreniach v znení neskorších predpisov), ktoré definujú záväzné bezpečnostné opatrenia a povinnosti hlásenia incidentov podľa zákona č. 69/2018 o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Bez tohto prepojenia nie je jasné: • aké požiadavky musia jednotlivé rezorty splniť, • aké opatrenia musia implementovať VÚC, obce a nimi zriadené organizácie, • ako stratégia zabezpečuje zosúladenie so záväzným právom. Návrh na úpravu: Doplniť kapitolu, ktorá bude obsahovať: • Prepojenie stratégie na vyhlášku ž. 226/2025 Z. z., ktorou sa ustanovujú podrobnosti o hláseniach v znení neskorších predpisov (incidents). • Prepojenie na vyhlášku č. 227/2025 Z. z. o bezpečnostných opatreniach v znení neskorších predpisov (bezpečnostné opatrenia). • Zhrnutie povinností pre VS a samosprávu. • Harmonogram implementácie.	N	Stratégia má povahu deklarátorneho materiálu a nepresahuje všeobecne záväzný právny predpis (zákon, vyhláška), odráža faktický právny stav. Všetky povinnosti prevádzkovateľa základnej služby alebo subjekt verejnej správy, začleneného v konkrétnom sektore podľa prílohy I. alebo prílohy II. zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 69/2018 Z. z.“), sú ustanovené v zákone č. 69/2018 Z. z. a všeobecne záväzných právnych predpisov vydaných na jeho

		Odôvodnenie: Stratégia musí byť zosúladená s novými záväznými predpismi Národného bezpečnostného úradu, inak vzniká rozpor medzi povinnosťami a strategickými cieľmi.	vykonanie, čiže v súčasnosti vyhláška Národného bezpečnostného úradu č. 226/2025 Z. z., ktorou sa ustanovujú podrobnosti o hláseniach a vyhláška Národného bezpečnostného úradu č. 227/2025 Z. z. o bezpečnostných opatreniach. Časový rámec jednotlivých úlohy na plnenie opatrení v stratégii bude predmetom Akčného plánu realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030. Pripomienkujúci subjekt sa k vyhodnoteniu pripomienky v stanovenom termíne nevyjadril, ani sa nezúčastnil
--	--	---	--

				rozporového konania (mejl 20.01.2026). Rozpor netrvá.
BBSK Banskobystrický samosprávny kraj	O	K celému vlastnému materiálu Obyčajná pripomienka k celému vlastnému materiálu v nasledovnom znení: Stratégia ignoruje IAM, čo je základný pilier Zero Trust. Návrh: Doplniť povinnosť zaviesť IAM/IdP pre VS.	N	Pripomienku nie je možné akceptovať z hľadiska povahy predloženého materiálu (deklaratórny materiál, ktorý nepresahuje všeobecne záväzný právny predpis). V neposlednom rade požiadavku IAM rieši bezpečnostný štandard (vyhláška Národného bezpečnostného úradu č. 227/2025 Z. z. o bezpečnostných opatreniach, resp. Návrh vyhlášky Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej

				správy – LP/2025/610).
BBSK Banskobystrický samosprávny kraj	O	k celému vlastnému materiálu Obyčajná pripomienka k celému vlastnému materiálu v nasledovnom znení: Stratégia definuje ciele, ale žiadne indikátory úspešnosti. Návrh: Pre každý pilier doplniť minimálne 3–5 KPI.	ČA	Predložená stratégia je východiskovým strategickým dokumentom, ktorá nadväzuje na predchádzajúce strategické dokumenty v oblasti kybernetickej bezpečnosti a plnenie strategických cieľov v nej stanovených sa bude realizovať na základe jasne zadaných úloh, časovom harmonograme, zodpovednosti a merateľných ukazovateľov v Akčnom pláne realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030.
BBSK Banskobystrický samosprávny kraj	O	k celému vlastnému materiálu Obyčajná pripomienka k celému vlastnému materiálu v nasledovnom znení: Návrh: Doplniť:	A	Obsahuje na rôznych miestach.

		• rámec pre pozície, • národný vzdelávací program, • dotácie pre CISO vo VS.		
BBSK Banskobystrický samosprávny kraj	O	k celému vlastnému materiálu Obyčajná pripomienka k celému vlastnému materiálu v nasledovnom znení: Stratégia síce opisuje riziká, ale neprináša opatrenia. Návrh: Zaviesť povinnú certifikáciu dodávateľov a proces SCRM.	N	Pripomienku nie je možné akceptovať z hľadiska povahy predloženého materiálu (deklaratórny materiál, ktorý nepresahuje všeobecne záväzný právny predpis).
BBSK Banskobystrický samosprávny kraj	O	k celému vlastnému materiálu Obyčajná pripomienka k celému vlastnému materiálu v nasledovnom znení: Cloud nie je riešený vôbec. Návrh: Doplniť kapitolu „Bezpečný cloud vo verejnej správe“.	N	Predložená stratégia má povahu deklarátorneho materiálu a nepresahuje všeobecne záväzný právny predpis, odráža faktický právny stav. Je všeobecným strategickým dokumentom na národnej úrovni. Pripomienka sa viaže na špecifiká konkrétneho sektora, kde ústredným orgánom je Ministerstvo investícií, regionálneho rozvoja a

				informatizácie Slovenskej republiky.
BBSK Banskobystrický samosprávny kraj	O	k celému vlastnému materiálu Obyčajná pripomienka k celému vlastnému materiálu v nasledovnom znení: Stratégia nepoužíva kľúčové dáta ENISA, len ich všeobecne cituje.	NEP	Nemá charakter pripomienky. Predkladaná stratégia bola vypracovaná v súlade s § 7 ods. 2 zákona č. 69/2018 Z. z. vychádzajúc z čl. 7 smernice NIS 2, pričom reflektuje na právne akty EÚ, ktoré predstavujú základné regulačné východiská pre oblasť kybernetickej bezpečnosti.
GPSR Generálna prokuratúra Slovenskej republiky	O	Všeobecne - O: K vyššie uvedenému materiálu Generálna prokuratúra Slovenskej republiky neuplatňuje pripomienky.	A	
Klub 500 Klub 500	Z	K bodu IV, časti „Akčný plán“ (str. 32) Na konci navrhujeme doplniť poslednú vetu v znení: „Navrhované úlohy však nesmú neprímeraným spôsobom finančne a administratívne zaťažovať podnikateľské subjekty, ktoré boli určené ako prevádzkovatelia základných služieb alebo ako prevádzkovatelia kritických základných služieb.“. Odôvodnenie: Podnikateľské subjekty identifikované ako prevádzkovatelia	A	Doplnený text: „Navrhované opatrenia budú vychádzať z analýzy prostredia, rizík a potrieb subjektu, pričom financovanie bude prebiehať v rámci vlastných rozpočtov,

		základných služieb alebo ako prevádzkovatelia kritických základných služieb budú povinné plniť rozsiahle povinnosti a znášať finančné náklady spojené s implementáciou povinností vyplývajúcich zo zákona o kybernetickej bezpečnosti v znení jeho poslednej novely, a preto je potrebné, aby nové procesy, formy spolupráce, výmena informácií a ostatné povinnosti, ktoré môžu vyplývať z navrhovaných úloh boli realizované spôsobom, ktorý rešpektuje primeranosť, minimalizuje administratívnu a finančnú záťaž a nevytvára dodatočné povinnosti nad rámec zákonných požiadaviek. Uvedené opatrenia by preto mali byť vykonávané s dôrazom na efektívnosť, minimálne finančné a administratívne zaťaženie podnikateľských subjektov a na zachovanie rovnováhy medzi verejným záujmom a ochranou podnikateľského prostredia.	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. NBÚ 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.“. Do Doložky vybraných vplyvov v časti 10. Poznámky doplnená informácia: „Financovanie v oblasti kybernetickej bezpečnosti bolo zohľadnené pri legislatívnom procese zákona 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. Financovanie naplánovaných opatrení bude
--	--	--	--

			zabezpečené v rámci kapitol jednotlivých ústredných orgánov (sektorové politiky), rozpočtových opatrení pre rozpočtové organizácie, medzirezortných programov (napr. v rámci ochrany kritickej infraštruktúry je vytvorený medzirezortný rozpočtový program 0AS Ochrana kritickej infraštruktúry v SR), zdieľaných zdrojov EÚ [programy kohéznej politiky (napr. Program Slovensko), priamo riadené programy (napr. Digital Europe Programme], bilaterálnych programov SR zameraných na vedu a výskum, a iných, ktoré podporujú činnosti v oblasti vedy, výskumu a inovácií aj z oblasti
--	--	--	---

				bezpečnosti) a príspevkov jednotlivých prevádzkovateľov základnej služby.“. Spracovateľ odstránil rozpor s pripomienkujúcim subjektom mejlom 20.01.2026.
Klub 500 Klub 500	Z	K bodu II, časti „Kvantové technológie“ (str. 6) V druhom odseku navrhujeme za druhú vetu doplniť novú vetu v znení: „Pre súkromný sektor má prípadná realizácia opatrení prechodu na PQC odporúčací charakter.“. Odôvodnenie: Odporúčanie Európskej komisie o Pláne koordinovaného vykonávania prechodu na postkvantovú kryptografiu ako aj následne vypracovaný Koordinovaný plán vykonávania prechodu na postkvantovú kryptografiu, majú nezáväzný, odporúčací charakter a nepredstavujú právne záväzné akty EÚ. Cieľom navrhovaného doplnenia je predísť výkladovým nejasnostiam, podľa ktorých by mohli byť tieto dokumenty vnímané ako implicitne záväzné pre súkromný sektor. Zároveň sa tým sleduje snaha zabrániť vzniku neprimeranej alebo predčasnej finančnej a administratívnej záťaže pre súkromné subjekty, najmä v situácii, keď prechod na PQC môže vyžadovať významné investície do technológií, systémov a odborných kapacít.	A	Doplnený text: „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.“. Spracovateľ odstránil rozpor s
--	--	--	--

				pripomienkujúcim subjektom mejlom 20.01.2026.
MDSR Ministerstvo dopravy Slovenskej republiky	Z	kapitole VI. Strategické piliere a ciele, Pilier 1: Ochrana národného kybernetického priestoru V kapitole VI. Strategické piliere a ciele, Pilier 1: Ochrana národného kybernetického priestoru, Cieľ 1.2: Kybernetická odolnosť prevádzkovateľov základných služieb žiadame doplniť nový odsek, ktorý znie: "V súvislosti s posilnením kybernetickej bezpečnosti v sektore riadenia leteckej dopravy a bezpilotných systémov plným nasadením systému U-space a zvyšujúcou sa frekvenciou používania bezpilotných systémov je potrebné definovať záväzné bezpečnostné štandardy a metodiky pre U-space a súvisiace riadiace centrá (UTM). Tieto štandardy musia zabezpečiť: integritu a dôvernosť navigačných a identifikačných dát bezpilotných prostriedkov, kybernetickú odolnosť kritických sieťových prvkov U-space proti narušeniu dostupnosti a prevzatiu riadenia (takeover), zavedenie mechanizmov kontinuálneho monitorovania hrozieb a zraniteľností, špecifických pre bezpilotné prostriedky a ich komunikačné systémy. Odôvodnenie: Drony (bezpilotné systémy) predstavujú novú formu kritickej infraštruktúry/služby, ktorej kybernetické narušenie môže mať zásadný dopad na verejnú bezpečnosť a hospodárstvo, čo vyžaduje strategické riešenie.	ČA	Pripomienka smeruje k špecifickým sektorovým opatreniam a vzhľadom na povahu predloženého materiálu nie je možné ju plnohodnotne akceptovať. Pripomienka bude zohľadnená pri príprave Akčného plánu realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030. Súčasný text bol upravený s prihliadnutím na pripomienku Ministerstva financií Slovenskej republiky nasledujúco: „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 centrálnou určenou metodikou a vlastnou analýzou rizík s dôrazom na posilnenie kybernetickej bezpečnosti a zabezpečenie kybernetickej odolnosti.“. Pripomienkujúci subjekt súhlasil s predloženým návrhom vyhodnotenia mejlom 20.01.2026.
MFSR Ministerstvo financií	O	K vlastnému materiálu Kapitola IV Východiská, podkapitola Záväzný právny rámec (str. 13): Z formálnych dôvodov navrhujeme za slovným spojením „Nariadenie Európskeho parlamentu a Rady (EÚ)“	A	Text primerane upravený doplnením dôvetku „v platnom znení“:

Slovenskej republiky		doplniť text „2025/37 z 19. decembra 2024, ktorým sa mení nariadenie (EÚ)“.		„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.“.
MFSR Ministerstvo financií Slovenskej republiky	Z	K vlastnému materiálu Kapitola VI Strategické piliere a ciele, časť „Cieľ 1.2: Kybernetická odolnosť prevádzkovateľov základných služieb“ (str. 19): V odseku „Cieľový stav“ žiadame text prvej vety upraviť nasledovne: „Bezpečnostné štandardy sú na úrovni štátu definované a systematicky zavádzané na základe odborne vykonanej analýzy rizík štátu.“. Zároveň za prvú vetu žiadame vložiť novú vetu, ktorá znie: „Prevádzkovatelia základných služieb ich implementujú a rozvíjajú vo svojich plánoch kontinuity činností v súlade s centrálnou určenou metodikou a vlastnou analýzou rizík.“.	A	Súčasný text bol upravený aj s prihliadnutím na pripomienku Ministerstva dopravy Slovenskej republiky nasledujúco: „Bezpečnostné štandardy sú na úrovni štátu definované a systematicky

		Odôvodnenie: Pripomienka vychádza z absencie jednotného rámca plánov kontinuity na úrovni štátu a sektorovej analýzy rizík, vrátane stanovenia sektorových bezpečnostných opatrení podľa § 32 ods. 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti v znení neskorších predpisov, dôsledkom ktorého je izolované hodnotenie aktív, chýbajúci jednotný havarijný scenár, nekoordinované parametre RTO/RPO (Recovery Time Objective/Recovery Point Objective). Bez jasného pomenovania týchto systémových problémov hrozí, že implementácia stratégie nebude adresovať ich príčiny, ale iba rozšíri povinnosti koncových organizácií bez centrálnej koordinácie. Zásadným problémom v oblasti kritickej infraštruktúry je absencia sektorovej analýzy rizík a chýbajúca jednotná analýza rizík na najvyššej celoštátnej úrovni. Táto medzera v strategickom plánovaní výrazne ovplyvňuje schopnosť štátu koordinovať odolnosť svojich subjektov voči výpadkom a krízovým situáciám. Praktická aplikačná prax ukazuje, že nie je vhodné, aby si jednotlivé organizácie samostatne určovali hodnotu svojich interných aktív a na základe toho nastavovali parametre pre riadenie kontinuity činností. Takýto izolovaný prístup vedie k neobjektívnemu hodnoteniu rizík, pretože nezohľadňuje širší význam organizácie ako celku vo vzťahu k štátu. Každý subjekt verejnej správy alebo kritickej infraštruktúry by mal byť najprv identifikovaný ako aktívum štátu s vlastnou hodnotou, ktorá zahŕňa jeho funkčný, ekonomický a bezpečnostný význam. Až následne je možné objektívne vyhodnocovať jeho vnútorné aktíva v kontexte celkovej hodnoty organizácie. Tento systémový prístup umožňuje zosúladenie parametrov BCM (Business continuity management – riadenie kontinuity činností) medzi subjektmi a zabezpečuje funkčnosť	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 centrálnou určenou metodikou a vlastnou analýzou rizík s dôrazom na posilnenie kybernetickej bezpečnosti a zabezpečenie kybernetickej odolnosti.“.
--	--	--	--

		vzájomne závislých procesov. Štát pritom funguje ako jeden celok, rozdelený do viacerých právnych subjektov, ktoré sú pri aktivácii svojich plánov kontinuity často závislé od minimálne jedného iného subjektu. V dôsledku toho vzniká nesúlad v parametroch RTO, čo môže viesť k narušeniu kritických väzieb medzi organizáciami. Zásadným nedostatkom je aj absencia jednotného havarijného scenára, ktorý by si organizácie mohli premietnuť do svojich interných procesov. Ministerstvo investícií, regionálneho rozvoja a informatizácie SR síce vydalo vzorovú smernicu pre riadenie kontinuity činností, ktorá sa venuje aj kontextu RTO, avšak táto smernica zatiaľ nerieši vyššie uvedené systémové problémy. Navyše, architektúra IKT a jej financovanie sú priamo závislé od zvolenej stratégie štátu. Táto stratégia by mala vychádzať z jednotnej analýzy rizík, ktorá však na celoštátnej úrovni v súčasnosti chýba. Bez nej nie je možné efektívne plánovať, určiť priority ani zabezpečiť odolnosť štátnych systémov. Neexistencia jednotnej analýzy rizík na celoštátnej a sektorovej úrovni má nepriamy, ale zásadný dopad na štátny rozpočet Slovenskej republiky. V dôsledku absencie koordinovaného hodnotenia rizík nie je možné efektívne plánovať investície do kybernetickej bezpečnosti, infraštruktúry a personálnych kapacít. Dynamicky sa meniacia legislatíva zároveň zvyšuje technické, personálne, organizačné a procesné nároky na organizácie verejnej správy, pričom tieto požiadavky často nie sú sprevádzané primeraným finančným krytím v rámci rozpočtu SR. Výsledkom je, že štát vynakladá prostriedky reaktívne, nekoordinovane a bez jasného prepojenia na skutočné riziká, čo vedie k neefektívnemu využívaniu verejných zdrojov. Legislatívna prax v oblasti kybernetickej bezpečnosti ukazuje, že		
--	--	---	--	--

		pri prijímaní zákonov a ich novelizáciách býva v dôvodových správach často deklarovaný nulový finančný a personálny dopad na štátny rozpočet. Tento rozpor medzi legislatívnymi požiadavkami a reálnymi kapacitami organizácií vedie k systémovému podfinancovaniu a prevádzkovému napätiu, ktoré ohrozuje efektívne plnenie povinností v oblasti kybernetickej bezpečnosti. Riadenie kontinuity činností v rámci kritickej infraštruktúry na Slovensku čelí zásadným systémovým problémom, najmä v oblasti koordinácie medzi subjektmi, objektívneho hodnotenia rizík a zosúladenia parametrov obnovy (RTO/RPO). V kontexte kybernetickej bezpečnosti je tento problém obzvlášť závažný, keďže výpadky a incidenty v digitálnom prostredí majú okamžitý a často kaskádový dopad na fungovanie štátu. Súčasný stav, v ktorom si subjekty samostatne definujú hodnotu svojich aktív a nastavujú parametre BCM bez jednotného rámca, vedie k nejednotnosti a ohrozuje funkčnosť vzájomne závislých procesov. Tento nesúlad má negatívny dopad na celkovú odolnosť štátu a jeho schopnosť efektívne reagovať na kybernetické hrozby a krízové situácie.		
MFSR Ministerstvo financií Slovenskej republiky	Z	K vlastnému materiálu Kapitola VI Strategické piliere a ciele, Cieľ 2.3: Reakcia na kybernetické bezpečnostné incidenty, krízové situácie a spolupráca s justičnými orgánmi, podkapitola Cieľový stav, siedmy odsek (str. 24): Žiadame text „v problematike kyberšikany a jej prevencie.“ nahradiť textom „v problematike dezinformácií, kyberšikany a ich prevencie.“ Odôvodnenie: Úpravu textu navrhujeme za účelom zosúladenia s východiskovým stavom, kde sa uvádza „Zraniteľnou skupinou sú primárne deti, ktoré sú často vystavené kyberšikane, dezinformáciám a iným hrozbám.“	A	Text upravený aj s prihliadnutím na pripomienku Ministerstva vnútra Slovenskej republiky: „Je zavedené vzdelávanie žiakov, pedagógov, výchovných poradcov, ďalších spolupracujúcich

				odborníkov, nepedagogických zamestnancov a rodičov v problematike dezinformácií, kybernetických hrozieb a ich prevencie.“.
MFSR Ministerstvo financií Slovenskej republiky	O	K vlastnému materiálu Kapitola II Vonkajšie faktory ovplyvňujúce kybernetickú bezpečnosť, podkapitola Umelá inteligencia, produkty s digitálnymi prvkami a kybernetická bezpečnosť, ôsmy odsek (str. 7): Navrhujeme z formálnych dôvodov text „AI“ nahradiť používaným pojmom „umelá inteligencia“.	A	Text upravený v zmysle pripomienky: „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.“.
MFSR Ministerstvo financií Slovenskej republiky	O	K vlastnému materiálu Kapitola IV Východiská, podkapitola Záväzný právny rámec (str. 16): Z formálnych dôvodov navrhujeme slovné spojenie „Zákonom č. 366/2024 Z. z., ktorým sa mení a dopĺňa zákon o kybernetickej bezpečnosti“ nahradiť slovným spojením „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“.	A	Text upravený v zmysle pripomienky: „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.“.
MFSR Ministerstvo financií Slovenskej republiky	Z	K vlastnému materiálu V kapitole VI Implementačný rámec, podkapitola Financovanie (str.34) je uvedené „Aby bolo Slovensko schopné naplniť svoje predpoklady a docieľiť 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.“. Rovnako sa v danej časti dokumentu uvádza „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.“. V nadväznosti na uvedené žiadame všetky negatívne vplyvy vyvolané jednotlivými úlohami stratégie, ako aj následne pripraveného akčného plánu, zabezpečiť v rámci schválených limitov dotknutých subjektov verejnej správy na príslušné roky, čo je potrebné uviesť v doložke.	A	Do Doložky vybraných vplyvov v časti 10. Poznámky doplnená informácia: „Financovanie v oblasti kybernetickej bezpečnosti bolo zohľadnené pri legislatívnom procese zákona 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.

				Financovanie opatrení v predkladanej stratégii bude zabezpečené v rámci kapitol jednotlivých ústredných orgánov (sektorové politiky), rozpočtových opatrení pre rozpočtové organizácie, medzirezortných programov (napr. v rámci ochrany kritickej infraštruktúry je vytvorený medzirezortný rozpočtový program OAS Ochrana kritickej infraštruktúry v SR), zdieľaných zdrojov EÚ [programy kohéznej politiky (napr. Program Slovensko), priamo riadené programy (napr. Digital Europe Programme], bilaterálnych programov SR zameraných na vedu a výskum, a iných, ktoré
--	--	--	--	--

				podporujú činnosti v oblasti vedy, výskumu a inovácií aj z oblasti bezpečnosti) a príspevkov jednotlivých prevádzkovateľov základnej služby.“.
MFSR Ministerstvo financií Slovenskej republiky	O	K vlastnému materiálu Kapitola IV Východiská, podkapitola Záväzný právny rámec (str. 14): Z formálnych dôvodov navrhujeme za slovným spojením „Nariadenie Európskeho parlamentu a Rady (EÚ)“ doplniť text „2021/694“.	A	Text upravený v zmysle pripomienky s doplnením dôvetku „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.“.
MFSR Ministerstvo financií Slovenskej republiky	O	K vlastnému materiálu Kapitola VI Implementačný rámec, podkapitola Zainteresované subjekty (str. 33): Navrhujeme medzi kľúčových partnerov Národného bezpečnostného úradu doplniť aj Ministerstvo financií Slovenskej republiky z dôvodu koordinovaného finančného zabezpečenia realizácie národnej stratégie zo zdrojov rozpočtu Slovenskej republiky.	A	Text upravený primerane k pripomienke: „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).“.
MFSR Ministerstvo financií Slovenskej republiky	O	K vlastnému materiálu Kapitola VI Strategické piliere a ciele, Pilier 1: Ochrana národného kybernetického priestoru (str.18-20): Navrhujeme zväčšiť dôraz na kybernetickú odolnosť štátu/organizácií štátnej správy. Najmä z pohľadu potreby budovania kapacít pre kontinuitu služieb štátu v prípade rozsiahleho závažného kybernetického bezpečnostného incidentu (napr. pre scenáre nedostupnosť/poškodenie primárnej lokality, nedostupnosť siete internet, DDoS, kompromitácia kritických služieb štátu a pod.).	ČA	Kybernetická odolnosť štátu je vo všeobecnosti upravená v stratégii v celi 1.2 Kybernetická odolnosť prevádzkovateľov základných služieb, taktiež v nadväznosti na interakciu s ochranou kritickej infraštruktúry a posilňovaním jej odolnosti (Stratégia odolnosti kritických subjektov SR schválená uznesením vlády SR č. 3 z 09.01.2026). V neposlednom rade problematika kybernetickej odolnosti bude riešená

				národnou právnou úpravou, ktorá implementuje Akt o kybernetickej odolnosti [Cyber Resilience Act (CRA)].
MFSR Ministerstvo financií Slovenskej republiky	Z	K vlastnému materiálu Kapitola VI Strategické piliere a ciele, Cieľ 4.2: Zvyšovanie digitálnej gramotnosti občanov a bezpečnostného povedomia, Cieľový stav (str.28): Z dôvodu vecnej súvislosti žiadame v druhom odseku za text „Základné znalosti o kybernetickej bezpečnosti,“ vložiť text „hybridných hrozbách,“.	A	Text upravený v zmysle pripomienky: „Základné znalosti o kybernetickej bezpečnosti, hybridných hrozbách, umelej inteligencii a jej etických, právnych a spoločenských dôsledkoch, sú prirodzenou súčasťou všeobecného vzdelania.“.
MFSR Ministerstvo financií Slovenskej republiky	O	K vlastnému materiálu Kapitola VI Implementačný rámec (str. 32): Odporúčame slovné spojenie „VI. Implementačný rámec“ nahradiť slovným spojením „VII. Implementačný rámec“. Odôvodnenie: Kapitola č. VI sa v materiáli vyskytuje dvakrát. Žiadame upraviť číslovanie vyššie uvedenej kapitoly a následne aj celého dokumentu.	A	Text upravený v zmysle pripomienky: „VII. Implementačný rámec“.
MFSR Ministerstvo financií	O	K vlastnému materiálu Kapitola VI Strategické piliere a ciele, Cieľ 3.2: Zavádzanie bezpečných digitálnych produktov, služieb a inovácií (str. 26): Navrhujeme zaviesť potrebu legislatívnej úpravy uprednostnenia	ČA	Preferencia zavádzania certifikovaných produktov je vo všeobecnosti v

Slovenskej republiky		certifikovaných produktov a služieb v procese verejného obstarávania.		predloženej stratégii dostatočne uvedená. Pripomienka bude zohľadnená pri príprave Akčného plánu realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030.
MFSR Ministerstvo financií Slovenskej republiky	O	K vlastnému materiálu Kapitola VI Implementačný rámec, podkapitola Zainteresované subjekty (str.32): Popri dotknutých subjektoch "prevádzkovatelia základných služieb" navrhujeme špecifikovať aj subjekty "prevádzkovatelia kritických služieb kritickej infraštruktúry" ktorí sú podmnožinou prevádzkovateľov základných služieb, ale s oveľa väčším významom (a povinnosťami).	N	Pripomienku nemožno akceptovať z dôvodu, že v právnom poriadku Slovenskej republiky absentuje pojem „prevádzkovateľ/prevádzkovatelia kritických služieb kritickej infraštruktúry“. Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov vymedzuje pojmy „prevádzkovateľ základnej služby“, „kritická základná služba“. Zákon č. 367/2024 Z. z. o

				kritickej infraštruktúre a o zmene a doplnení niektorých zákonov ustanovuje pojmy „kritická infraštruktúra“, „základná služba“, „kritický subjekt“.
MIRRI SR Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky	O	K Vlastnému materiálu. Odporúčame do Piliera 2, Cieľ 2.2.: Efektívne zavádzanie bezpečnostných technológií - Východiskový stav doplniť nový odsek, ktorý znie: „Procesy riadenia zraniteľností vo verejnej správe nie sú jednotne zavedené a ich úroveň sa výrazne líši naprieč sektormi. Mnohé orgány verejnej moci riešia zraniteľnosti až v reakcii na incident, čo zvyšuje pravdepodobnosť narušenia poskytovania služieb alebo úniku údajov. Prevádzkovatelia informačných systémov verejnej správy často nemajú prehľad o aktuálnych zraniteľnostiach v používaných informačných technológiách ani o dostupných mechanizmoch na ich preverovanie a odstraňovanie. VJ-CSIRT (vládna jednotka CSIRT) pritom poskytuje bezplatné technické služby, napríklad periodické skenovanie a testovanie zraniteľností alebo penetračné testovanie, ktoré významne zlepšujú situačné povedomie a umožňujú preventívne znižovať riziká v prostredí verejnej správy.“. Odporúčame do Piliera 2, Cieľ 2.2: Efektívne zavádzanie bezpečnostných technológií - Cieľový stav doplniť nový odsek, ktorý znie: „Riadenie zraniteľností je bežnou súčasťou prevádzky informačných systémov verejnej správy a je vykonávané pravidelne a preventívne. Orgány verejnej moci majú prehľad o dostupných riešeniach a aktívne využívajú	ČA	V cieľi 2.1 časti „Východiskový stav“ doplnený odsek v nasledujúcom znení: „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

		podporu VJ-CSIRT pri odhaľovaní a odstraňovaní zraniteľností, ako aj pri overovaní bezpečnostnej úrovne svojich systémov. Tým sa zvyšuje kybernetická odolnosť štátu, znižujú sa dopady potenciálnych incidentov a efektívnejšie sa využívajú finančné prostriedky verejnej správy.“. ODÔVODNENIE: Požiadavky NIS2 ukladajú prevádzkovateľom základných služieb a poskytovateľom digitálnych služieb povinnosť nielen reagovať na kybernetické incidenty, ale aj zaviesť mechanizmy proaktívneho riadenia zraniteľností, vrátane ich pravidelnej identifikácie, hodnotenia a nápravy. Bez systematického riadenia zraniteľností hrozí zvýšené riziko veľkých incidentov, narušenia dostupnosti služieb alebo masívneho úniku dát, čo môže ohroziť kritickú infraštruktúru a dôveru verejnosti.	základných služieb často nemajú prehľad o aktuálnych zraniteľnostiach v používaných informačných technológiách, ani o dostupných mechanizmoch na ich preverovanie a odstraňovanie.“. V celi 2.1 časti „Cieľový stav“ doplnený odsek v nasledujúcom znení: „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.“. Konkrétne úlohy na znižovanie rizík v sektore verejná správa budú zohľadnené pri príprave Akčného plánu realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030.
MIRRI SR Ministerstvo investícií, regionálneho	O	K Vlastnému materiálu, kapitola VI. Strategické piliere a ciele. Odporúčame v časti Cieľ 1.1. – Východiskový stav vetu: „Malé a stredné podniky nie vždy kybernetickú bezpečnosť ako súčasť	A	Text upravený v zmysle pripomienky: „Malé a stredné podniky nie vždy

rozvoja a informatizácie Slovenskej republiky		ich zodpovedného podnikania a berú ju skôr dodatočnú finančnú záťaž, ktorej venujú obmedzené zdroje.“ preformulovať a doplniť vetu o sloveso. ODÔVODNENIE: Formálna pripomienka.		kybernetickú bezpečnosť vnímajú ako súčasť ich zodpovedného podnikania a berú ju skôr ako dodatočnú finančnú záťaž, ktorej venujú obmedzené zdroje.“.
MIRRI SR Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky	O	K Vlastnému materiálu, I. Úvod. Odporúčame v poslednej vete, v časti Úvod preformulovať znenie vety s doplnením zvratného zámena „sa“. ODÔVODNENIE: Formálna pripomienka. Odporúčame preformulovať celú vetu, alebo ju rozdeliť do dvoch samostatných viet. Uvedená formulácia nie je v tejto forme dostatočne zrozumiteľná.	A	Text upravený aj po zohľadnení pripomienky Ministerstva obrany Slovenskej republiky nasledujúco: „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.“.
MIRRI SR Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky	O	K Vlastnému materiálu, II. Vonkajšie faktory ovplyvňujúce kybernetickú bezpečnosť. Odporúčame v piatom odseku, odsek upraviť v poslednej vete doplniť koniec hranatej zátvorky za slovami „OBSE“. ODÔVODNENIE: Formálna pripomienka.	A	Text upravený v zmysle pripomienky: „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.“.
MKSR Ministerstvo kultúry Slovenskej republiky	O	K návrhu uznesenia vlády V navrhovanom bode B.3. odporúčame zväžiť zmenu termínu splnenia úlohy predložiť riaditeľovi Národného bezpečnostného úradu návrh na realizáciu opatrení v rámci kľúčových oblastí Národnej stratégie kybernetickej bezpečnosti na roky 2026 až	A	Text upravený v zmysle pripomienky nasledujúco: „B.3. predložiť riaditeľovi Národného

		2030 vo svojej pôsobnosti, ako podklad pre vypracovanie Akčného plánu realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030. Odôvodnenie: Krátky časový úsek od predpokladaného schválenia materiálu po splnenie úlohy.		bezpečnostného úradu návrh na realizáciu opatrení v rámci kľúčových oblastí Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030 vo svojej pôsobnosti, ako podklad pre vypracovanie Akčného plánu realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030 do 31. marca 2026,“.
MOSR Ministerstvo obrany Slovenskej republiky	Z	vlastnému materiálu, cieľu 5.1: Efektívna medzinárodná spolupráca, Východiskový stav K Cieľu 5.1: Efektívna medzinárodná spolupráca, Východiskový stav V texte „Východiskový stav“ v Ciele 5.1: Efektívna medzinárodná spolupráca v prvej vete žiadam za slová „kybernetická bezpečnosť“ vložiť slová „a kybernetickej obrany“. Túto pripomienku považujem za zásadnú. Odôvodnenie:	A	Text upravený v zmysle pripomienky: „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

		Zahrnutie pojmu kybernetická obrana je nevyhnutné pre komplexné pokrytie úloh štátu v kybernetickej doméne, pre zosúladenie s terminologickými a strategickými štandardami NATO a pre vytvorenie komplexného, realistického a medzinárodne kompatibilného strategického rámca. Používanie len pojmu kybernetická bezpečnosť by pokrývalo len civilnú a technickú časť problematiky, nie však obrannú, vojenskú a aliančnú dimenziu.		prostredníctvom bilaterálnych dohôd.“.
MOSR Ministerstvo obrany Slovenskej republiky	O	Posledný odsek úvodu, s. 2 Vetu Návrh strategických cieľov reaguje na vnútorné a vonkajšie faktory, ktoré v súčasnosti kybernetickú bezpečnosť ovplyvňujú, dosiahnuté výsledky z predchádzajúceho obdobia a súčasný stav kybernetickej bezpečnosti, ale aj dynamiku budúceho vývoja, či už týka vývoja bezpečnostných hrozieb, alebo technológií navrhujeme upraviť nasledovne: 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. Odôvodnenie: Gramatika a štylistika.	A	Text upravený v zmysle pripomienky: „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.“.

MOSR Ministerstvo obrany Slovenskej republiky	O	1. Odsek úvodu, s. 2 Navrhujeme prvé dve vety v úvode upraviť nasledovne: Fungovanie modernej digitálnej spoločnosti si vyžaduje dôveru v technológie a ich bezpečnosť, v čom kľúčovú úlohu zohráva štát. Odôvodnenie: Nie sme si vedomí žiadneho zákona, ktorý by ukladal štátu úlohu garanta služieb pre občanov. Slovíčko „musí“ vnímame ako žiaduci stav, nie imperatív.	A	Text upravený v zmysle pripomienky: „Fungovanie modernej digitálnej spoločnosti si vyžaduje dôveru v technológie a ich bezpečnosť, v čom kľúčovú úlohu zohráva štát.“.
MOSR Ministerstvo obrany Slovenskej republiky	O	4. odstavec, s. 4 Vo štvrtom odstavci na strane 4 odporúčame slová životný priestor pre Slovensko predstavuje predovšetkým EÚ a Organizácia Severoatlantickej zmluvy nahradiť slovami: bezpečnostné garancie pre Slovensko predstavujú predovšetkým Organizácia Severoatlantickej zmluvy (ďalej len NATO) a EÚ. Odôvodnenie: Od čias Druhej svetovej vojny sa slová životný priestor bežne v strategických dokumentoch európskych krajín nepoužívajú – majú zlú povesť. Keďže hovoríme o umiestnení SR v geopolitickom priestore a nie len čisto v kybernetickom, tak na prvom mieste by sme mali vymenovať NATO, ktoré zohráva oveľa dôležitejšiu geopolitickú úlohu než EÚ.	A	Text upravený v zmysle pripomienky: „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.“.
MOSR Ministerstvo	Z	vlastnému materiálu, k Cieľu 5.1: Efektívna medzinárodná spolupráca, Východiskový stav	A	Text upravený v zmysle pripomienky:

obrany Slovenskej republiky		K Cieľu 5.1: Efektívna medzinárodná spolupráca, Východiskový stav V texte „Východiskový stav“ v Ciele 5.1: Efektívna medzinárodná spolupráca v štvrtej vete žiadam slovo „excelentnosti“ nahradiť slovom „výnimočnosti“. Túto pripomienku považujem za zásadnú. Odôvodnenie: Výraz „výnimočnosť“ je správnym slovenským ekvivalentom pre používanie prekladu názvu NATO Centres of Excellence. Je dlhodobo používaný v oficiálnych dokumentoch Slovenskej republiky a aj v oficiálnych prekladoch NATO a zabezpečí sa tým konzistentnosť, zrozumiteľnosť a stabilita terminológie v národných a aj aliančných dokumentoch.		„Dôležitú rolu zohráva aj pôsobenie Slovenskej republiky v Centre výnimočnosti NATO pre kooperatívnu kybernetickú obranu.“.
MOSR Ministerstvo obrany Slovenskej republiky	O	4. odstavec, s. 3 V odstavci 4 na strane 3 navrhujeme slová hegemóna juhozápadnej Ázie nahradiť slovami: globálnej supervel'moci. Odôvodnenie: Ambície Číny sa neobmedzujú na rolu hegemonu niektorej z častí Ázie, ale za cieľ majú vyrovnať sa USA v roli globálneho mocenského hráča.	A	Text upravený primerane k pripomienke nasledujúco: „Čína, ktorá je nepochybne hegemonom juhozápadnej Ázie, sa postupne stáva globálnou veľmocou a jej centrálna riadená politika ovplyvňuje tiež zvyšné kontinenty sveta vrátane Európy.“.

MOSR Ministerstvo obrany Slovenskej republiky	O	Druhý odstavec, s. 4 V druhom odstavci na strane 4 vetu EÚ sa dnes preto cíti byť najviac ohrozená za uplynulé dekády navrhujeme upraviť nasledovne: Preto sa dnes EÚ cíti byť ohrozenejšia než kedykoľvek pred tým. Odôvodnenie: Keďže EÚ jestvuje len tri dekády, tak sa dá povedať, že sa cíti byť najohrozenejšia od svojho vzniku.	A	Text upravený v zmysle pripomienky: „Preto sa dnes EÚ cíti byť ohrozenejšia než kedykoľvek pred tým.“.
MOSR Ministerstvo obrany Slovenskej republiky	O	Posledný odstavec, s. 3 V poslednom odstavci na strane 3 slová že na americké vedenie sa v niektorých prípadoch na medzinárodnej scéne nemožno bezpodmienečne spoliehať navrhujeme nahradiť slovami: že miera zodpovednosti za vlastnú bezpečnosť amerických spojencov a partnerov rastie. Odôvodnenie: Diplomatickejší jazyk.	N	Ponechaný pôvodný text.
MOSR Ministerstvo obrany Slovenskej republiky	O	1. Odsek úvodu, s. 2 Vo vete A aj v tejto oblasti je kybernetická bezpečnosť zásadným a kľúčovým faktorom na dosiahnutie vysokej úrovne kvality riadenia štátu, udržanie demokratickej spoločnosti a ekonomického rastu navrhujeme nahradiť demokratickej spoločnosti slovami udržanie ústavno-právneho poriadku štátu. Odôvodnenie: Ústavno-právny poriadok je presnejší pojem, než pojem demokratická spoločnosť, ktorý je možné interpretovať rôzne.	A	Text upravený primerane k pripomienke nasledujúco: „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.“.
MOSR Ministerstvo obrany Slovenskej republiky	O	s. 3 Na strane 3 vetu Kybernetický priestor je doménou globálnej politiky a celkového bezpečnostného prostredia navrhujeme nahradiť vetou: Kybernetický priestor je doménou globálneho bezpečnostného prostredia. Odôvodnenie: Pojem globálna politika je nejasný, zatiaľ čo kybernetický priestor ako operačná doména má oporu v strategických dokumentoch NATO a jeho členských krajín.	N	Ponechaný pôvodný text.
MOSR Ministerstvo obrany Slovenskej republiky	O	1. odsek, s. 3 Vo vete 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 navrhujeme nahradiť slová polarizácia ideových skupín slovami: klesajúca vnútorná kohézia európskych spoločností. Odôvodnenie: Polarizácia ideových skupín je nejasné: nevedno, či ide o polarizáciu spoločnosti ideovými skupinami alebo o polarizáciu vnútri ideových skupín samotných.	N	Ponechaný pôvodný text.
MOSR Ministerstvo obrany Slovenskej republiky	O	Celému materiálu Všeobecne k materiálu V celom návrhu Stratégie kybernetickej bezpečnosti na roky 2026 až 2030 odporúčam zosúladiť používanie jednotného pojmu názvu štátu Slovenská republika. Túto pripomienku považujem za odporúčajúcu. Odôvodnenie:	A	Text upravený v zmysle pripomienky. Zavedený jednotný pojem názvu štátu Slovenská republika v príslušnom tvare.

		Odporúčam v celom návrhu stratégie používať jednotný názov pre Slovenskú republiku, nakoľko ide o strategický materiál ústredného orgánu štátnej správy a oficiálnym názvom štátu podľa Ústavy Slovenskej republiky je Slovenská republika. Rovnako používanie jednotnej terminológie a názvu zabezpečuje súlad so základnými právnymi predpismi. Predmetný strategický dokument reprezentuje dlhodobé záujmy štátu a používanie úplného názvu štátu podporuje vážnosť, oficiálnosť a dôveryhodnosť dokumentu.		
MOSR Ministerstvo obrany Slovenskej republiky	O	3. odsek, s. 3 V treťom odstavci na strane 3 navrhujeme pred militantnými moslimskými skupinami doplniť slová Iránom a. Odôvodnenie: Konflikt medzi Izraelom a Iránom má prvoradý strategický význam a má aj priamu medzištátnu rovinu - netýka sa len militantných skupín, ktoré Irán podporuje.	A	Text upravený v zmysle pripomienky: „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.“.

MOSR Ministerstvo obrany Slovenskej republiky	O	4. odstavec, s. 3 V odstavci 4 na strane 3 navrhujeme slová ale zároveň aj geopolitickým rivalom navrhujeme nahradiť slovami: ale zároveň aj systémovým rivalom. Odôvodnenie: Pojem systémový rival má oporu vo viacerých strategických dokumentoch NATO a EÚ. Čína a Európa sa nachádzajú na opačných koncoch zemegule a nemajú bezprostredné geografické trecie plochy.	A	Text upravený v zmysle pripomienky: „Čína je pre Európu nielen významným obchodným partnerom, ale zároveň aj systémovým rivalom.“.
MSSR Ministerstvo spravodlivosti Slovenskej republiky	O	k vlastnému materiálu K bodu VI., cieľu 1.3 K dodávateľským reťazcom odporúčame doplniť požiadavku jednotného rámca hodnotenia rizikových dodávateľov pre subjekty verejnej správy, zosúladiť hodnotenie dodávateľov s požiadavkami smernice NIS2 a zákona č. 69/2018 Z. z. (ustanovenia o zraniteľnostiach a súvisiacich notifikáciách) a zohľadniť aj špecifiká systémov prevádzkovaných prostredníctvom externých dodávateľov (Managed Services).	ČA	Vzhľadom na povahu predloženého materiálu pripomienka bude zohľadnená pri tvorbe Akčného plánu realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030.
MSSR Ministerstvo spravodlivosti Slovenskej republiky	O	k vlastnému materiálu K bodu VI., cieľu 2.3 Vzhľadom na to, že rezort spravodlivosti obhospodaruje osobitne citlivé údaje, navrhujeme doplniť osobitný dôraz na bezpečnosť justičných informačných systémov ako súčasť ochrany demokratických procesov a zvýraznenie požiadaviek na integritu elektronických služieb súdov a orgánov súdnictva. Taktiež navrhujeme doplniť, aby Národná stratégia kybernetickej bezpečnosti na roky 2026 až 2030 explicitne upravila aj postupnosť eskalácie kybernetických bezpečnostných incidentov a pravidiel krízového riadenia v súlade s požiadavkami smernice NIS2 a zákona č. 69/2018 Z. z. V dokumente absentuje presné určenie, akým spôsobom majú byť	ČA	K prvej časti pripomienky: Vzhľadom na povahu predloženého materiálu pripomienka bude zohľadnená pri tvorbe Akčného plánu realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030. K druhej časti

		incidenty hlásené sektorovému orgánu, CSIRT.SK, SK-CERT a NCKB, a aké sú podmienky prechodu od incidentu do krízovej situácie. Jasné definovanie týchto mechanizmov je nevyhnutné na zabezpečenie koordinovanej reakcie a obnovy činností v prostredí verejnej správy, najmä pri systémoch, ktorých nedostupnosť má priamy právny dopad na výkon spravodlivosti. V nadväznosti na potrebu efektívneho vyšetrovania kybernetickej kriminality odporúčame doplniť aj požiadavku na jednotnú metodiku práce s elektronickými dôkazmi, vrátane zabezpečenia integrity dôkazného materiálu a rozvoja digitálnych forenzných kapacít v spolupráci s políciou, prokuratúrou a súdmi. Zároveň odporúčame doplniť, aby stratégia počítala s pravidelným testovaním pripravenosti orgánov verejnej správy a prevádzkovateľov základných služieb formou cvičení reakcie na kybernetické incidenty. Takéto testovanie je dôležité na overenie funkčnosti procesov, rýchlosti odozvy a úrovne koordinácie medzi subjektmi. Vzhľadom na osobitný charakter rezortu spravodlivosti navrhujeme uviesť, že informačné systémy súdov, Zboru väzenskej a justičnej stráže, Obchodného registra a ďalšie kľúčové služby rezortu musia byť pri plánovaní reakcie na incidenty posudzované ako systémy s osobitnými kritériami dopadu, keďže ich nedostupnosť môže mať následky na procesné lehoty, výkon súdnictva a právnu istotu.		pripomienky: Vzhľadom na povahu predloženého materiálu pripomienka bude zohľadnená pri tvorbe Národného plánu reakcie na rozsiahle kybernetické bezpečnostné incidenty a kybernetické krízy.
MSSR Ministerstvo spravodlivosti Slovenskej republiky	O	k vlastnému materiálu K bodu VI., cieľu 2.1 Odporúčame explicitne pomenovať zodpovednosť ústredných orgánov štátnej správy za koordináciu v rámci vlastného rezortu, povinnosť zabezpečiť úplnú implementáciu zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení	ČA	Pripomienku nemožno akceptovať z dôvodu, že pôsobnosť orgánov verejnej moci na úseku kybernetickej bezpečnosti je

		niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 69/2018 Z. z.“) vrátane kategorizácie informačných služieb, analýzy rizík, auditov a incident managementu a mechanizmus sektorovej eskalácie incidentov medzi CSIRT.SK – SK-CERT – EU CyCLONe.		ustanovená zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Konkrétne úlohy a zodpovednosť ústredných orgánov (orgánov verejnej moci) a časový harmonogram na dosiahnutie strategických cieľov v priatich prioritných oblastiach predloženej stratégie budú zadefinované v Akčnom pláne realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030.
MSSR Ministerstvo spravodlivosti Slovenskej republiky	O	k vlastnému materiálu K bodu VI., cieľu 4.1 V oblasti vzdelávania odporúčame rozvíjať špecializované vzdelávacie programy pre justičné prostredie prostredníctvom externých odborných a akademických kapacít, ktoré zabezpečia obsahovú prípravu aj samotnú realizáciu vzdelávania. Ministerstvo spravodlivosti SR bude plniť koordinačnú úlohu	ČA	Vzhľadom na povahu predloženého materiálu pripomienka bude zohľadnená pri tvorbe Akčného plánu realizácie Národnej stratégie kybernetickej

		tak, aby bola zabezpečená súladnosť vzdelávacích aktivít s požiadavkami zákona č. 95/2019 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a s potrebami rezortu.“		bezpečnosti na roky 2026 až 2030.
MVSR Ministerstvo vnútra Slovenskej republiky	O	Celému materiálu V celom texte navrhujeme slovo „polícia“ nahradiť slovami „Policajný zbor“.	A	Text upravený v zmysle pripomienky. V celom texte sa slovo „polícia“ nahrádza slovami „Policajný zbor“ v príslušnom tvare.
MVSR Ministerstvo vnútra Slovenskej republiky	O	str.10 V kapitole III. časti „Vnútorne faktory ovplyvňujúce kybernetickú bezpečnosť - Stav kybernetickej bezpečnosti v Slovenskej republike“ odporúčame na konci posledného odstavca bodku nahradiť čiarkou a doplniť slová „ktorí nie sú (najmä v sektore verejná správa) dostatočne finančne ohodnotení.“. Jeho finálne znenie by bolo nasledovné: „Stále však pretrvávajú významné rozdiely v úrovni bezpečnosti medzi jednotlivými sektormi, pričom výzvou je najmä zabezpečenie požadovanej úrovne bezpečnosti v sektore verejná správa a zdravotníctvo. V oboch sektoroch spôsobuje problém aj nedostatočné finančné 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	A	Text upravený v zmysle pripomienky: „Zároveň pretrváva problém s ľudskými zdrojmi, najmä so zamestnávaním špecialistov na kybernetickú bezpečnosť, ktorí nie sú (najmä v sektore verejná správa) dostatočne finančne ohodnotení.“.

		špecialistov na kybernetickú bezpečnosť, ktorí nie sú (najmä v sektore verejná správa) dostatočne finančne ohodnotení.“		
MVSR Ministerstvo vnútra Slovenskej republiky	O	Celému materiálu Predkladaný materiál je potrebné koordinovať s Národnou koncepciou informatizácie verejnej správy. Stratégia kybernetickej bezpečnosti podporuje decentralizovaný systém riadenia, zatiaľ čo Národná koncepcia informatizácie preferuje centralizovaný prístup. Tento rozdiel je potrebné monitorovať a zabezpečiť, aby boli kompetencie v súlade s príslušnými právnymi predpismi a organizačnými zodpovednosťami. Odôvodnenie: Kým predkladaná stratégia Kybernetickej bezpečnosti podporuje (vychádzajúc z aktuálne platných právnych predpisov) decentralizovaný systém riadenia kybernetickej bezpečnosti v Slovenskej republike, Národná koncepcia informatizácie verejnej správy navrhuje silne centralizovaný prístup. Ministerstvo vnútra Slovenskej republiky plne podporuje decentralizovaný systém, kde sú kompetencie delimitované na sektorové ústredné orgány, ako je podporené aj v tejto stratégii (cieľ 2.1, kde sa uvádza, že „zodpovednosť za kybernetickú bezpečnosť je zmysluplne distribuovaná medzi Národný bezpečnostný úrad ako národnú autoritu a ústredné orgány štátnej správy, či už v pozícií sektorových autorít alebo špecifických orgánov zodpovedných za kybernetickú diplomáciu, kybernetickú obranu alebo za boj proti kybernetickej kriminalite.“).	A	Národný bezpečnostný úrad uplatňoval zásadné pripomienky k Národnej koncepcia informatizácie verejnej správy (LP/2025/546), ktorá bola vládou Slovenskej republiky schválená uznesením č. 649 zo 17. decembra 2025, pričom pripomienky Národného bezpečnostného úradu boli akceptované, resp. čiastočne akceptované.
MVSR Ministerstvo vnútra Slovenskej republiky	O	Celému materiálu Reportovanie incidentov a eskalačná procedúra pre EÚ systémy Žiadame doplniť samostatný proces pre incidenty v EÚ veľkých systémoch (SIS II/EES/ETIAS/VIS/Eurodac), ktorý zahŕňa okamžitú notifikáciu eu-LISA cez IRMA, prepojenie so	ČA	Vzhľadom na povahu predloženého materiálu bude pripomienka zohľadnená pri

		SIRENE, 24/7 dostupnosť a špecifickú klasifikáciu incidentov. Taktiež postupy pri eskalačných procedúrach, keď nastane dlhší výpadok. Stratégia musí definovať orgán zodpovedný za business continuity európskych systémov pre riadenie hraníc a justičnú spoluprácu. Navrhujeme doplniť povinnosť vykonávať pravidelné conformance testy, bezpečnostné testy a integritné audity podľa pravidiel eu-LISA.		príprave Akčného plánu realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030.
MVSR Ministerstvo vnútra Slovenskej republiky	Z	str.9 V kapitole III. časti „Vnútorne faktory ovplyvňujúce kybernetickú bezpečnosť - Stav kybernetickej bezpečnosti v Slovenskej republike“ v štvrtom odseku na konci navrhujeme vypustiť bodku a vložiť slová: „a zároveň pre verejnú správu na úseku ústredných orgánov štátnej správy je organizovaný Ministerstvom vnútra Slovenskej republiky.“ Jeho finálne znenie by bolo nasledovné: „Sektor verejnej správy, v zmysle chápania regulácie kybernetickej bezpečnosti, predstavuje významnú oblasť národného kybernetického priestoru. Tento sektor je organizovaný Ministerstvom investícií, regionálneho rozvoja a informatizácie Slovenskej republiky, v rámci ktorého pôsobí vládna jednotka CSIRT (CSIRT.SK), ktorá pre sektor verejnej správy zabezpečuje tak preventívne opatrenia, ako aj reakciu na incidenty v tomto sektore a zároveň pre verejnú správu na úseku ústredných orgánov štátnej správy je organizovaný Ministerstvom vnútra Slovenskej republiky.“ Odôvodnenie: Text uvedený v predloženom znení nie je v súlade so súčasne platnou právnou úpravou (najmä, nie však výlučne so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov). Navrhovaná úprava je nevyhnutná pre zabezpečenie zosúladenia	A	Text upravený primerane k pripomienke nasledujúco: „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

		obsahu materiálu s platnou právnou úpravou v oblasti kybernetickej bezpečnosti. Považujeme za nevyhnutné do NKSB explicitne uviesť, že sektor verejná správa na úrovni ústredných orgánov štátnej správy je organizovaný aj sektorovým ústredným orgánom, ktorým je Ministerstvo vnútra Slovenskej republiky. Ak táto skutočnosť nebude v materiáli uvedená, môže dochádzať k nesprávnej interpretácii kompetencií a k nejasnostiam pri určovaní zodpovedností v rámci sektora verejná správa. Túto pripomienku uplatňujeme ako zásadnú.		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.“.
MVSR Ministerstvo vnútra Slovenskej republiky	O	Celému materiálu Ochrana biometrických a schengenských údajov Navrhujeme stanoviť kategóriu „kritické osobné údaje EÚ systémov“ s prísnejšími bezpečnostnými požiadavkami vrátane segregácie infraštruktúry a zákazu outsourcingu mimo EÚ – hlavne pre Schengenský IS, ale aj EES, EURODAC, VIS.	N	Uvedená problematika nie je primárnou oblasťou predloženého materiálu.

MVSR Ministerstvo vnútra Slovenskej republiky	O	Celému materiálu V súčasnosti sledujeme narastajúci počet zraniteľností informačných systémov, ako aj systematickú snahu zahraničných aktérov/agentúr vyhľadávať a zneužívať tzv. 0-day zraniteľností. V NSKB však absentuje priame pomenovanie tohto problému, hľadanie riešení a systematický prístup k danej problematike. Navrhujeme preto doplniť túto oblasť ako samostatný bod, prípadne ju explicitne pomenovať a zaradiť medzi cieľové stavy v niektorom z už navrhnutých pilierov. Nejde pritom primárne o systematické skenovanie zraniteľností, ale o definovanie metód a postupov, ako odhaľovať 0-day zraniteľností, predchádzať im a v neposlednom rade aj o určenie spôsobov komunikácie s tretími stranami a dodávateľmi pri ich identifikácii a riešení.	ČA	Pripomienka bude zohľadnená pri príprave Akčného plánu realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030.
MVSR Ministerstvo vnútra Slovenskej republiky	O	Celému materiálu Bezpečnosť EU sietí (TESTA NG, VIS testa, Eurodomain) Stratégia musí obsahovať opatrenia pre ochranu medzinárodných komunikačných sietí, vrátane kryptografických zariadení, obnovy prevádzky, monitoringu a SLA požiadaviek.	ČA	Vzhľadom na povahu predloženého materiálu bude pripomienka zohľadnená pri príprave Akčného plánu realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030.
MVSR Ministerstvo vnútra Slovenskej republiky	O	Celému materiálu Európske informačné systémy – chýbajúca kategória kritických systémov Žiadame doplniť samostatnú sekciu o európskych informačných systémoch (SIS II, VIS, EES, ETIAS, Eurodac, ECRIS-TCN), ktoré predstavujú najvyššiu úroveň citlivosti údajov a majú osobitné bezpečnostné požiadavky podľa agentúry eu-LISA.	ČA	Vzhľadom na povahu predloženého materiálu bude pripomienka zohľadnená pri príprave Akčného plánu realizácie

		Súčasný návrh tieto systémy neidentifikuje, čo môže viesť k nedostatočnému riadeniu rizík. Taktiež navrhujeme doplniť povinnosť zosúladiť národnú kybernetickú bezpečnosť pre EÚ IS s požiadavkami eu-LISA (SLA, SecOP, LCSR, Incident Taxonomy, IRMA reporting). Ide o záväzné pravidlá, ktoré musia byť reflektované v strategickom dokumente.		Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030.
MVSR Ministerstvo vnútra Slovenskej republiky	O	str.12 V kapitole IV. časti „Strategicko-politický rámec“ druhom odseku navrhujeme slová „ochrany kritickej infraštruktúry“ nahradiť slovami „odolnosť kritickej infraštruktúry“ s poukazom na bod 6. Taktiež v tomto odseku navrhujeme na konci doplniť vetu, ktorá znie: „Predmetné požiadavky ďalej vo svojej pôsobnosti rozpracováva Stratégia odolnosti kritických subjektov.“. Jeho finálne znenie by bolo nasledovné: „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 incidenty väčšieho rozsahu. Stratégia tiež kladie dôraz na dosahovanie technologickej suverenity a prehĺbovanie 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.“ Odôvodnenie: Navrhovaná úprava je požadovaná z dôvodu zabezpečenia terminologickej presnosti a konzistentnosti so schváleným právnym rámcom v oblasti odolnosti kritickej infraštruktúry.	A	Text upravený v zmysle pripomienky: „Do popredia dáva najmä odolnosť kritickej infraštruktúry, rozvoj technológií a kapacít a schopnosť predchádzať, detegovať a reagovať na kybernetické bezpečnostné incidenty väčšieho rozsahu.“. Na konci odseku doplnená veta: „Predmetné požiadavky ďalej vo svojej pôsobnosti rozpracováva Stratégia odolnosti kritických subjektov Slovenskej republiky schválená uznesením vlády Slovenskej republiky č. 3 z 09.01.2026.“.

		Zároveň vzhľadom na to, že Stratégia odolnosti kritických subjektov a Národná stratégia kybernetickej bezpečnosti budú v januári 2026 predkladané na rokovanie Bezpečnostnej rady Slovenskej republiky a následne vlády Slovenskej republiky, považujeme za účelné, aby obe strategické dokumenty na seba vzájomne odkazovali. Doplnenie textu tak zabezpečí vecnú nadväznosť a zamedzí nesúladu medzi strategickými materiálmi.		
MVSR Ministerstvo vnútra Slovenskej republiky	O	str. 12 V kapitole IV. „Východiská“ časti „Závazný právny rámec“ navrhujeme doplniť medzi kľúčové právne akty nový bod „Nariadenie (EÚ) 2022/2554 zo 16. januára 2023 (Digital Operational Resilience Act – DORA)“. Odôvodnenie: Cieľom nariadenia je zabezpečiť, aby subjekty finančného sektora (napr. banky, poisťovne, investičné spoločnosti) disponovali primeranými opatreniami na prevenciu, detekciu a riešenie kybernetických útokov a prevádzkových výpadkov. Z tohto nariadenia ako aj zo zákona o kybernetickej bezpečnosti vyplýva povinnosť nahlasovať závažné IKT incidenty. V rámci implementácie hlavných bodov nariadenia DORA sa môžu vládne orgány ďalej podieľať na legislatívnych procesoch týkajúcich sa vymedzenia kritickej informačnej infraštruktúry, pričom Slovensko sa musí v oblasti finančného sektora naďalej snažiť zabezpečiť komplexné naplnenie cieľov tohto nariadenia (riadenie IKT rizík, manažment IKT incidentov, testovanie digitálnej odolnosti, atď.).	ČA	Pripomienku nemožno akceptovať v plnom rozsahu z dôvodu, že nariadenie DORA je sektorovou reguláciou a povaha predloženého dokumentu vyžaduje sektorovo neutrálne (súčasný) znenie.
MVSR Ministerstvo vnútra Slovenskej republiky	O	str. 17 V kapitole VI. Pilier 1 Cieľ 1.1: „Ochrana občanov, malých a stredných podnikateľov a podnikov“ v časti „Východiskový stav“ navrhujeme upraviť vetu „Malé a stredné podniky nie vždy	A	Text upravený v zmysle pripomienky: „Malé a stredné podniky nie vždy

		kybernetickú bezpečnosť ako súčasť ich zodpovedného podnikania a berú ju skôr dodatočnú finančnú záťaž, ktorej venujú obmedzené zdroje.“. Uvedené znenie nedáva zmysel a je potrebné ho preformulovať (absentuje prísudok).		kybernetickú bezpečnosť vnímajú ako súčasť ich zodpovedného podnikania a berú ju skôr dodatočnú finančnú záťaž, ktorej venujú obmedzené zdroje.“.
MVSR Ministerstvo vnútra Slovenskej republiky	O	str. 22 V kapitole VI. Pilier 2 Cieľ 2.3: „Reakcia na kybernetické bezpečnostné incidenty, krízové situácie a spolupráca s justičnými orgánmi“ navrhujeme v prvom odseku za vetu „Nie sú interne zavedené manuály vzhľadom na závažnosť alebo rozsah kybernetického bezpečnostného incidentu.“ vložiť vetu „Proces riešenia kybernetických bezpečnostných incidentov je v dôsledku organizačných, technických a ľudských faktorov zdĺhavý.“. Odôvodnenie: Uvedenie nedostatku v rýchlosti procesov riešenia a vyšetrovania kybernetických bezpečnostných incidentov je žiadúce, nakoľko cieľom národnej stratégie by malo byť aj tento stav zmeniť, pretože rýchle a efektívne riešenie takýchto incidentov je možné dosiahnuť (napr. zavedením pravidelných cvičení v praxi a overovaním pripravenosti na kybernetické útoky). Na navrhované doplnenie textu reaguje aj text už uvedený v časti Cieľový stav (strana 27, Budovanie národných znalostných kapacít a vzdelávanie).	A	Textu upravený v zmysle pripomienky. Vložená veta: „Proces riešenia kybernetických bezpečnostných incidentov je v dôsledku organizačných, technických a ľudských faktorov zdĺhavý.“.
MVSR Ministerstvo	O	str. 9 V kapitole III. časti „Vnútorne faktory ovplyvňujúce kybernetickú bezpečnosť – Stav kybernetickej bezpečnosti v	A	Text upravený v zmysle pripomienky: „Hierarchické

vnútra Slovenskej republiky		Slovenskej republike“ odporúčame v prvej vete tretieho odseku doplniť na záver vety „Hierarchické usporiadanie riadenia kybernetickej bezpečnosti zastrešuje Národný bezpečnostný úrad ako samostatný ústredný orgán štátnej správy pre oblasť kybernetickej.“ doplniť slovo „bezpečnosti.“.		usporiadanie riadenia kybernetickej bezpečnosti zastrešuje Národný bezpečnostný úrad ako samostatný ústredný orgán štátnej správy pre oblasť kybernetickej bezpečnosti.“.
MVSR Ministerstvo vnútra Slovenskej republiky	O	Celému materiálu Interoperabilita EÚ databáz Stratégia by mala reflektovať pôsobenie SR v rámci EÚ prichádzajúcej interoperability (CIR, sBMS, MID, ESP) a doplniť súvisiace bezpečnostné požiadavky.	N	Uvedená problematika nie je primárnou oblasťou predloženého materiálu.
MVSR Ministerstvo vnútra Slovenskej republiky	O	str. 24 V kapitole VI. Pilier 2 Cieľ 2.3: „Reakcia na kybernetické bezpečnostné incidenty, krízové situácie a spolupráca s justičnými orgánmi“ časť „Cieľový stav“ (str. 24 vlastného materiálu) navrhujeme v šiestom odseku text „Polícia má personálne posilnené špecializované útvary na boj proti kyberterorizmu a kyberšpionáži.“ nahradiť textom „Policajný zbor má personálne posilnené špecializované útvary na boj proti trestným činom spáchaným v kyberpriestore“. Odôvodnenie: Policajný zbor nemá legislatívne oprávnenie na vykonávanie boja proti kyberšpionáži. Policajný zbor vykonáva vyšetrovanie trestných činov a nezaoberá sa vyšetrovaním kybernetických incidentov, ak nebola naplnená skutková podstata niektorého z trestných činov uvedených v Trestnom zákone.	A	Text upravený v zmysle pripomienky: „Policajný zbor má personálne posilnené špecializované útvary na boj proti trestným činom spáchaným v kyberpriestore.“.
MVSR Ministerstvo	O	str.22 V kapitole VI. Pilier 2 Cieľ 2.3: „Reakcia na kybernetické	A	Názov cieľa upravený v zmysle pripomienky:

vnútra Slovenskej republiky		bezpečnostné incidenty, krízové situácie a spolupráca s justičnými orgánmi“ navrhujeme názov cieľa „Reakcia na kybernetické bezpečnostné incidenty, krízové situácie a spolupráca s justičnými orgánmi“ nahradiť novým názvom, a to: „Reakcia na kybernetické bezpečnostné incidenty, kybernetické krízy a situácie a spolupráca s justičnými orgánmi“. Odôvodnenie: Zmenu názvu cieľa požadujeme z dôvodu, že pojem „krízová situácia“ inklinuje k § 2 písm. a) zákona č. 387/2002 Z.z. o riadení štátu v krízových situáciách mimo času vojny a vojnového stavu v znení neskorších predpisov, podľa ktorého nie sú úplne harmonizované legislatívne požiadavky. Vhodnejším pojmom pre účely materiálu je pojem „kybernetické krízy“ v zmysle § 3 písm. l) zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.		„Cieľ 2.3: Reakcia na kybernetické bezpečnostné incidenty, kybernetické krízy a spolupráca s justičnými orgánmi“.
MVSR Ministerstvo vnútra Slovenskej republiky	O	str. 22 V kapitole VI. Pilier 2 Cieľ 2.3: „Reakcia na kybernetické bezpečnostné incidenty, krízové situácie a spolupráca s justičnými orgánmi“ navrhujeme v prvom odseku za vetu „Polícia a justičné orgány nie sú prispôsobené a vybavené na efektívne odhaľovanie a vyšetrovanie kybernetickej kriminality.“ vložiť vetu „Pretrvávajú rozdiely v postupoch pri získavaní a zaisťovaní digitálnych dôkazov, čo je spôsobené faktormi ako sú rôzna vnútroštátna právna legislatíva, technologická zložitosť, problém teritoriality, komplikovaná jurisdikcia, nejednotnosť celoeurópskych štandardov pre nástroje a metodiky používané k získaniu, zaisteniu, analýze a uchovávaní digitálnych dôkazov a nedostatok špecializovaných školení pre políciu a justičné orgány.“. Odôvodnenie:	A	Textu upravený v zmysle pripomienky. Vložená veta: „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,

		Uvedenie problematiky získavania a zaist'ovania digitálnych dôkazov pokladáme za náležité, nakoľko práve digitálne dôkazy sú kľúčové a podstatné v boji proti kybernetickej kriminalite, pričom sa často jedná o jediné dostupné dôkazy. Táto problematika pretrváva a tvorí prekážku v efektívnom stíhaní kybernetickej kriminality. Na navrhované doplnenie textu reaguje aj text už uvedený v časti Cieľový stav (strana 24).		nejednotnosť celoeurópskych štandardov pre nástroje a metodiky používané k získaniu, zaisteniu, analýze a uchovávaní digitálnych dôkazov a nedostatok špecializovaných školení pre Policajný zbor a justičné orgány.“.
MVSR Ministerstvo vnútra Slovenskej republiky	O	str. 7 V kapitole II. časti „Technologické trendy a globalizácia dodávateľských reťazcov – Umelá inteligencia, produkty s digitálnymi prvkami a kybernetická bezpečnosť“ odporúčame na konci predposledného odstavca doplniť text, ktorý znie: „V súvislosti s hybridnými hrozbami, s odvolaním sa na AI False Claim monitor z augusta 2025 spracovaný spoločnosťou NewsGuard (https://www.newsguardtech.com/ai-monitor/august-2025-ai-false-claim-monitor/), problematiku zneužitia AI nepriateľskými aktérmi cieleným zaplavovaním online prostredia obsahom nielen s cieľom ovplyvniť používateľov priamo, ale aj LLM modely, ktoré z dôvodu snahy o poskytnutie uspokojivej odpovede tieto príspevky citujú, legitimizujú a ďalej rozširujú. NewsGuard v tomto prípade na základe ročného sledovania hovorí o systémovom probléme s AI, ktorá v snahe rýchlo a uspokojivo odpovedať môže uprednostňovať rýchlu reakciu pred presnosťou, čo zvyšuje riziko postupnej erózie informačného prostredia.“.	N	Ponechaný pôvodný text.

MVSR Ministerstvo vnútra Slovenskej republiky	O	str. 22 V kapitole VI. Pilier 2 Cieľ 2.3: „Reakcia na kybernetické bezpečnostné incidenty, krízové situácie a spolupráca s justičnými orgánmi“ navrhujeme v celom texte slovo „kyberšikana“ nahradiť všeobecnejším nadradeným pojmom, napríklad „kybernetické hrozby“. Odôvodnenie: Pojem „kyberšikana“ predstavuje len úzky segment neželaných aktivít v kybernetickom priestore. Použitý pojem „kyberšikana“ nemá jednotnú právnu definíciu, nie je zakotvený v zákone o kybernetickej bezpečnosti, ani v Trestnom zákone. Strategický dokument celonárodného charakteru by mal pokrývať aj ďalšie kategórie protiprávných a škodlivých kybernetických javov, resp. iné formy sociálneho inžinierstva. Použitie pojmu, ktorý má užší význam, môže byť v takomto strategickom dokumente hodnotené ako vecne nesprávne a legislatívne nepresné. Uvedená úprava zabezpečí širší vecný záber dokumentu a jeho udržateľnosť vzhľadom na jeho dlhodobý charakter.	A Text upravený v zmysle pripomienky: - v časti „Východiskový stav“: „Zraniteľnou skupinou sú primárne deti, ktoré sú často vystavené dezinformáciám a kybernetickým hrozbám.“; - v časti „Cieľový stav“ (aj s prihliadnutím na pripomienku Ministerstva financií Slovenskej republiky): „Je zavedené vzdelávanie žiakov, pedagógov, výchovných poradcov, ďalších spolupracujúcich odborníkov, nepedagogických zamestnancov a rodičov v problematike dezinformácií, kybernetických hrozieb a ich prevencie.“.
---	----------	---	--

MVSR Ministerstvo vnútra Slovenskej republiky	O	str. 18 V kapitole VI. Pilier 1 Cieľ 1.2: „Kybernetická odolnosť prevádzkovateľov základných služieb“ v časti „Cieľový stav“ piamom odseku navrhujeme slová „so systémom ochrany kritickej infraštruktúry“ nahradiť slovami „s odolnosťou kritickej infraštruktúry“. Jeho finálne znenie by bolo nasledovné: „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.“ Odôvodnenie: Navrhovaná zmena je nevyhnutná z dôvodu terminologického zosúladenia so smernicou CER, v zmysle ktorej bol pojem „ochrana kritickej infraštruktúry“ nahradený pojmom „odolnosť kritických subjektov“. Tento prístup bol transponovaný do právneho poriadku Slovenskej republiky zákonom č. 367/2024 Z. z. o kritickej infraštruktúre a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, ktorý v § 2 písm. d) ustanovuje pojem „odolnosť kritickej infraštruktúry“. Používanie pôvodnej terminológie by v strategickom dokumente spôsobovalo nesúlad s platnou legislatívou a mohlo by viesť k nepresnej interpretácii kompetencií a úloh. Terminologicky správne by bolo odkazovať sa na odolnosť kritickej infraštruktúry alebo na zabezpečenie odolnosti kritickej infraštruktúry.	A	Text upravený v zmysle pripomienky: „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.“.
MZVEZ SR Ministerstvo zahraničných	O	vlastnému materiálu, časti III. Vnútorne faktory ovplyvňujúce kybernetickú bezpečnosť Vo vlastnom materiáli, časti III. v texte pod podnadvpisom Stav	N	Ponechaný pôvodný text.

vecí a európskych záležitostí Slovenskej republiky		kybernetickej bezpečnosti v Slovenskej republike na str. 10 odporúčame vo vete „Problém s nedostatkom disponibilných zdrojov na investície čiastočne nahrádzajú grantové programy EÚ, ktoré je však možné čerpať iba na vopred definované účely.“ Vložiť za slovo „účely“ slová „a nezabezpečujú trvalú alebo dlhodobú udržateľnosť projektov vzhľadom k vysokým licenčným poplatkom, ktoré nie je možné pokrývať z týchto programov.“. Odôvodnenie: Považujeme za potrebné poukázať na problém s vysokými licenčnými poplatkami, ktoré nie je možné hradit' z grantových programov EÚ, čím je ohrozená dlhodobá udržateľnosť projektov.		
MZVEZ SR Ministerstvo zahraničných vecí a európskych záležitostí Slovenskej republiky	O	vlastnému materiálu, časti III. Vnútorne faktory ovplyvňujúce kybernetickú bezpečnosť Vo vlastnom materiáli, časti III. v texte pod podnadpisom Stav kybernetickej bezpečnosti v Slovenskej republike na str. 9 odporúčame doplniť chýbajúce slovo na konci vety „Hierarchické usporiadanie riadenia kybernetickej bezpečnosti zastrešuje Národný bezpečnostný úrad ako samostatný ústredný orgán štátnej správy pre oblasť kybernetickej.“. Odôvodnenie: Gramatická pripomienka.	A	Text upravený v zmysle pripomienky: „Hierarchické usporiadanie riadenia kybernetickej bezpečnosti zastrešuje Národný bezpečnostný úrad ako samostatný ústredný orgán štátnej správy pre oblasť kybernetickej bezpečnosti.“.
MŠVVaMSR Ministerstvo školstva, výskumu, vývoja a mládeže	O	Pilier 5: Strategické partnerstvá a medzinárodná spolupráca Jasné kompetenčné matice (RACI) Návrh: Pri outsourcingu služieb vyžadovať presné vymedzenie zodpovedností medzi štátom (garant bezpečnosti) a súkromným dodávateľom (prevádzka), ako je to definované v projekte DigiNET.	ČA	Vzhľadom na povahu predloženého materiálu bude pripomienka zohľadnená pri príprave Akčného

Slovenskej republiky		Cieľ 2.1: Integrovaná architektúra riadenia kybernetickej bezpečnosti časť Cieľový stav. Konkrétne k bodu: „Sú jasne stanovené a ohraničené kompetencie jednotlivých orgánov“ a k distribúcii zodpovednosti.		plánu realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030.
MŠVVaMSR Ministerstvo školstva, výskumu, vývoja a mládeže Slovenskej republiky	O	Pilier 4: Vzdelávanie, zručnosti a povedomie Rola digitálneho koordinátora Návrh: Formalizovať rolu koordinátora na koncových bodoch (napr. v školách), ktorý slúži ako predĺžená ruka sektorového SOC pri riešení incidentov. Cieľ 4.1: Budovanie národných znalostných kapacít a vzdelávanie časť Cieľový stav. Doplniť k časti o príprave kvalifikovaných odborníkov naprieč profesiami.	ČA	Vzhľadom na povahu predloženého materiálu bude pripomienka zohľadnená pri príprave Akčného plánu realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030.
MŠVVaMSR Ministerstvo školstva, výskumu, vývoja a mládeže Slovenskej republiky	O	Kapitola Technologické trendy a globalizácia dodávateľských reťazcov, s. 5 V kapitole absentuje trend masívneho využívania dronov v stále vyššej miere autonómnosti a miere využívania bežne dostupných komponentov. Má to dopad na plánovanie kontinuity činnosti štátu, kritickej infraštruktúry aj jednotlivých OVM.	NEP	Nemá charakter pripomienky.
MŠVVaMSR Ministerstvo školstva, výskumu, vývoja a mládeže Slovenskej republiky	O	Pilier 3: Bezpečné a inovatívne digitálne produkty a služby Bezpečnosť dodávateľského reťazca Návrh: Zaviesť prísne pravidlá pre riadenie životného cyklu hardvéru a softvéru. Zariadenia bez garantovanej podpory výrobcu a bezpečnostných záplat (EoL/EoS) nesmú byť súčasťou kritickej infraštruktúry. Cieľ 1.3: Bezpečnosť dodávateľských reťazcov časť Cieľový stav. Doplniť k bodu o posudzovaní rizík z dodávateľských	N	Vzhľadom na povahu predloženého materiálu ponechaný pôvodný text.

		reťazcov alebo do Cieľa 3.1 (Životný cyklus produktov) k požiadavke na uplatňovanie primeranej bezpečnosti počas celého životného cyklu.		
MŠVVaMSR Ministerstvo škola, výskumu , vývoja a mládeže Slovenskej republiky	O	Kapitola Stav kybernetickej bezpečnosti v Slovenskej republike, str. 11. Text „Stále však pretrvávajú významné rozdiely v úrovni bezpečnosti medzi jednotlivými sektormi, pričom výzvou je najmä zabezpečenie požadovanej úrovne bezpečnosti v sektore verejná správa a zdravotníctvo. V oboch sektoroch spôsobuje problém aj nedostatočné finančné 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.“ Navrhujeme upraviť na: „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 oboch týchto sektoroch spôsobuje problém aj nedostatočné finančné 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.“.	A	Text upravený v zmysle pripomienky: „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 finančné krytie nákladov na kybernetickú bezpečnosť.“.
MŠVVaMSR Ministerstvo škola, výskumu , vývoja a mládeže	O	Pilier 1: Ochrana národného kybernetického priestoru Viacvrstvá ochrana pred DDoS Návrh: Stratégia by mala vyžadovať ochranu proti volumetrickým útokom už na úrovni poskytovateľa centrálnych služieb, nie až na koncových bodoch.	N	Vzhľadom na povahu predloženého materiálu ponechaný pôvodný text.

Slovenskej republiky		Cieľ 1.2: Kybernetická odolnosť prevádzkovateľov základných služieb časť Cieľový stav. Vhodné doplniť k požiadavke na „účinnosť bezpečnostných mechanizmov“		
MŠVVaMSR Ministerstvo školstva, výskumu, vývoja a mládeže Slovenskej republiky	O	Pilier 3: Bezpečné a inovatívne digitálne produkty a služby Centralizovaný manažment Návrh: Podporovať obstarávanie technológií s otvoreným API, ktoré umožňujú centrálnu správu, auditovateľnosť zmien a jednotný dohľad nad tisíckami zariadení (model CRSD). Cieľ 2.1: Integrovaná architektúra riadenia kybernetickej bezpečnosti. Konkrétne k požiadavke na integrované a systematicky koordinované riadenie.	N	Vzhľadom na povahu predloženého materiálu ponechaný pôvodný text.
MŠVVaMSR Ministerstvo školstva, výskumu, vývoja a mládeže Slovenskej republiky	O	Kapitola Umelá inteligencia, produkty s digitálnymi prvkami a kybernetická bezpečnosť, str. 6. 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) prináša nový druh hodnotenia rizík v kybernetickom priestore (FRIA – Fundamental Rights Impact Assessment), ktorý je za rámcom štandardného posudzovania kybernetických rizík. Komplexné posudzovanie rizík v kybernetickom priestore aktuálne zahŕňa požiadavky legislatívy KB, ITVS, GDPR a AI, v prípade finančných inštitúcií aj DORA.	NEP	Nemá charakter pripomienky.
MŠVVaMSR Ministerstvo školstva, výskumu, vývoja a mládeže Slovenskej republiky	O	Kapitola Stav kybernetickej bezpečnosti v Slovenskej republike, str. 11. Súčasťou aktuálneho stavu je aj istá dualita riadenia kybernetickej bezpečnosti verejnej správy (legislatíva a kompetencie NBÚ a MIRRI nie sú v plnom súlade), ktorej legislatívny rámec nie je v plnom vzájomnom súlade (napr. ako realizovať analýzu rizík).	NEP	Nemá charakter pripomienky.
MŠVVaMSR Ministerstvo	O	Kapitola „Právny rámec“, str. 14. Absentuje oblasť ochrany osobných údajov (GDPR), ktorá je	NEP	Nemá charakter pripomienky.

škola, výskumu , vývoja a mládeže Slovenskej republiky		úzko prepojená s KB a bez KB nie je možné zabezpečiť požiadavky GDPR (viď článok 32).		
MŠVVaMR Ministerstvo škola, výskumu , vývoja a mládeže Slovenskej republiky	Z	Kapitola Pilier I Absentuje cieľ: Ochrana mládeže v kybernetickom priestore, ktorý je relatívne samostatný oproti cieľu 1.1 Pritom tento cieľ sa už objavuje v samostatných strategických dokumentoch na úrovni EÚ. Vid' napr. Communication from the Commission – Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065 https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors	A	Vzhľadom na povahu predloženého materiálu možno konštatovať, že predmetnou problematikou sa materiál zaoberá v zodpovedajúcej miere. V rámci cieľa 4.2 je v časti „Cieľový stav“ na konci druhého odseku doplnená veta: „Systematická ochrana detí, žiakov a mládeže v kybernetickom priestore je zabezpečená.“. Národný bezpečnostný úrad zaraďuje ochranu najzraniteľnejších skupín v kybernetickom priestore medzi svoje prioritné záujmy a pripomienka bude

				d ďalej zohľadnená pri príprave Akčného plánu realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030.
MŠVVaMSR Ministerstvo školstva, výskumu, vývoja a mládeže Slovenskej republiky	O	Pilier 1: Ochrana národného kybernetického priestoru Zero Trust a segmentácia Návrh: Zaviesť požiadavku na identitne riadený prístup do sietí (napr. štandard 802.1x), kde sa prístup prideľuje na základe digitálnej identity používateľa, nie len fyzického pripojenia. Cieľ 3.2: Zavádzanie bezpečných digitálnych produktov, služieb a inovácií časť Cieľový stav. Tento cieľ už explicitne spomína „uplatnenie tzv. zero-trust prístupov (riadenie prístupov, segmentácia)“. Odporúčam tento bod v texte zvýrazniť alebo rozšíriť o požiadavku na dynamické riadenie prístupu (NAC).	N	Vzhľadom na povahu predloženého materiálu ponechaný pôvodný text.
MŠVVaMSR Ministerstvo školstva, výskumu, vývoja a mládeže Slovenskej republiky	O	Pilier 4: Vzdelávanie, zručnosti a povedomie Ochrana pred škodlivým obsahom Návrh: Explicitne spomenúť potrebu centrálného filtrovania nevhodného obsahu na úrovni štátnej infraštruktúry (školy), doplnenú o edukáciu používateľov. Cieľ 1.1: Ochrana občanov, malých a stredných podnikateľov a podnikov časť Cieľový stav. Doplniť k bodu o podpore nástrojov na ochranu pred hrozbami.	A	Národný bezpečnostný úrad zaraďuje ochranu najzraniteľnejších skupín v kybernetickom priestore medzi svoje prioritné záujmy a pripomienka bude ďalej zohľadnená pri príprave Akčného plánu realizácie Národnej stratégie kybernetickej bezpečnosti na roky

				2026 až 2030, resp. pri príprave ďalších legislatívnych a nelegislatívnych materiálov.
MŠVVaMSR Ministerstvo školstva, výskumu, vývoja a mládeže Slovenskej republiky	O	Pilier 2: Budovanie národných kapacít v oblasti kybernetickej bezpečnosti Sektorové bezpečnostné operačné centrá (SOC) Návrh: Definovať vznik sektorových SOC (ako je NCU SOC), ktoré budú proaktívne monitorovať tisíce koncových bodov, vykonávať triage alertov a reagovať na incidenty v spolupráci s národným SK-CERT. Cieľ 2.1: Integrovaná architektúra riadenia kybernetickej bezpečnosti časť Cieľový stav. Konkrétne k bodu o vybudovaní optimalizovanej a integrovanej architektúry vo verejnom sektore a k systému detekcie hrozieb. Prípadne prepojiť s Cieľom 2.3 (Reakcia na incidenty).	N	Vzhľadom na povahu predloženého materiálu ponechaný pôvodný text.
MŠVVaMSR Ministerstvo školstva, výskumu, vývoja a mládeže Slovenskej republiky	O	Kapitola: Umelá inteligencia, produkty s digitálnymi prvkami a kybernetická bezpečnosť - na koniec, alebo do samostatného doplniť pripomienku – Upozornenie na zraniteľnosť žiakov v kontexte umelej inteligencie. V kapitole venovanej umelej inteligencii odporúčame doplniť, že žiaci, deti a mládež predstavujú najzraniteľnejšiu skupinu vo vzťahu k rizikám spojeným s využívaním AI technológií. Je potrebné explicitne uviesť, že zavádzanie AI do vzdelávacieho procesu a digitálneho prostredia musí byť sprevádzané špecifickými bezpečnostnými a etickými opatreniami, ktoré zohľadnia ich ochranu pred manipuláciou, dezinformáciami, zneužitím údajov a ďalšími hrozbami.	A	Vzhľadom na povahu predloženého materiálu možno konštatovať, že predmetnou problematikou sa materiál zaoberá v zodpovedajúcej miere. V rámci cieľa 4.2 je v časti „Cieľový stav“ na konci tretieho odseku doplnená veta: „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.“. Národný bezpečnostný úrad zaraďuje ochranu najzraniteľnejších skupín v kybernetickom priestore medzi svoje prioritné záujmy a pripomienka bude ďalej zohľadnená pri príprave ďalších legislatívnych a nelegislatívnych materiálov.
--	--	--	---

MŠVVaMSR Ministerstvo školy, výskumu , vývoja a mládeže Slovenskej republiky	Z	k pilier 1, cieľ 1.1, str. 16 a/alebo k pilier 4, cieľ 4.2 Bezpečnosť žiakov, detí a mládeže v kybernetickom priestore. V návrhu stratégie odporúčame explicitne posilniť dôraz na systematické riešenie bezpečnosti žiakov, detí a mládeže v kybernetickom priestore. Táto skupina patrí medzi najzraniteľnejšie, pričom čelí špecifickým rizikám, ako sú kyberšikana, manipulácia, zneužívanie osobných údajov či vystavenie škodlivému obsahu.	A Vzhľadom na povahu predloženého materiálu možno konštatovať, že predmetnou problematikou sa materiál zaoberá v zodpovedajúcej miere. V rámci cieľa 4.2 je v časti „Cieľový stav“ na konci druhého odseku doplnená veta: „Systematická ochrana detí, žiakov a mládeže v kybernetickom priestore je zabezpečená.“. Národný bezpečnostný úrad zaraďuje ochranu najzraniteľnejších skupín v kybernetickom priestore medzi svoje prioritné záujmy a pripomienka bude ďalej zohľadnená pri príprave Akčného plánu realizácie Národnej stratégie kybernetickej
--	-----------------	---	---

				bezpečnosti na roky 2026 až 2030.
MŠVVaMSR Ministerstvo školsťva,výskumu ,vývoja a mládeže Slovenskej republiky	O	Pilier 1: Ochrana národného kybernetického priestoru Centralizácia bezpečnostných brán Návrh: Odporúčam stanoviť ako štandard budovanie sektorových centrálnych uzlov (podľa vzoru národného centrálného uzla, ďalej len NCU, súčasti projektu DigiEDU), ktoré poskytujú „dáždnikovú ochranu“ pre podriadené organizácie. Tým sa zabezpečí unifikované nasadenie centrálnych firewallov, IDS/IPS systémov a SSL inšpekcie. Cieľ 1.2: Kybernetická odolnosť prevádzkovateľov základných služieb časť Cieľový stav. Konkrétne doplniť do odseku, ktorý hovorí o tom, že „Systém kybernetickej bezpečnosti interaguje so systémom ochrany kritickej infraštruktúry“, alebo do časti o nasadzovaní produktov zaručujúcich vysokú odolnosť.	N	Vzhľadom na povahu predloženého materiálu ponechaný pôvodný text.
MŠVVaMSR Ministerstvo školsťva,výskumu ,vývoja a mládeže Slovenskej republiky	O	Pilier 2: Budovanie národných kapacít v oblasti kybernetickej bezpečnosti Automatizácia bezpečnosti Návrh: Zdôrazniť potrebu automatizácie (napr. Zero Touch Provisioning, SOAR) pre zvládnutie bezpečnosti v prostredí s nedostatkom lokálnych IT špecialistov. Cieľ 2.2: Efektívne zavádzanie bezpečnostných technológií a procesov časť Cieľový stav. Ideálne doplniť k časti o využívaní automatizovaných detekčných nástrojov a technológií zabezpečujúcich včasnú detekciu incidentných stavov.	N	Vzhľadom na povahu predloženého materiálu ponechaný pôvodný text.
RÚZSR Republiková únia zamestnávateľov	O	Celému materiálu Navrhujeme doplniť sadu kľúčových výkonnostných indikátorov (KPI) pre každý strategický cieľ, vrátane merateľných výsledkov a termínov na roky 2026–2030. Odôvodnenie:	ČA	Predložená stratégia je východiskovým strategickým dokumentom, ktorá nadväzuje na predchádzajúce

		Stratégia je prevažne deklaratívna a neobsahuje konkrétne merateľné ukazovatele výkonu ani termíny realizácie. Bez KPI nie je možné vyhodnocovať priebeh implementácie ani riadiť verejné investície.		strategické dokumenty v oblasti kybernetickej bezpečnosti a plnenie strategických cieľov v nej stanovených sa bude realizovať na základe jasne zadaných úloh, časovom harmonograme, zodpovednosti a merateľných ukazovateľov v Akčnom pláne realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030.
RÚZSR Republiková únia zamestnávateľov	Z	Celému materiálu Navrhujeme doplniť záväzné mechanizmy financovania, najmä: • národný fond kybernetickej odolnosti KI, • možnosť čerpania z fondov EÚ (DIGITAL EUROPE, CEF2, Horizon Europe), • daňové stimuly pre investície do kyberbezpečnosti, • schému spolufinancovania pre povinné opatrenia podľa NIS2/CER, • cenovú reguláciu v regulovaných odvetviach umožňujúcu premietnutie nákladov. Odôvodnenie: Prevádzkovatelia KI budú musieť investovať do rozsiahlych	ČA	Pripomienku nie je možné akceptovať v plnom rozsahu, vzhľadom na charakter predloženého materiálu. Stratégia má povahu deklarátórneho materiálu a nepresahuje všeobecne záväzný právny predpis, odráža faktický právny stav. Financovanie v oblasti

		bezpečnostných úprav (sieťová segmentácia, monitoring, detekčné systémy, penetračné testovanie, audity, implementácia PQC, certifikácie, školenia). Bez definovaného mechanizmu spolufinancovania, grantových schém, daňových úľav alebo európskych finančných nástrojov môže byť implementácia pre niektoré odvetvia ekonomicky neudržateľná, najmä pre regulované sektory (energia, voda, doprava, zdravotníctvo).	kybernetickej bezpečnosti bolo zohľadnené pri legislatívnom procese zákona 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. Do Doložky vybraných vplyvov v časti 10. Poznámky doplnená informácia: „Financovanie v oblasti kybernetickej bezpečnosti bolo zohľadnené pri legislatívnom procese zákona 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. Financovanie opatrení v predkladanej stratégii bude zabezpečené v rámci kapitol jednotlivých ústredných orgánov (sektorové politiky), rozpočtových opatrení pre rozpočtové organizácie, medzirezortných programov (napr. v rámci ochrany kritickej infraštruktúry je vytvorený medzirezortný rozpočtový program 0AS Ochrana kritickej infraštruktúry v SR), zdieľaných zdrojov EÚ [programy kohéznej politiky (napr. Program Slovensko), priamo riadené
--	--	--	--	--

			programy (napr. Digital Europe Programme], bilaterálnych programov SR zameraných na vedu a výskum, a iných, ktoré podporujú činnosti v oblasti vedy, výskumu a inovácií aj z oblasti bezpečnosti) a príspevkov jednotlivých prevádzkovateľov základnej služby.“. Financovanie kritických subjektov pri plnení opatrení (bývalých prevádzkovateľov prvkov kritickej infraštruktúry) je riešené v Stratégii odolnosti kritických subjektov Slovenskej republiky, schválenej uznesením vlády Slovenskej republiky č. 3 z 09.01.2026.
--	--	--	---

RÚZSR Republiková únia zamestnávateľov	Z	časti VII, str. 33 Strana 33 Implementačný rámec navrhujeme doplnenia: Kybernetická bezpečnosť priamo súvisí alebo úzko interaguje s inými oblasťami práva a správy vecí verejných. Ide predovšetkým o oblasti súvisiace s: – informatizáciou a digitalizáciou verejnej správy, – ochranou kritickej infraštruktúry, – krízovým riadením štátu, – obranou štátu, – ochranou osobných údajov – „interoperabilitu 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.“	A Text upravený v zmysle pripomienky: „Kybernetická bezpečnosť priamo súvisí alebo úzko interaguje s inými oblasťami práva a správy vecí verejných. Ide predovšetkým o oblasti súvisiace s: – informatizáciou a digitalizáciou verejnej správy, – ochranou kritickej infraštruktúry, – krízovým riadením štátu, – obranou štátu, – ochranou osobných údajov – interoperabilitu 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.“.
RÚZSR Republiková únia zamestnávateľov	Z	Celému materiálu Navrhujeme doplniť záväzný finančný rámec stratégie, ktorý bude obsahovať: • minimálne ročné investičné potreby podľa jednotlivých pilierov, • mechanizmus spolufinancovania investícií prevádzkovateľov KI (granty, dotácie, daňové nástroje, úvery), • záväzok vyčlenenia stabilného rozpočtu štátu na kybernetickú odolnosť, • prepojenie na európske finančné mechanizmy v období 2026–2030. Odôvodnenie: Návrh stratégie definuje množstvo opatrení s významnými investičnými dopadmi na prevádzkovateľov kritickej infraštruktúry (napr. prechod na post-kvantovú kryptografiu, budovanie SOC kapacít, bezpečnostné certifikácie, modernizácia OT/IT prostredí, dodávateľské audity, implementácia AI bezpečnostných mechanizmov). Dokument však neobsahuje žiadny rámcový finančný plán, investičné odhady, časové rozdelenie ani mechanizmy spolufinancovania zo strany štátu či EÚ. Bez finančného rámca nie je možné posúdiť uskutočniteľnosť cieľov ani pripravovať investičné plány	ČA	Pripomienku nie je možné akceptovať v plnom rozsahu, vzhľadom na charakter predloženého materiálu. Stratégia má povahu deklaratórneho materiálu a nepresahuje všeobecne záväzný právny predpis, odráža faktický právny stav. Financovanie v oblasti kybernetickej bezpečnosti bolo zohľadnené pri legislatívnom procese zákona 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

		prevádzkovateľov KI. Ide o nedostatok, ktorý môže výrazne ohroziť implementáciu stratégie.	zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony. Do Doložky vybraných vplyvov v časti 10. Poznámky doplnená informácia: „Financovanie v oblasti kybernetickej bezpečnosti bolo zohľadnené pri legislatívnom procese zákona 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. Financovanie opatrení v predkladanej stratégii bude zabezpečené v rámci
--	--	--	--

				kapitol jednotlivých ústredných orgánov (sektorové politiky), rozpočtových opatrení pre rozpočtové organizácie, medzirezortných programov (napr. v rámci ochrany kritickej infraštruktúry je vytvorený medzirezortný rozpočtový program 0AS Ochrana kritickej infraštruktúry v SR), zdieľaných zdrojov EÚ [programy kohéznej politiky (napr. Program Slovensko), priamo riadené programy (napr. Digital Europe Programme], bilaterálnych programov SR zameraných na vedu a výskum, a iných, ktoré podporujú činnosti v oblasti vedy, výskumu a inovácií aj z oblasti bezpečnosti) a
--	--	--	--	--

				príspevkov jednotlivých prevádzkovateľov základnej služby.“. Financovanie kritických subjektov pri plnení opatrení (bývalých prevádzkovateľov prvkov kritickej infraštruktúry) je riešené v Stratégii odolnosti kritických subjektov Slovenskej republiky, schválenej uznesením vlády Slovenskej republiky č. 3 z 09.01.2026.
RÚZSR Republiková únia zamestnávateľov	Z	časti III, str. 12 V časti III. str. 12 navrhujeme doplniť 2. ods. takto: 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.	A	V texte sú doplnené vety v zmysle pripomienky: „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.“.
RÚZSR Republiková únia zamestnávateľov	O	Celému materiálu Navrhujeme doplniť mechanizmy pre: • diplomatickú podporu pri útokoch na KI, • technickú a politickú atribúciu s priamym zapojením KI sektorov, • zdieľanie informácií s európskymi partnermi. Odôvodnenie: Prevádzkovatelia KI sú častými cieľmi štátom podporovaných útokov. Strategické dokumenty EÚ v oblasti kyberdiplomacie zdôrazňujú potrebu prepojenia atribúcie, sankčných mechanizmov a ochrany infraštruktúry. Návrh stratégie tieto väzby ignoruje.	ČA	Predložená stratégia sa vzťahuje na všetkých prevádzkovateľov základnej služby, aj tých ktorí sú kritickými subjektmi. Kybernetická diplomacia, účinný atribučný mechanizmus, strategické partnerstvá a medzinárodná spolupráca sú v predloženej stratégii riadne zadefinované. V oblasti kritickej infraštruktúry bola prijatá Stratégia

				odolnosti kritických subjektov SR (uznesenie vlády SR č. 3 z 09.01.2026), ktorá okrem iného rieši aj spoluprácu (vrátane zdieľania informácií) aj na medzinárodnej úrovni.
RÚZSR Republiková únia zamestnávateľov	O	časti VI. Cieľ 4.1 posledný ods. str. 27 Aké centrum, na čo sa zameriava a samotnú formuláciu je potrebné doplniť.	NEP	Nemá charakter pripomienky. Nie je zrozumiteľné.
RÚZSR Republiková únia zamestnávateľov	Z	Celému materiálu Navrhujeme vytvoriť jednotný model implementácie NIS2 + CER pre kritickú infraštruktúru, ktorý bude obsahovať: • harmonizované procesy riadenia rizík, • jednotnú terminológiu, • spoločné auditné štandardy, • zjednotený reporting incidentov, • spoločný rámec pre kontrolnú a dohľadovú činnosť štátu. Odôvodnenie: V praxi tvoria opatrenia NIS2 a CER jeden spoločný systém riadenia rizík prevádzkovateľov kritickej infraštruktúry. Stratégia však pristupuje k týmto rámcom izolovane, bez harmonizácie postupov, terminológie, kontrolných mechanizmov a reportingových požiadaviek. To môže viesť k duplicite kontrol, regulačnej neistote a neprimeranému administratívne zaťaženiu. Prevádzkovatelia KI potrebujú jednotný ucelený rámec.	ČA	Z hľadiska povahy predloženého materiálu je prepojenie na oblasť kritickej infraštruktúry dostatočné (previazanie na smernicu CER, zvyšovanie odolnosti kritických subjektov, prevádzkovateľov kritickej základnej služby). Povinnosti kritického subjektu pri zabezpečovaní odolnosti kritickej infraštruktúry a zabezpečovaní

				kontinuity poskytovania základnej služby upravuje zákon č. 367/2024 Z. z. o kritickej infraštruktúre a o zmene a doplnení niektorých zákonov, ktorého gestorom je Ministerstvo vnútra Slovenskej republiky. V schválenej Národnej stratégii odolnosti kritických subjektov (uznesenie vlády SR č. 3 z 09.01.2026) sú definované opatrenia, ktoré riešia jednotný model implementácie (napr. IS na reporting incidentov v správe MV SR, ktorý bude kompatibilný s JISKB, aktualizácia terminologického slovníka a pod.). V prípade aplikačných nejasností NBÚ aj MV SR vie metodicky usmerniť a ak by problémy v aplikačnej
--	--	--	--	---

				praxi pretrvávali je možné iniciovať zmenu všeobecne záväzných právnych predpisov.
RÚZSR Republiková únia zamestnávateľov	O	Celému materiálu Navrhujeme doplniť opatrenia na podporu odborníkov v KI sektoroch, najmä: • národné programy certifikácií, • podporné schémy pre odborníkov pracujúcich v KI, • finančné a kariérne stimuly, • spoločné vzdelávacie programy s priemyslom Odôvodnenie: Na trhu práce pretrvávajú nedostatok kvalifikovaných odborníkov v oblasti kybernetickej a infraštruktúrnej bezpečnosti. Stratégia neobsahuje systémové opatrenia na stabilizáciu personálnych kapacít v kritických odvetviach (napr. podpora certifikácií, kariérne programy, štátne stimuly, sektorové školenia). Bez riešenia tejto oblasti nie je možné zabezpečiť dlhodobú udržateľnosť implementácie.	ČA	Pripomienka bude zohľadnená pri tvorbe Akčného plánu realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030.
RÚZSR Republiková únia zamestnávateľov	Z	časti VI. Cieľ 5.1. VI. Cieľ 5.1 posledná veta na str. 30 znie: „V úzkej spolupráci medzi Ministerstvom zahraničných vecí a európskych záležitostí Slovenskej republiky a ďalšími relevantnými orgánmi Slovensko aktívne pôsobí v medzinárodných organizáciách, svetových a európskych fórach, ktoré formujú normy, štandardy a politiky v oblasti kybernetickej bezpečnosti s cieľom zvyšovať diplomatickú angažovanosť Slovenska, posilňovať jeho viditeľnosť a budovať	A	Text upravený v zmysle pripomienky aj s ohľadom na pripomienku Ministerstva obrany Slovenskej republiky nasledujúco: „V úzkej spolupráci medzi Ministerstvom zahraničných vecí a

		tzv. image modernej a bezpečnej krajiny a prispievať k utváraniu medzinárodného prostredia založeného na zodpovednom správaní štátov v kybernetickom priestore.“		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.“.
RÚZSR Republiková únia zamestnávateľov	Z	časti IV, str. 13 V časti IV. str. 13 Závazný právny rámec chýba zohľadnenie aj právnych rámcov, ktoré buď priamo alebo aj nepriamo majú	ČA	Pripomienku nemožno akceptovať v plnom rozsahu z dôvodu, že

		vpływ na obszar cybernetycznej bezpieczeństwa, np.: 1. W obszarze odporności krytycznej infrastruktury: rozporządzenie DORA-2022/2554 2. W obszarze tożsamości, poufności i ochrony danych: rozporządzenie eIDAS-910/2014 GDPR, + błąd zaniechanie aktualnych trendów - wymiany, udziały i interoperacyjności danych użytkowników- Rozporządzenie Data Governance act a Rozporządzenie Data Act 3. w obszarze cyfrowych usług: Rozporządzenie DSA 2022/2065 Odwołanie: Domniemy, że NBU by miało także w strategii KB jasno zdefiniować rolę głównego zarządcy cybernetycznej bezpieczeństwa SR, który obejmuje wszystkie obszary cybernetycznej bezpieczeństwa.		wprowadzone akty prawne są sektorowymi regulacjami a charakter przedłożonego dokumentu wymaga sektorowo neutralnego (aktualnego) zaniechania.
RÚZSR Republiková únia zamestnávateľov	O	Celému materiálu Navrhujeme doplniť do stratégie explicitnú úlohu SC-KI-SR ako súčasť národného ekosystému monitoringu a reakcie. Odôvodnenie: SC-KI-SR predstavuje už existujúci projekt s významným dopadom na monitoring a ochranu kritickej infraštruktúry. Jeho úplné vynechanie zo stratégie môže viesť k duplicite národných kapacít a k neefektívnemu riadeniu zdrojov.	N	Pripomienka bude zohľadnená pri tvorbe Akčného plánu realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030. Zároveň je potrebné prihliadať na zákonné rámce a úlohy stanovené v oblasti kybernetickej bezpečnosti jednotlivým ústredným orgánom.
RÚZSR Republiková únia zamestnávateľov	Z	časti VI. Cieľ 3.1 predposledný ods. str. 25 VI. Cieľ 3.1 predposledný ods. str. 25, prvá veta znie: „Digitálne produkty a služby sú vyvíjané a uvádzané na trh v	A	Text upravený v zmysle pripomienky: „Digitálne produkty a služby sú vyvíjané a

		súlade s požiadavkami aktu o kybernetickej odolnosti, aktu o umelej inteligencii a ďalšími legislatívnymi požiadavkami.“ Odôvodnenie: Vid komentár v časti IV.-Záväzný právny rámec		uvádzané na trh v súlade s požiadavkami aktu o kybernetickej odolnosti, aktu o umelej inteligencii a ďalšími legislatívnymi požiadavkami.“.
RÚZSR Republiková únia zamestnávateľov	Z	Celému materiálu Doplniť Republikovú únie zamestnávateľov (RÚZ) ako: • povinného konzultačného partnera, • člena pracovných skupín pre PQC, SCRM, NIS2/CER implementáciu a architektúru SOC, • partnera pri tvorbe akčného plánu, • partnera Monitorovacieho výboru Odôvodnenie: RÚZ a v nej združené sektorové profesijné organizácie zabezpečujú odbornú koordináciu, výmenu informácií a pripomienkovanie opatrení na úrovni jednotlivých odvetví kritickej infraštruktúry. Návrh stratégie však ignoruje ich systémovú úlohu a nezaraduje ich medzi partnerov implementácie, konzultácií ani do pracovných skupín. Takýto prístup obmedzuje možnosť participácie sektorov na formovaní štátnych opatrení a môže viesť k nízkej akceptácii regulácií zo strany prevádzkovateľov KI.	A	V kapitole VII. Implementačný rámec v časti „Zainteresované subjekty“ doplnený text: „ • zástupcovia podnikov, podnikateľov a prevádzkovateľov základných služieb zo súkromného sektora“.
RÚZSR Republiková únia zamestnávateľov	Z	časti VI, cieľ 2.1 Cieľový stav V 2. vete je nevyhnutne skonštatovať, kto je hlavný garant kybernetickej bezpečnosti SR.	A	Text upravený v zmysle pripomienky: „Zodpovednosť za kybernetickú bezpečnosť je zmysluplne

				distribúovaná 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.“.
RÚZSR Republiková únia zamestnávateľov	Z	časti VI. Cieľ 4.2: VI. Cieľ 4.2: Zvyšovanie digitálnej gramotnosti občanov a bezpečnostného povedomia V rámci tohto bodu chýba, že NBU zároveň na národnej úrovni podporuje cielenú a systematickú digitalizáciu verejných služieb a ich bezpečné využívanie, pretože získané zručnosti a znalosti v oblasti digitálnej gramotnosti je nevyhnutné každodenne využívať a rozvíjať praxou.	A	Text upravený v zmysle pripomienky primerane. Doplnená veta: „Národný bezpečnostný úrad na národnej úrovni podporuje cielenú a systematickú digitalizáciu verejných služieb a ich bezpečné využívanie.“.

RÚZSR Republiková únia zamestnávateľov	Z	časti II, odsek Kvantové technológie, strana 6 V druhom odseku navrhujeme za druhú vetu doplniť novú vetu v znení: „Pre súkromný sektor má prípadná realizácia opatrení prechodu na PQC dobrovoľný charakter.“. Odôvodnenie: Odporúčanie Európskej komisie o Pláne koordinovaného vykonávania prechodu na postkvantovú kryptografiu ako aj následne vypracovaný Koordinovaný plán vykonávania prechodu na postkvantovú kryptografiu, majú nezáväzný, odporúčací charakter a nepredstavujú právne záväzné akty EÚ. Cieľom navrhovaného doplnenia je predísť výkladovým nejasnostiam, podľa ktorých by mohli byť tieto dokumenty vnímané ako implicitne záväzné pre súkromný sektor. Zároveň sa tým sleduje snaha zabrániť vzniku neprimeranej alebo predčasnej finančnej a administratívnej záťaže pre súkromné subjekty, najmä v situácii, keď prechod na PQC môže vyžadovať významné investície do technológií, systémov a odborných kapacít.	A Doplnený text: „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.“. Pripomienkujúci subjekt súhlasil s kompromisným znením textu mejlom 20.01.2026.
RÚZSR Republiková únia zamestnávateľov	Z	časti VII, str. 32 Časť VI. má byť označená „VII.“ Na strane 32 Implementačný rámec navrhujeme úpravy v 2. a 4. vete: „Akčný plán musí byť v súlade s prioritami stratégie a zároveň dostatočne flexibilný, aby mohol reagovať na trendy, meniace sa podmienky a potreby spoločnosti. ...“	A	Text upravený primerane v zmysle pripomienky: „Akčný plán musí byť v súlade s prioritami stratégie a zároveň dostatočne flexibilný, aby mohol reagovať na

		„...Po prijatí národnej stratégie, Slovenská republika notifikuje o národnej stratégii kybernetickej bezpečnosti SR Európsku komisiu do troch mesiacov od jej prijatia.“		trendy, meniace sa podmienky a potreby spoločnosti.“„Po prijatí národnej stratégie, Slovenská republika notifikuje o národnej stratégii Európsku komisiu do troch mesiacov od jej prijatia.“.
RÚZSR Republiková únia zamestnávateľov	Z	časti VII, str. 32, odsek Akčný plán Časť VI. má byť označená „VII.“ Na konci navrhujeme doplniť poslednú vetu v znení: „Navrhované úlohy však nesmú neprimeraným spôsobom finančne a administratívne zaťažovať podnikateľské subjekty, ktoré boli určené ako prevádzkovatelia základných služieb alebo ako prevádzkovatelia kritických základných služieb. Odôvodnenie: Podnikateľské subjekty identifikované ako prevádzkovatelia základných služieb alebo ako prevádzkovatelia kritických základných služieb budú povinné plniť rozsiahle povinnosti a znášať finančné náklady spojené s implementáciou povinností vyplývajúcich zo zákona o kybernetickej bezpečnosti v znení jeho poslednej novely, a preto je potrebné, aby nové procesy, formy spolupráce, výmena informácií a ostatné povinnosti, ktoré môžu vyplývať z navrhovaných úloh boli realizované spôsobom, ktorý rešpektuje primeranosť, minimalizuje administratívnu a finančnú záťaž a nevytvára dodatočné povinnosti nad rámec	A	K prvej časti pripomienky - Text upravený v zmysle pripomienky: „VII. Implementačný rámec“. K druhej časti pripomienky - Doplnený text: „Navrhované opatrenia budú vychádzať z analýzy prostredia, rizík a potrieb subjektu, pričom financovanie bude prebiehať v rámci vlastných rozpočtov, programov a projektov, medzirezortných

		zákonných požiadaviek. Uvedené opatrenia by preto mali byť vykonávané s dôrazom na efektívnosť, minimálne finančné a administratívne zaťaženie podnikateľských subjektov a na zachovanie rovnováhy medzi verejným záujmom a ochranou podnikateľského prostredia.	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.“. Do Doložky vybraných vplyvov v časti 10. Poznámky doplnená informácia: „Financovanie v oblasti kybernetickej bezpečnosti bolo zohľadnené pri legislatívnom procese zákona 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. Financovanie naplánovaných opatrení bude
--	--	--	--

			zabezpečené v rámci kapitol jednotlivých ústredných orgánov (sektorové politiky), rozpočtových opatrení pre rozpočtové organizácie, medzirezortných programov (napr. v rámci ochrany kritickej infraštruktúry je vytvorený medzirezortný rozpočtový program 0AS Ochrana kritickej infraštruktúry v SR), zdieľaných zdrojov EÚ [programy kohéznej politiky (napr. Program Slovensko), priamo riadené programy (napr. Digital Europe Programme], bilaterálnych programov SR zameraných na vedu a výskum, a iných, ktoré podporujú činnosti v oblasti vedy, výskumu a inovácií aj z oblasti
--	--	--	---

				bezpečnosti) a príspevkov jednotlivých prevádzkovateľov základnej služby.“. Pripomienkujúci subjekt súhlasil s kompromisným znením textu mejlom 20.01.2026.
RÚZSR Republiková únia zamestnávateľov	Z	Celému materiálu Navrhujeme doplniť technickú architektúru národného situačného povedomia, vrátane: • definície dátových tokov KI ↔ sektorové CSIRT ↔ SK-CERT ↔ štátne orgány, • jednotných API a bezpečnostných štandardov, • požiadaviek na PQC-ready komunikáciu • pravidiel pre integráciu sektorových SOC, • štandardov pre AI-asistované detekčné mechanizmy. Odôvodnenie: Stratégia deklaruje potrebu vybudovania národného systému situačného povedomia, no neobsahuje žiadny opis architektúry, štandardov, rozhraní, požiadaviek na integráciu ani modelu zdieľania údajov. Prevádzkovatelia KI tak nemajú možnosť plánovať integráciu svojich SOC alebo OT systémov. Absencia architektúry hrozí duplicitou investícií, nekompatibilitou systémov a právnou neistotou pri ochrane údajov.	ČA	Vzhľadom na povahu predloženého materiálu nepovažujeme za potrebné problematiku riešiť v tomto dokumente. Oblasť post-quantovej kryptografie (PQC) bude ukotvená v samostatnom strategickom dokumente, čiže doplnením do predloženej stratégie by vznikla nadbytočná duplicita aj v súvislosti s plnením jednotlivých opatrení a ich odpočtom.

				Architektúra národného situačného povedomia bude budovaná a konzultovaná postupne v súlade s právnym rámcom a bezpečnostnými štandardmi.
SOCPOIST Sociálna poisťovňa, Ul. 29 augusta č. 8 a 10, 813 63 Bratislava 1	O	K vlastnému materiálu – IV. Východiská - Záväzný právny rámec, str. 13 Navrhujeme doplniť medzi záväzné právne akty aj ochranu osobných údajov a dátovú legislatívu, napr. vetou: „V oblasti ochrany osobných údajov a správy dát národná stratégia zohľadňuje rámec všeobecného nariadenia (EÚ) 2016/679 (GDPR), zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, nariadenia (EÚ) 2023/2854 (akt o údajoch) a nariadenia (EÚ) 2022/868 (akt o správe údajov).“. Stratégia už pracuje s kľúčovými európskymi aktmi (NIS2, AI Act, CRA, CER, akt o kybernetickej solidarite), ale explicitne neuvádza GDPR a dátovú legislatívu, ktorá je pre subjekty verejnej správy (vrátane Sociálnej poisťovne) kľúčová. Doplnenie zvýši úplnosť a konzistentnosť právneho rámca, bez dopadu na vecnú podstatu dokumentu.	ČA	Pripomienku nemožno akceptovať v plnom rozsahu z dôvodu, uvedení nariadenia sa dotýkajú oblasti údajov a povaha predloženého dokumentu vyžaduje sektorovo neutrálne (súčasnú) znenie. Pripomienka sa bude zohľadňovať pri príprave ďalších legislatívnych a nelegislatívnych materiálov.
SOCPOIST Sociálna poisťovňa, Ul. 29 augusta č. 8 a 10, 813 63 Bratislava 1	O	K vlastnému materiálu – IV. Východiská – Strategicko-politický rámec, str. 13 Odporúčame doplniť explicitný odkaz na právny rámec informačných technológií verejnej správy a e-Governmentu, napr. „V oblasti digitalizácie verejnej správy a informačných technológií verejnej správy, národná stratégia nadväzuje na	N	Pripomienku nemožno akceptovať vzhľadom na povahu predloženého materiálu. Národná koncepcia

		zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení neskorších predpisov, ako aj na ich vykonávacie predpisy.“. Stratégia sa výrazne opiera o bezpečnú digitalizáciu verejnej správy, no právny rámec informačných technológií verejnej správy a e-Governmentu nie je menovite spomenutý. Pre subjekty ako Sociálna poisťovňa, ktoré sú orgánom riadenia informačných technológií verejnej správy, je takéto explicitné prepojenie dôležité pre čitateľnosť, zrozumiteľnosť a správnu interpretáciu dokumentu. Uvedenie konkrétnych právnych predpisov umožňuje jednoznačne identifikovať právny rámec, na ktorý stratégia nadväzuje, a predchádza nejasnostiam pri výklade jej obsahu.		informatizácie verejnej správy bola schválená uznesením vlády Slovenskej republiky č. 649 zo 17. decembra 2025.
SOCPOIST Sociálna poisťovňa, Ul. 29 augusta č. 8 a 10, 813 63 Bratislava 1	O	K predkladacej správe Navrhujeme doplniť do predkladacej správy vysvetľujúcu vetu v znení: „Samotná národná stratégia ako strategický dokument nemá priamy dopad na rozpočet verejnej správy; konkrétne finančné a kapacitné vplyvy na dotknuté subjekty budú identifikované a posúdené v procese prípravy Akčného plánu realizácie národnej stratégie a pri jednotlivých implementačných projektoch.“. V doložke vplyvov sú pri rozpočte verejnej správy, informatizácii a službách verejnej správy uvedené „žiadne vplyvy“. To je formálne správne pre samotný strategický dokument, avšak praktická realizácia cieľov bude vyžadovať investície a personálne kapacity. Doplnením vysvetľujúcej vety, sa zabezpečí jasnosť a transparentnosť dokumentu a zabráni sa nesprávnej interpretácii, že naplnenie stratégie je „bez nákladov“	ČA	Do Doložky vybraných vplyvov v časti 10. Poznámky doplnená informácia: „Financovanie v oblasti kybernetickej bezpečnosti bolo zohľadnené pri legislatívnom procese zákona č. 366/2024 Z. z., ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene

		a súčasne ponechá vyhodnotenie konkrétnych vplyvov na úroveň akčného plánu.	a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony. Financovanie opatrení v predkladanej stratégii bude zabezpečené v rámci kapitol jednotlivých ústredných orgánov (sektorové politiky), rozpočtových opatrení pre rozpočtové organizácie, medzirezortných programov (napr. v rámci ochrany kritickej infraštruktúry je vytvorený medzirezortný rozpočtový program 0AS Ochrana kritickej infraštruktúry v SR), zdieľaných zdrojov EÚ [programy kohéznej politiky (napr. Program Slovensko), priamo riadené programy (napr.
--	--	--	--

				Digital Europe Programme], bilaterálnych programov SR zameraných na vedu a výskum, a iných, ktoré podporujú činnosti v oblasti vedy, výskumu a inovácií aj z oblasti bezpečnosti) a príspevkov jednotlivých prevádzkovateľov základnej služby.“.
SOCPOIST Sociálna poisťovňa, Ul. 29 augusta č. 8 a 10, 813 63 Bratislava 1	O	K doložke vybraných vplyvov - časť 4. Dotknuté subjekty, str. 1 Odporúčame spresnenie zoznamu dotknutých subjektov doplnením slovného spojenia: „vrátane verejnoprávných inštitúcií so celoštátnou pôsobnosťou v oblasti sociálneho zabezpečenia a iných systémovo významných inštitúcií verejnej správy“. V doložke sú dotknuté subjekty zoskupené do všeobecných kategórií (ministerstvá, ostatné ÚOŠS, orgány štátnej správy, prevádzkovatelia základných služieb, kritické subjekty). Navrhované spresnenie pomôže lepšej identifikácii systémovo významných verejnoprávných inštitúcií s celoslovenskou pôsobnosťou, ktoré zohrávajú kľúčovú úlohu v systéme sociálneho zabezpečenia a verejnej správy.	A	Text upravený primerane k pripomienke: 4. Dotknuté subjekty ministerstvá, ostatné ústredné orgány štátnej správy, ďalšie orgány štátnej správy s celoštátnou pôsobnosťou, vrátane verejnoprávných inštitúcií s celoštátnou pôsobnosťou a iných systémovo významných inštitúcií verejnej správy, miestne orgány štátnej

				správy, prevádzkovatelia základných služieb, kritické subjekty, akademická obec
TTSK Trnavský samosprávny kraj	Z	Celému materiálu Stratégia veľmi korektne pomenúva, že medzi najzraniteľnejšie a dlhodobé problémové oblasti patria verejná správa a zdravotníctvo, prípadne ďalšie sektory (vzdelávanie, sociálne služby). Zároveň však neobsahuje ani rámcové rozdelenie úloh podľa sektorov a odkazuje len všeobecne na Akčný plán. Navrhujeme, aby stratégia obsahovala aspoň rámcový záväzok, že práve pre tieto dlhodobé problémové sektory budú v Akčnom pláne definované špecifické sektorové úlohy, ciele a minimálne štandardy, ktoré povedú k reálnemu zvýšeniu úrovne kybernetickej bezpečnosti. Návrh doplnenia textu (napr. do časti Ciele / Implementácia): „Vzhľadom na identifikované dlhodobé nedostatky v oblasti kybernetickej bezpečnosti vo verejnej správe, zdravotníctve, vzdelávaní a sociálnych službách bude Akčný plán obsahovať samostatné sektorové kapitoly s konkrétnymi úlohami, minimálnymi štandardmi a harmonogramom zvyšovania úrovne kybernetickej bezpečnosti v týchto sektoroch.“ Týmto sa zabezpečí, že stratégia nebude len všeobecným rámcom, ale bude mať aj jasný dopad práve tam, kde sú dnes najväčšie riziká a kde je dlhodobá implementačná slabina.	ČA	Z povahy materiálu (Akčný plán) je zrejmé, že bude obsahovať špecifické sektorové ciele a nástroje na ich realizáciu. Pre potreby TTSK však dávame do pozornosti strategické materiály aj ústredného ohránu pre sektor verejnej správy (MIRRI SR). Stratégia má povahu deklaratorného materiálu a nepresahuje všeobecne záväzný právny predpis, odráža faktický právny stav. Vzhľadom na pripomienky ďalších subjektov, budú pripomienky v Akčnom pláne realizácie Národnej

		IoT zariadenia – úplne chýbajú, pritom sú kritický problém		stratégie kybernetickej bezpečnosti na roky 2026 až 2030 zohľadnené, pričom materiál bude predmetom pripomienkového konania. Pripomienkujúci subjekt súhlasil s vyhodnotením predkladateľa a netrvá na svojom stanovisku (mejl 16.01.2026). Rozpor bol odstránený.
TTSK Trnavský samosprávny kraj	Z	Celému materiálu Stratégia definuje ciele a princípy na úrovni štátu, avšak nešpecifikuje, akými konkrétnymi podpornými nástrojmi a službami bude štát (NBÚ a ďalšie rezorty) jednotlivým sektorom pri implementácii pomáhať. V prostredí verejnej správy, zdravotníctva a samospráv dlhodobo platí, že subjekty majú limitované kapacity (personálne, finančné, expertné) a nie sú schopné samostatne „znovu vynaliezať koleso“ pre každú oblasť (politiky, metodiky, šablóny, nástroje na monitoring, vzdelávanie a pod.). Bez jasne popísaných centrálnych podporných nástrojov, ktoré budú sektorom reálne k dispozícii, hrozí, že stratégia zostane	N	Vítame snahu a vnímame cieľ pripomienky, avšak z povahy predloženého materiálu ju nie je možné akceptovať. Stratégia má povahu deklarátorneho materiálu a nepresahuje všeobecne záväzný právny predpis, odráža faktický právny stav. Predkladaná stratégia

	prevažne deklaratórna a praktická implementácia bude nerovnomerná – najslabšie sektory (verejná správa, zdravotníctvo, samosprávy) zostanú opäť pozadu. Navrhujeme doplniť do stratégie záväzkov predkladateľa (NBÚ) a dotknutých rezortov, že: Vypracujú a sprístupnia konkrétne podporné balíky pre sektory – najmä verejná správa, zdravotníctvo, vzdelávanie a samosprávy (napr. vzorové smernice a politiky, incident response playbooky, minimálne technické štandardy, vzorové zmluvné klauzuly pre VO, vzdelávacie moduly). Zvážia zriadenie alebo rozšírenie kompetencií napr. pre VUC (napr. národné alebo sektorové SOC/SIEM, portál nástrojov a metodík, centrálné licencie pre vzdelávacie platformy), ktoré budú môcť sektory využívať bez potreby plne individuálnych investícií. Kde môžeme pomáhať našim organizáciám, vzdelávať a pod. V Akčnom pláne bude pre každý kľúčový sektor jasne uvedené, aké konkrétne nástroje, metodiky a služby zo strany štátu budú k dispozícii, vrátane zodpovednosti za ich údržbu a aktualizáciu. Cieľom pripomienky je, aby stratégia nepresúvala celé bremeno implementácie len „nadol“ na jednotlivé subjekty, ale aby jasne deklarovala aj úlohu štátu a NBÚ ako aktívneho poskytovateľa podpory, nie iba regulátora. Napr. stránka https://nis2.nbu.gov.sk/ uz dlho nic neponuka, na stránke NBU je skoro ťažko niečo nájsť, vid CZ https://nukib.gov.cz/cs/kyberneticka-bezpecnost/vzdelavani/?id=168 alebo u nas sú informácie aktuálne od 2018 https://www.sk-cert.sk/sk/rady-a-navody/rady-pre-verejnost/zabezpecenie-uctov-a-zariadeni/index.html a	bola vypracovaná v súlade s § 7 ods. 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 69/2018 Z. z.“), vychádzajúc z čl. 7 smernice NIS 2, kde je jednoznačne vymedzené, čo má stratégia obsahovať a aké sú úlohy zainteresovaných subjektov v oblasti kybernetickej bezpečnosti. Je na zvážení ústredného orgánu ako bude realizovať zákonom stanovené povinnosti. Národný bezpečnostný úrad je koordinačným orgánom a v zmysle zákona č. 69/2018 Z. z. má povinnosť spolupracovať.
--	---	--

		hlavne aj rozbité medzi mirri https://csirt.sk/index.html .. JSIB https://www.sk-cert.sk/sk/rady-a-navody/nahlasit-incident/index.html je zastaralý a pod.		Pripomienkujúci subjekt súhlasil s vyhodnotením predkladateľa a netrvá na svojom stanovisku (mejl 16.01.2026). Rozpor bol odstránený.
TTSK Trnavský samosprávny kraj	Z	Celému materiálu V dokumente absentuje samostatná reflexia IoT zariadení (spotrebiteľské, priemyselné, zdravotnícke, smart city, kamerové systémy, senzory a pod.), hoci práve IoT predstavuje v praxi výrazný zdroj zraniteľností a vstupných bodov pre útoky – a to tak v prostredí verejnej správy, ako aj v kritických a základných službách. Stratégia sa zameriava na certifikáciu produktov, CRA a bezpečnosť dodávateľských reťazcov, avšak IoT ako špecifická kategória nie je pomenovaná ani v analytickej, ani v strategickej časti dokumentu. Navrhujeme doplniť do stratégie: Explicitné pomenovanie IoT zariadení ako významného zdroja kybernetických rizík (najmä v kontexte verejnej správy, zdravotníctva, smart city, dopravy, energetiky a domácností). Zámer NBÚ a štátu podporovať používanie IoT zariadení s preukázanou úrovňou kybernetickej bezpečnosti, preferenčne produktov spĺňajúcich požiadavky EÚ legislatívy (napr. CRA) a EÚ certifikačných schém.	N	Hlavným cieľom predloženej stratégie, ako východiskového strategického dokumentu je systematické posilňovanie odolnosti národného Hlavným cieľom predloženej stratégie, ako východiskového strategického dokumentu je systematické posilňovanie odolnosti národného kybernetického priestoru tak, aby bola adekvátne zabezpečená ochrana práv a bezpečnosť občanov v kybernetickom

		Návrh doplnenia textu (napr. do piliera o bezpečných digitálnych produktoch a službách): „Špecifickú výzvu predstavujú IoT zariadenia (spotrebiteľské, priemyselné, zdravotnícke, mestské a ďalšie), ktoré sa v prostredí verejnej správy a kritických služieb masívne rozširujú, často bez adekvátneho zohľadnenia kybernetickej bezpečnosti. Stratégia preto kladie dôraz na podporu používania IoT zariadení spĺňajúcich požiadavky európskej legislatívy v oblasti kybernetickej bezpečnosti (najmä CRA) a príslušných certifikačných schém, a zároveň na obmedzovanie používania zariadení s nejasným pôvodom alebo nedostatočnou úrovňou zabezpečenia.“ Zohľadnenie IoT zariadení v stratégii je dôležité nielen z technického, ale aj z politického hľadiska – umožní štátu aj samosprávam jasnejšie nastavovať pravidlá a preferencie pri verejnom obstarávaní a pri budovaní infraštruktúry typu „smart city“, kamerových systémov, telemedicíny a pod. Zohľadnenie IoT zariadení v stratégii je dôležité nielen z technického, ale aj z vykonávacieho hľadiska. Bez konkrétnych podporných nástrojov pre sektory ostane stratégia len „na papieri“ Bez konkrétnych podporných nástrojov pre sektory ostane stratégia len „na papieri“	priestore, ochrana kritickej infraštruktúry štátu a prevádzkovateľov základných služieb, ako aj iných životne dôležitých aktív v národnom kybernetickom priestore. Vníname zmysel a cieľ pripomienky avšak bude zohľadnená pri prijímaní ďalších legislatívnych a nelegislatívnych materiálov. Prevádzkovateľ základnej služby má povinnosť, vychádzajúc zo všeobecne záväzných právnych predpisov, v rámci bezpečnostných opatrení, okrem iného, aj identifikovať zraniteľnosti a reagovať na ne. Pripomienkujúci
--	--	--	---

				subjekt súhlasil s vyhodnotením predkladateľa a netrvá na svojom stanovisku (mejl 16.01.2026). Rozpor bol odstránený.
TTSK Trnavský samosprávny kraj	Z	Celému materiálu V texte stratégie sa opakovane odkazuje na budúci Akčný plán, ktorý má konkretizovať úlohy, termíny a zodpovednosti. Dokument však neobsahuje žiadny časový rámec na jeho vypracovanie a schválenie. Navrhujeme, aby stratégia explicitne stanovila termín, dokedy bude Akčný plán vypracovaný a schválený, a zároveň aby bolo zrejmé, že ide o záväzný implementačný dokument, nie dobrovoľný rámec. Návrh doplnenia textu (napr. do časti Implementácia a financovanie): „Na základe tejto Stratégie bude do 6 mesiacov od jej schválenia vypracovaný a vládou SR schválený Akčný plán realizácie Národnej stratégie kybernetickej bezpečnosti, ktorý bude obsahovať konkrétne úlohy, merateľné ukazovatele, termíny a zodpovedné subjekty. Akčný plán sa bude pravidelne aktualizovať minimálne raz za dva roky alebo pri zásadných zmenách regulačného a bezpečnostného prostredia.“ Bez jasného termínu a záväzku na úrovni vlády hrozí, že Akčný plán bude oddialený alebo nebude mať dostatočnú váhu na reálnu implementáciu stratégie.	N	Stratégia sa vydáva v zmysle ustanovení zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, stratégiu schvaľuje vláda Slovenskej republiky, nie je teda zverejňovaná v Zbierke zákonov Slovenskej republiky a nemá všeobecne záväzný charakter. Vzhľadom na povahu dokumentu teda nie je nevyhnutné konkretizovať termíny aj vzhľadom na úlohy navrhnuté v uznesení vlády Slovenskej republiky a ich termín

		Chýbajú sektorové úlohy – najmä pre problémové sektory (VS, zdravotníctvo)		plnenia. Ponechaný pôvodný text. Pre potreby TTSK však dávame do pozornosti strategické materiály ústredného ogránu pre sektor verejnej správy (MIRRI SR). Pripomienkujúci subjekt súhlasil s vyhodnotením predkladateľa a netrvá na svojom stanovisku (mejl 16.01.2026). Rozpor bol odstránený.
UPVSR POaZE Úrad podpredsedu vlády Slovenskej republiky pre Plán obnovy a znalostnú ekonomiku	O	Celému materiálu Strategické ciele potrebujú KPI už teraz: materiál jasne pomenúva prioritné oblasti a strategické ciele, ktoré v nich chce naplňať. K nim však neboli ustanovené indikátory, ktoré by ich urobili v čase odpočítateľnými. Hoci materiál v kap. 6 Implementačný rámec hovorí o KPI, ktoré pre implementáciu pomenuje budúci Akčný plán, v zmysle Metodiky (príloha 4, fáza 5) by indikátory ku strategickým cieľom mali byť už súčasťou tohto strategického materiálu. Akčný plán sa bude môcť zamerať na indikátory úspešnosti implementácie konkrétnych opatrení, ktoré budú pre naplnenie vízie a strategických cieľov prijaté. Úrad podpredsedu vlády SR pre Plán obnovy a znalostnú ekonomiku poskytuje ako gestor	ČA	Predložená stratégia je východiskovým strategickým dokumentom, ktorá nadväzuje na predchádzajúce strategické dokumenty v oblasti kybernetickej bezpečnosti a plnenie strategických cieľov v nej stanovených sa bude realizovať na základe jasne

		Metodiky konzultácie tvorcom materiálov strategického charakteru. V budúcnosti v prípade záujmu o konzultáciu v procese prípravy strategických materiálov sa obráťte na metodika@vlada.gov.sk. Absencia odhadovaných nákladov je riziková a znemožňuje posúdiť realizovateľnosť: Hoci presné sumy bude možné zadať až pri tvorbe Akčných plánov, aj zastrešujúca stratégia by mala obsahovať aspoň rámcový odhad nákladov na realizáciu (Fáza 6, Aktivita 8 Metodiky), bez ktorého nie je možné posúdiť reálnosť stanovených cieľov. Odporúčame tento odhad uviesť aj v doložke vybraných vplyvov. Absentuje overenie vízie a prognóza budúceho vývoja v prioritných oblastiach: materiál nehodnotí realizovateľnosť a adekvátnosť vízie žiadnou špecifickou analýzou, neobsahuje ani výsledok prognózy vývoja v prioritných oblastiach v scenári, kedy by stratégia nevznikla (Fáza 3, Aktivita 4 Metodiky). Absentuje informácia o procese tvorby stratégie a o spôsobe zapojenia relevantných aktérov a partnerov do tvorby stratégie (Fáza 2 Metodiky). Spôsob riadenia implementácie stratégie nie je dostatočne detailne popísaný. Nie je jasné, ako bude vznikajúci monitorovací výbor štruktúrovaný, aké bude mať kompetencie nad rámec monitorovania, ani to, ako sa v ňom budú kompetencie distribuovať či ako sa v ňom budú rodiť rozhodnutia s dopadom na projekt (Fáza 6 Metodiky).	zadeľovaných úloh, časového harmonogramu, zodpovednosti a merateľných ukazovateľov v Akčnom pláne realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030. Všetky povinnosti prevádzkovateľa základnej služby alebo subjekt verejnej správy, začleneného v konkrétnom sektore podľa prílohy I. alebo prílohy II. zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 69/2018 Z. z.“), sú ustanovené v zákone č. 69/2018 Z. z. vychádzajúc zo
--	--	--	---

				smernice NIS 2. Predkladaná stratégia bola vypracovaná v súlade s § 7 ods. 2 zákona č. 69/2018 Z. z. vychádzajúc z čl. 7 smernice NIS 2, pričom reflektuje na právne akty EÚ, ktoré predstavujú základné regulačné východiská pre oblasť kybernetickej bezpečnosti, kde sú explicitne uvedené obsahové náležitosti stratégie. Do Doložky vybraných vplyvov v časti 10. Poznámky doplnená informácia: „Financovanie v oblasti kybernetickej bezpečnosti bolo zohľadnené pri legislatívnom procese zákona 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. Financovanie opatrení v predkladanej stratégii bude zabezpečené v rámci kapitol jednotlivých ústredných orgánov (sektorové politiky), rozpočtových opatrení pre rozpočtové organizácie, medzirezortných programov (napr. v rámci ochrany kritickej infraštruktúry je vytvorený medzirezortný rozpočtový program OAS Ochrana kritickej infraštruktúry v SR), zdieľaných zdrojov EÚ [programy kohéznej politiky (napr.
--	--	--	--	---

				Program Slovensko), priamo riadené programy (napr. Digital Europe Programme], bilaterálnych programov SR zameraných na vedu a výskum, a iných, ktoré podporujú činnosti v oblasti vedy, výskumu a inovácií aj z oblasti bezpečnosti) a príspevkov jednotlivých prevádzkovateľov základnej služby.“.
Verejnost' Verejnost'	O	k vlastnému materiálu K bodu VI., cieľu 1.3 K dodávateľským reťazcom odporúčame doplniť požiadavku jednotného rámca hodnotenia rizikových dodávateľov pre subjekty verejnej správy, zosúladiť hodnotenie dodávateľov s požiadavkami smernice NIS2 a zákona č. 69/2018 Z. z. (ustanovenia o zraniteľnostiach a súvisiacich notifikáciách) a zohľadniť aj špecifiká systémov prevádzkovaných prostredníctvom externých dodávateľov (Managed Services).	ČA	Pripomienka bude zohľadnená pri príprave Akčného plánu realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030.
ÚVSR Úrad vlády Slovenskej republiky	Z	kap. VI. Strategické ciele a piliere Navrhujeme doplniť v Pilieri 4 nový cieľ orientovaný na vzdelávanie zamestnancov verejnej správy, ktorí pracujú finančnými prostriedkami príjmovej a výdavkovej časti rozpočtu EÚ a s verejnými prostriedkami Slovenskej republiky.	ČA	Platí rovnako ako vyššie. Vzhľadom na špecifické postavenie finančného sektora v oblasti kybernetickej

		Zdôvodnenie: Európska komisia vo 36. výročnej správe o ochrane finančných záujmov EÚ vyzýva členské štáty, aby začlenili digitalizáciu boja proti podvodom do svojich národných stratégií, a to s cieľom posúdiť úroveň hrozieb, ktoré pre rozpočet EÚ predstavuje nárast kybernetickej kriminality a využívanie umelej inteligencie, identifikovať medzery vo vedomostiach a zručnostiach pri využívaní inovatívnych technológií a prijať opatrenia na riešenie týchto hrozieb a zraniteľností. S odkazom na článok 325 Zmluvy o fungovaní EÚ sa táto potreba sa týka zamestnancov, ktorí pracujú nielen s príjmovou a výdavkovou časťou rozpočtu EÚ ale aj s verejnými prostriedkami Slovenskej republiky. Cílené vzdelávanie v oblasti kybernetickej bezpečnosti, digitálne podporovaných podvodov, rizík umelej inteligencie a práce s dátami predstavuje kľúčový predpoklad na posilnenie prevencie, včasného odhaľovania a účinného riešenia podvodov v digitálnom prostredí.		bezpečnosti a taktiež na povahu pedkladaného materiálu nie je možné zohľadniť pripomienku v navrhovanom znení, avšak máme za to, že cieľ pripomienky je v predloženej stratégii zohľadnený dostatočne. Budovanie bezpečnostného povedomia a znalostné štandardy v oblasti kybernetickej bezpečnosti sa vzťahujú jednak na prevádzkovateľov základných služieb, ale aj na zamestnancov v špecifických sektoroch. pri príprave Akčného plánu realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030.
--	--	--	--	---

				Pripomienkujúci subjekt vzal na vedomie vyhodnotenie pripomienky a stanovisko predkladateľa mejlom 20.01.2026. Rozpor odstránený.
ÚVSR Úrad vlády Slovenskej republiky	Z	Celému materiálu Navrhujeme doplniť do stratégie v časti venovanej umelej inteligencii aj špecifické riziká jej zneužitia na finančné podvody vo vzťahu k verejným prostriedkom Slovenskej republiky a k rozpočtu Európskej únie (napr. falšovanie dokumentov, neoprávnené transakcie, a pod.). Zdôvodnenie: Umelá inteligencia sa stáva jedným z hlavných nástrojov modernej digitálnej kriminality a je čoraz častejšie využívaná aj pri sofistikovaných finančných podvodoch. Európska komisia v 36. výročnej správe o ochrane finančných záujmov EÚ vyzýva členské štáty, aby začlenili digitalizáciu boja proti podvodom do svojich národných stratégií, a to s cieľom posúdiť úroveň hrozieb, ktoré pre rozpočet EÚ predstavuje nárast kybernetickej kriminality a využívanie umelej inteligencie, identifikovať medzery vo vedomostiach a zručnostiach pri využívaní inovatívnych technológií a prijať opatrenia na riešenie týchto hrozieb a zraniteľností. Opis hrozieb umelej inteligencie v predloženej stratégii má prevažne technický charakter a explicitne nepokrýva riziká finančných podvodov, ktoré majú priamy dopad na verejné prostriedky a rozpočet Európskej únie. Doplnenie tohto aspektu je nevyhnutné z hľadiska komplexného prístupu.	ČA	Platí rovnako ako vyššie. Pripomienku, aj napriek tomu, že sa týka prevádzkovateľov základnej služby, nie je možné akceptovať z dôvodu absencie všeobecne záväzného právneho predpisu v oblasti umelej inteligencie na národnej úrovni. Napriek tomu, že problematika umelej inteligencie sa v mnohých oblastiach prelína v súčasnosti nie je možné ísť nad rámec kompetencií a pôsobnosti ústredných orgánov štátnej správy. V súčasnosti prebieha legislatívny proces k

				návrhu zákona o organizácii štátnej správy v oblasti umelej inteligencie a o zmene a doplnení niektorých zákonov (LP/2025/401). Pripomienkujúci subjekt vzal na vedomie vyhodnotenie pripomienky a stanovisko predkladateľa mejlom 20.01.2026. Rozpor odstránený.
ÚVSR Úrad vlády Slovenskej republiky	Z	Celému materiálu Navrhujeme doplniť do stratégie priority a cieľa na dosiahnutie adekvátnej kybernetickej bezpečnosti v kontexte zabezpečenia ochrany finančných záujmov SR a EÚ. Zároveň navrhujeme, aby stratégia a akčný plán obsahovali rámec pre ochranu digitálnych procesov súvisiacich so správou verejných prostriedkov ako aj s príjmovou a výdavkovou časťou rozpočtu EÚ. Zdôvodnenie: Dokument v predloženom znení nepokrýva kybernetické riziká spojené so správou verejných financií SR ani s ochranou príjmovej a výdavkovej časti rozpočtu EÚ (napr. daňové, colné, rozpočtové, transferové a dotačné procesy). Tieto oblasti pritom predstavujú vysoko atraktívny cieľ kybernetickej	ČA	Akčný plán realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030 bude obsahovať definície cieľov a nástrojov smerujúcich k zabezpečeniu aj uvedených záujmov. Akčný plán realizácie Národnej stratégie kybernetickej bezpečnosti na roky

		kriminality a digitálne podporovaných podvodných schém. Európska komisia vo 36. výročnej správe o ochrane finančných záujmov EÚ vyzýva členské štáty, aby začlenili digitalizáciu boja proti podvodom do svojich národných stratégií, a to s cieľom posúdiť úroveň hrozieb, ktoré pre rozpočet EÚ predstavuje nárast kybernetickej kriminality a využívanie umelej inteligencie, identifikovať medzery vo vedomostiach a zručnostiach pri využívaní inovatívnych technológií a prijať opatrenia na riešenie týchto hrozieb a zraniteľností. Podľa článku 325 Zmluvy o fungovaní Európskej únie je Slovenská republika povinná chrániť finančné záujmy Európskej únie rovnakými nástrojmi a opatreniami, aké uplatňuje pri ochrane vlastných verejných prostriedkov. Zohľadnenie tohto rozmeru v národnej stratégii kybernetickej bezpečnosti je preto nevyhnutné.	2026 až 2030 sa vytvára pre jednotlivé sektory a v spolupráci so zainteresovaným subjektom. Predložená stratégia je prierezovaná a vzhľadom na to, že realizácia jednotlivých cieľov bude obsiahnutá v inom dokumente, akceptácia pripomienky by spôsobila nevyváženosť materiálu. Vzhľadom na špecifické postavenie finančného sektora v oblasti kybernetickej bezpečnosti a taktiež na povahu pedkladaného materiálu nie je možné zohľadniť pripomienku v navrhovanom znení, avšak máme za to, že cieľ pripomienky je v predloženej stratégii zohľadnený
--	--	--	---

				dostatočne. Finančný sektor je prierezový – v rámci regulácie sa zohľadňujú viaceré špecifické rámce (nariadenie DORA, smernica NIS 2, smernica CER). Subjekty zaradené ako prevádzkovatelia základných služieb do finančného sektora majú tiež povinnosť plniť bezpečnostné opatrenia na základe vykonanej analýzy rizík, čo sa v predloženej stratégii aj zohľadňuje a podporuje. Čiastkové, resp. prípadné sektorové stratégie sú záležitosťou príslušného ústredného orgánu (§ 4 a § 9 zákona č. 69/2018 o kybernetickej bezpečnosti a o zmene a doplnení niektorých
--	--	--	--	--

				zákonov v znení neskorších predpisov). Pripomienkujúci subjekt vzal na vedomie vyhodnotenie pripomienky a stanovisko predkladateľa mejlom 20.01.2026. Rozpor odstránený.
ÚVSR Úrad vlády Slovenskej republiky	Z	Celému materiálu Navrhujeme doplniť do implementačného rámca a akčného plánu opatrenia pre zabezpečenie kybernetickej bezpečnosti pre finančnú digitálnu infraštruktúru štátu (najmä daňových a colných systémov, rozpočtových informačných systémov, elektronického verejného obstarávania, IT systémov pre fondy EÚ a pod.). Zdôvodnenie: Tieto systémy sú vysoko rizikové z hľadiska potenciálnych kybernetických útokov, ktoré môžu spôsobiť finančné straty štátu aj EÚ. Odporúčanie EK v rámci 36. výročnej správy o ochrane finančných záujmov EÚ explicitne vyzýva členské štáty k prijatiu opatrení na riešenie digitálnych rizík pre rozpočet EÚ, čo sa dotýka rovnako verejných prostriedkov Slovenskej republiky.	ČA	Platí rovnako ako vyššie. Vzhľadom na špecifické postavenie finančného sektora v oblasti kybernetickej bezpečnosti a taktiež na povahu predkladaného materiálu nie je možné zohľadniť pripomienku v navrhovanom znení, avšak máme za to, že cieľ pripomienky je v predloženej stratégii zohľadnený dostatočne. Pripomienka bude zohľadnená pri

				príprave Akčného plánu realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030. Pripomienkujúci subjekt vzal na vedomie vyhodnotenie pripomienky a stanovisko predkladateľa mejlom 20.01.2026. Rozpor odstránený.
ÚVSR Úrad vlády Slovenskej republiky	Z	Celému materiálu Navrhujeme, aby akčný plán k Národnej stratégii kybernetickej bezpečnosti obsahoval konkrétne opatrenia, zodpovednosti, časový harmonogram a merateľné ukazovatele zamerané na zabezpečenie kybernetickej bezpečnosti informačných systémov, ktoré pracujú s verejnými prostriedkami a rozpočtom Európskej únie. Bez jasne definovaného akčného plánu ostávajú ciele stratégie vo všeobecnej a deklaratórnej rovine. Keďže kybernetické hrozby majú v praxi vždy finančný dopad, je nevyhnutné, aby navrhované opatrenia reflektovali všetky fázy protipodvodného cyklu – prevenciu, odhaľovanie, vyšetrovanie a vymáhanie neoprávnene použitých verejných prostriedkov. Zahrnutie merateľných ukazovateľov umožní priebežne vyhodnocovať účinnosť prijatých opatrení a ich prínos k	A	Akčný plán realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2026 až 2030 je samostatným strategickým dokumentom, ktorý jasne zadefinuje úlohy, časový harmonogram, zodpovednosti a merateľné ukazovatele tak, aby proces dosahovania strategických cieľov

		znižovaniu digitálnych rizík pre verejné financie Slovenskej republiky a rozpočet Európskej únie.		bol efektívny a kontrolovateľný. Pripomienka bude zohľadnená v rámci prípravy akčného plánu. Pripomienkujúci subjekt vzal na vedomie vyhodnotenie pripomienky a stanovisko predkladateľa mejlom 20.01.2026.
MINCRS Ministerstvo cestovného ruchu a športu Slovenskej republiky		Odoslané bez pripomienok		
MPRVSR Ministerstvo pôdohospodárstva a rozvoja vidieka Slovenskej republiky		Odoslané bez pripomienok		
MPSVRSR Ministerstvo práce, sociálnych vecí a rodiny		Odoslané bez pripomienok		

Slovenskej republiky				
NBS Národná banka Slovenska		Odoslané bez pripomienok		
PMÚSR Protimonopolný úrad Slovenskej republiky		Odoslané bez pripomienok		
ÚJDSR Úrad jadrového dozoru Slovenskej republiky		Odoslané bez pripomienok		
ÚNMSSR Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky		Odoslané bez pripomienok		
ÚPVSR Úrad priemyselného vlastníctva Slovenskej republiky		Odoslané bez pripomienok		
ÚVO Úrad pre verejné obstarávanie		Odoslané bez pripomienok		

ŠÚSR Štatistický úrad Slovenskej republiky		Odoslané bez pripomienok		
---	--	--------------------------	--	--

Vznesené hromadné pripomienky

Subjekt	Podporo- vatelia	Pripomienka	Vyh.	Spôsob vyhodnotenia
Filter, z ktorého bol dokument vygenerovaný obsahoval iba nehromadné pripomienky. Uistite sa, že k materiálu neboli pridané aj hromadné pripomienky.				